مؤتمر ريمار الدولي الثالث للعلوم الصرفة والتطبيقية

III.International Rimar Congress of Pure, Applied Sciences

2024

Rimar Academy
Publishing House

مؤتمر ريمار الدولي الثالث للعلوم الصرفة والتطبيقية

FULL TEXT BOOK

كتاب الوقائع

ISBN 978-625956420-3

Publishing House:	دار النشر:	Rimar Academy
Editor:	المحرر:	Prof. Dr. Ghuson H. MOHAMMED
Publication Coordinator:	تنسيق النشر:	AMIR MUAENI
ISBN:	نظام الترميز الدولى لترقيم الكتاب:	978-625-95642-0-3
DOI :	رقم معرف الكائن الرقمي:	http://dx.doi.org/10.47832/RimarCongress03
Printing:	تاريخ الطباعة:	2024 / 12 / 29
Date of The Congress:	تاريخ المؤتمر:	2024 / 11 / 09-08-07
Pages:	عدد الصفحات:	133
URL:	رابط النشر:	www.rimaracademy.com
Certificate Printing Press Number	رقم شهادة المطبعة:	47843

PREFACE

The III. International Rimar Congress of Pure, Applied Sciences ‟Rimar CONGRESS‟, was organized by Igdir University, in collaboration with Remar Academy. The primary objective of this event was to compile and disseminate valuable scientific knowledge and make a meaningful contribution to the future.

Remarkably, a substantial number of researchers, both from local and international backgrounds, demonstrated their interest in this conference. The scientific committee meticulously reviewed the submissions and ultimately accepted a select group of individuals, totaling **22** applicants, **20** of them were accepted by the scientific committee.

The core of this conference was the presentation of **19** complete research papers, while the remaining articles and research findings are set to be featured in forthcoming issues of the MINAR Journal.

I would like to extend my sincere appreciation to all the contributors and scholars who played an essential role in making this conference a resounding success. Your dedication and valuable contributions are deeply respected and acknowledged.

Editor-in-Chief
Prof. Dr. Ghuson H. MOHAMMED

الرؤساء الفخريون
Honorary Committee

Prof. Dr. Mehmet Hakkı ALMA

Rector of Iğdır University
Türkiye

Prof. Dr. Waad Mahmood RAOOF

Rector of Tikrit University
Iraq

Prof. Dr. Alyaa A. Ali Al-ATTAR

Rector of Northern Technical University
Iraq

Prof. Dr. Tariq Hafdhi Abbd Tawfeeq

President of the University of Al-Farhidi
Iraq

Prof. Dr. Khamis A. ZIDAN

Vice Rector of Al-Iraqia University for Scientific Affairs
Iraq

رئيس المؤتمر
Chair of Congress

Prof. Dr. Ghuson H. MOHAMMED

Baghdad University

Iraq

رئيس الهيئة التحضيرية
Chairman of Organizing Committee

Prof. Dr. Muneer salim TAHA

Vice-president for Scientific Affairs of the University of Mosul
Iraq

الأمين العام للمؤتمر
General Secretary

Prof. Dr. Abdulkareem Dash ALI

Dean of the College of Education Pure Science-Tikrit University

Iraq

الهيئة الاستشارية
Consultative Committee

Prof. Dr. Jamal Naser Abed AL_ Rahman AL _Sadoon
Wasit University
Iraq

Prof. Dr. Emad Hasaan Ridha
Basrah University
Iraq

Prof. Dr. Ebtehag Zeki Sulyman Al Halim
University of Mosul
Iraq

Prof. Dr. Nezar Husein Ata Samarah
Jordan university of Science and Technology -Jordan

Dr. Eman SHARAF
Animal Health Research Institute
Egypt

Prof. Dr. Hayajneh, Firas Mahmoud Faleh
Free University, Berlin-Germany
Jordan

Dr. Bader AL-AİFAN
Kuwait University
Kuwait

Dr. Nabil Mohie Abdel–Hamid ALY
Kafrelsheikh University
Egypt

Dr. May Ahmed Fakhry Farhat Mousa
Alexandria University
Egypt

Dr. Osman TÜRK
Harran University
Türkiye

الهيئة التحضيرية
Organizing Committee

Assist. Prof. Dr. Methaq Abd Muslim GUDA
University of Kufa
Iraq

Dr. Haleemah Jaber MOHAMMED
Uruk university
Iraq

Prof.Dr. Jasim Mohammed Mansoor Alzanganawee
University of Diyala
Iraq

Prof. Dr. Lubna Abdulazeem Majeed AL–Bayati
University of Babylon
Iraq

Prof. Dr. Nihad Abdul–Lateef Ali
Al–Qasim Green University
Iraq

Assist. Prof. Jalil Talab ABDULLA
Wasit University
Iraq

Assist. Prof. Iman radha JASIM
University of Mosul
Iraq

Assistant Professor Saba Ali Kadhim
Al–Qasim Green University
Iraq

Lect. Dr. Bassim Kareem Mihsin
General Directorate of Education in Karbala
Iraq

Dr. Riyam Adnan Hammudi Al inizi
College of Medicine, Wasit University
Iraq

Dr. Ihab Qays Ali Aldalawi
f Ibn Sina university for medical and pharmaceutical sciences
Iraq

Dr. Esraa Habeeb Khaleel
Tikrit university
Iraq

Dr. sarab khashea Jameel
AL–Hikmah University College,
Iraq

الهيئة العلمية
Scientific Committee

Prof. Dr. Israa Abdul Razzaq Majed Al-Dobaissi
University of Baghdad
Iraq

Prof. Dr. Nawras Abdelah Alwan
Basrah University
Iraq

Prof. Dr. sheimaa Jabbar Hadi
Al karakh university
Iraq

Assist. Prof. Dr. Faris Ghanim Ahmed Al-Taee
University of Mosul
Iraq

Assist. Prof. Dr. Rana Tariq YAHYA
University of Mosul
Iraq

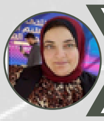
Assist. Prof. Dr. Nihad Taha Mohammed JADDOA
University of Baghdad
Iraq

Assist. Prof. Dr. Raed Obaıd Saleh Saleh
University of Fallujah
Iraq

Lect. Dr. Hadeel Waleed Abdulmalek AlJirjees
Baghdad University
Iraq

Lect. Dr. Sabah Noori HAMMOODİ
AShur University Collage
Iraq

Lect. Dr. Fairooz Faeq Kareem
Open Educational College
Iraq


Dr. May Ahmed Fakhry Farhat Mousa
Alexandria University
Egypt

Dr. Husam R. ABED
Ministry of Education
Iraq

Dr. Shatha Abdullah Mohammed
University of Mosul
Iraq

Dr. Bader AL-AİFAN
Kuwait University
Kuwait

Dr. Jenan Atiyah Ghafil
Baghdad University
Iraq

Dr. Muslim Muhsin ALI
University of Missouri
USA

Dr. Raja'a Al-Naimi
University of Petra
Jordan

Assist . Prof . Dr. Ielaf O Abdul Majjed
University of Mosul
Iraq

Dr. Baraa Ahmed Saeed
Ibn Sina University of Medical and Pharmaceutical Sciences
Iraq

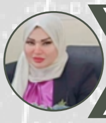
Dr. FOUZIA Youcef
University of Kasdi Merbah Ouargla
Algeria

Dr. Mutasim Ali Mohamed ELAGAB
Gezera University
Sudan

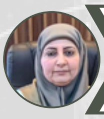
Assist. Prof. Dr. Fatima Rammadan ABDUL
Mustansiriyah University
Iraq

Assist Prof. Farah Tareq Mohammed
University of Mosul
Iraq

Wurood Hantoosh Neamah
University of Basrah
Iraq


Assist. Prof. Dr. Liqaa Zeki Hummady
University of Baghdad
Iraq

Dr.Ahmed Kateb Jumaah
Al-Manara University
Iraq


Dr. Mira Ausama Ahmed Al-Katib
University of Mosul
Iraq

Assist. Prof. Dr. Intisar Ghanim Taha
Damascus University
Syria

Dr. Nisreen SULAYMAN
Damascus University
Syrian

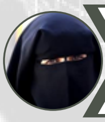
Hanane Elansari
Cadi Ayyad University
Morocco

Dr. Batool Abd Al Ameer Baqer ALSAFAR
Al Mustansiriyah University
Iraq

Dr. Shatha Hizem SHAKER
Tikrit University
Iraq

Dr. Rana Ramzi ABED
University of Mosul
Iraq

Dr. Adwia Jassim Abdul-Alkalik
General Directorate General of Education
Iraq


Assoc. Prof. Dr. Eda M. A. Alshailabi
Omar Almukhtar University
LIBYA

INDEX

PURE SCIENCES, APPLLED SC

Dispersion of unsaturated polyester compound using nano-barium titanate ceramic powder and study of its electrical insulation properties

Abd-Alrahman Khalid Alani [1]

Muna Khalifa Ali [2]

Abstract

To prepare the polymer composites, unsaturated polyester (UPE) was used as the matrix material while BaTiO3 (7-50 nm) was used as the dispersion material in weight proportions of (0.25, 0.75, 1.25 and 2 wt%). The results of this study showed the lowest and highest frequencies (50 Hz and 5 MHz) and the dielectric constant increased with the increase in addition rate. The dielectric constant (ε_r) also varied with the increase in the frequency of the applied electric field in the range of (50 Hz – 5 MHz) at room temperature. The addition rate of BaTiO3 increased with the increase in frequency at both (50Hz) and (5MHz) while the dielectric loss factor decreased with the increase in the frequency of the electric field applied to the fabricated insulating material. The composite samples were prepared using the hand lay-up technique and cut according to the specified parameters. The dielectric constant (ε_r), dielectric loss factor (ε_r^") and alternating conductivity (σ_(a.c)) at different frequencies and temperatures were studied. The results show that the dielectric constant and dielectric loss factor, on the other hand, were found to decrease with the increase of the frequency of the applied electric field, but increased with the increase of the addition ratio of barium and titanium. It increased with the increase of the frequency of the applied electric field..

Keywords: *Dielectric Loss Coefficient, Alternating Electrical, Dielectric Constant, Conductivity, Electric Field Frequency.*

http://dx.doi.org/10.47832/RimarCongress03-1

[1] Ministry of Education, Anbar Educational Directorate, Anbar, Iraq

[2] College of Medicine, Fallujah University, Anbar, Iraq muna.khalifa@uofallujah.edu.iq

1- Introduction

As many industries around the world have experienced tremendous industrial and technological progress, the demand for materials with a wide range of industrial uses, high specifications and low costs has been increasing. This is where the idea of producing so-called composite materials came from [1]. Due to their properties, such as excellent quality and performance as well as acceptable electrical and thermal properties, polymer composites play an important role in the industrial, construction and medical fields. One of the most important new materials that can help solve various challenging problems in daily life is nanocomposites based on a polymer matrix. The final properties of the composite are affected by the size, shape and distribution of the additional particles in the polymer as well as the interface area and bonding type between the particles and the matrix material [2]. In general, mixing or doping polymers leads to changes in their dielectric properties [3]. Ions and electrons are two different forms of charge carriers. Under the influence of an applied electric field, charge carriers in insulators can be transferred in various ways. Insulators differ from conductors and semiconductors in that the conduction band is essentially free of free electrons. Therefore, when an electric field is applied, no current can flow through the band because the electrons cannot move more than a few molecules through the material. However, this restricted movement greatly affects the electrical insulating properties of the material. Since macromolecules do not participate in the transfer of charges and the conductivity of polymers depends on the presence of free ions that are not chemically bound to them, the introduction of low molecular weight impurities becomes the main source of ions. [4].

- **Electrical relative permittivity or the dielectric constant (ε_r):**

Since the capacity of a dielectric depends on its shape and geometry, as well as the shape and type of electrodes across the insulator and the type and composition of the insulating material, it is a measure of the amount of stored charge or capacitance. The dielectric constant or relative permittivity (ε_r) is given by (1) [5].

$$\varepsilon_r = \frac{\varepsilon}{\varepsilon_\circ} = \frac{c}{c_\circ} \qquad (1)$$

or

$$\varepsilon_r = \frac{c\,d}{\varepsilon_\circ\,A} \qquad (2)$$

Where ε_r : dielectric constant, C: Capacity , d: distance between the two widening plates, $\varepsilon_\circ$: Space permittivity, A : cross-sectional area of the sample.

- **Dielectric loss coefficient ($\boldsymbol{\varepsilon_r^{''}}$):**

The insulating material in a capacitor reacts differently to an alternating electric field than to a continuous electric field in terms of its electrical polarization. The complex (combined) dielectric constant of an insulator is given by equation (3) [6] and depends on the frequency of the alternating electric field applied between the capacitor plates..

$$\varepsilon'' = \varepsilon_r' - j\varepsilon_r'' \qquad (3)$$

Where:

ε_r' : The dielectric's polarization or capacitance is represented by the real portion of the dielectric constant.

ε_r'' : The dielectric loss coefficient resulting from electrical conductivity and polarization is represented by the imaginary portion of the dielectric constant.

The quantity of energy held in the insulating medium is measured by the real component of the dielectric constant (ε_r'), which means that (ε_r) = (ε_r'). The imaginary part (ε_r''), also known as the dielectric loss coefficient, measures the amount of energy lost from the dielectric medium in energy storage devices like capacitors. Its value is always greater than zero and is typically lower than the real part, also known as the dielectric constant. The dissipation coefficient (Dissipation Factor: DF) is the ratio of the imaginary to real parts of the permittivity. It can be calculated using the tangent of the angle of loss) $tan\delta$ ((loss tangent) as in equation (4) [7].

$$\varepsilon_r'' = tan\delta\ \varepsilon_r' \qquad (4)$$

- **AC electrical conductivity($\boldsymbol{\sigma_{a.c}}$) :**

Alternating electrical conductivity ($\sigma_{a.c}$) is one of the parameters of the dielectric loss in insulating materials. It depends on the frequency of the applied field (f), and it is one of the factors that contribute to the loss of dielectric, AC electrical conductivity can be determined using eq.(5) [8].

$$\sigma_{a.c} = \frac{f\ \varepsilon_r\ tan\delta}{1.8 \times 10^{10}} \qquad (5)$$

Where:

$\sigma_{a.c}$: AC electrical conductivity, f: frequency of the applied electric field (Hz),

Two factors are responsible for the insulating material's electrical conductivity when an alternating electric field is applied to it:

1- The way that electric dipoles rotate.

2- Movement of electric charges in transition.

Electrical conductivity cannot be caused by the first cause. Regarding the second argument, given that free charges flow within the insulator, it can result in the conductivity of the insulating material. This mobility does not entail abrupt transitions or constant movement among the local levels of the issue. [8].

2- Materials and methods

barium titanate ($BaTiO_3$), (7–50 nm) was used as a reinforcement material with addition percents of (0.25, 0.75, 1.25, and 2wt). Unsaturated polyester resin (UPE) was used as the matrix material. The samples were given any necessary thermal treatment before being cut off in accordance with predetermined standards. Using an LCR Meter (Agilent 4294A type, Precision impedance analyzer) of American origin, with a frequency range (50 Hz - 5 MHz), the prepared composite samples' dielectric constant, dielectric loss coefficient, and alternating electrical conductivity were tested. The LCR Meter has two electrodes between which the sample is placed, and the electrodes must be directly connected to the two surfaces of the sample. Capacitance (C_p), dielectric constant (ε_r), loss angle ($tan\delta$), alternating resistance as a function of frequency for a range (50Hz - 5MHz), as well as continuous resistance as a function of the change in potential difference, are measured by the LCR Meter, which is connected to the computer to display the results immediately on the screen. Equation (2) was used to get the dielectric constant, equation (4) to determine the dielectric loss coefficient, and equation (5) to determine the conductivity of AC electricity.

3- Results and discussion

1- Dielectric constant (ε_r):

a- Effect of addition rate of $BaTiO_3$:

At the lowest and highest frequencies (50 Hz and 5 MHz), Figure 1 illustrates a rise in the dielectric constant with an increase in the addition rate. The reason for this is because $BaTiO_3$ has a ferroelectric property, which is indicated by a higher dielectric constant at laboratory temperature than the polymer does [9]. However, at high frequency (5MHz), the increase in the dielectric constant with the addition ratio will be less than it is at low frequency because the dipoles will not be able to keep up with the change in the high frequency of the effective electric field in addition to the disappearance of ionization. This is because the relaxation processes between the granules of ($BaTiO_3$) and the matrix material led to the emergence of interpolarization, especially at low frequency (50Hz) [10].

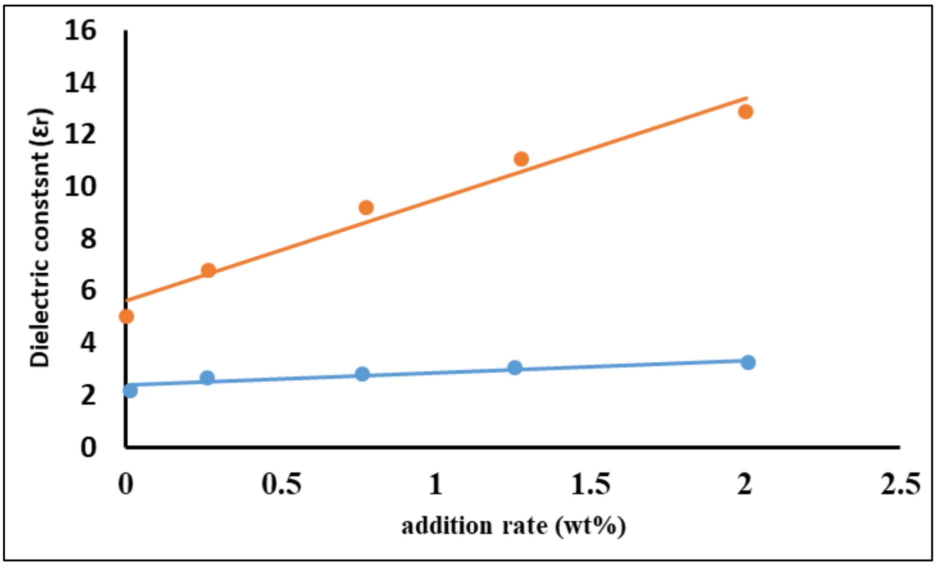


Figure (1) Change of dielectric constant (ε_r) vs addition rate at (50Hz) and (5MHz).

b- Effect of electric field frequency:

Figures (2&4) illustrate how the dielectric constant (ε_r) changes as the applied electric field frequency increases within the range of (50Hz-5MHz) at room temperature. It is important to note that the values of the dielectric constant are high at low frequencies because the dipoles are positioned in the applied electric field's direction and have the necessary time to keep up with the low frequencies. In the majority of insulating materials, this phenomenon is typical.

Additionally, as charges build up at grain boundaries, the samples' vacuole charges become more polarized, which raises the dielectric constant at low frequencies. However, as the frequency of the applied electric field rises, the dielectric constant decreases. Because the dipoles in this scenario are unable to keep up with the rapid reversal of the applied electric field's frequency and catch up with it, the dielectric constant will begin to decrease and become almost stable at high frequencies as if the dielectric constant no longer depends on the applied electric field's frequency. The cause of the low values of the dielectric constant, when the applied electric field's frequency increases, is that the dipoles are unable to keep up with the rapid reversal of the applied [11].

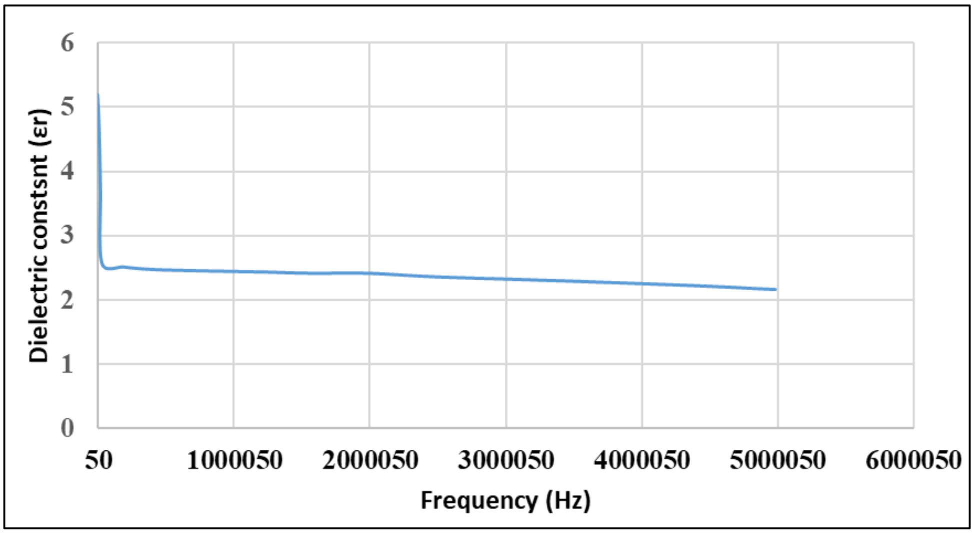


Figure 2: Variation of dielectric constant V_S frequency of [UPE].

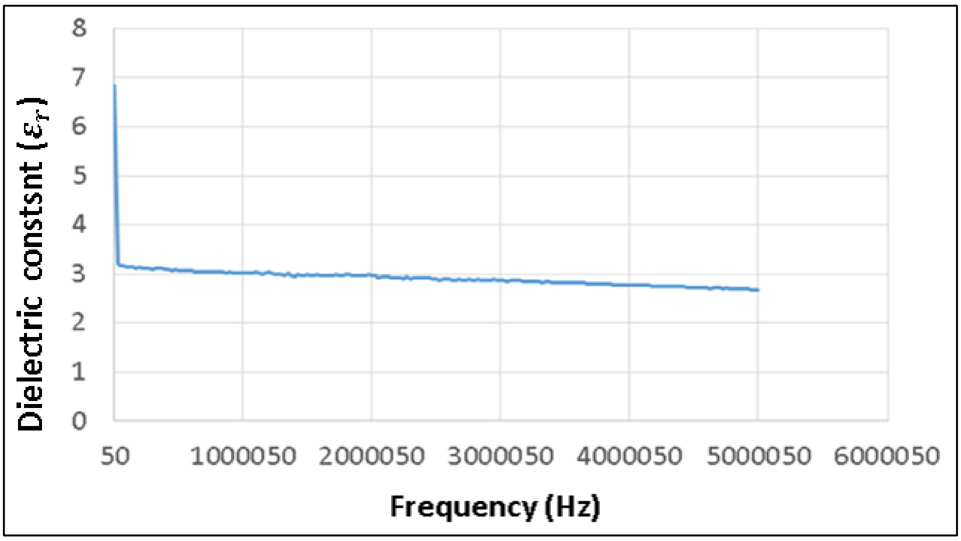


Figure 3: Variation of dielectric constant V_S frequency of [UPE + 0.25 wt% BaTiO3]

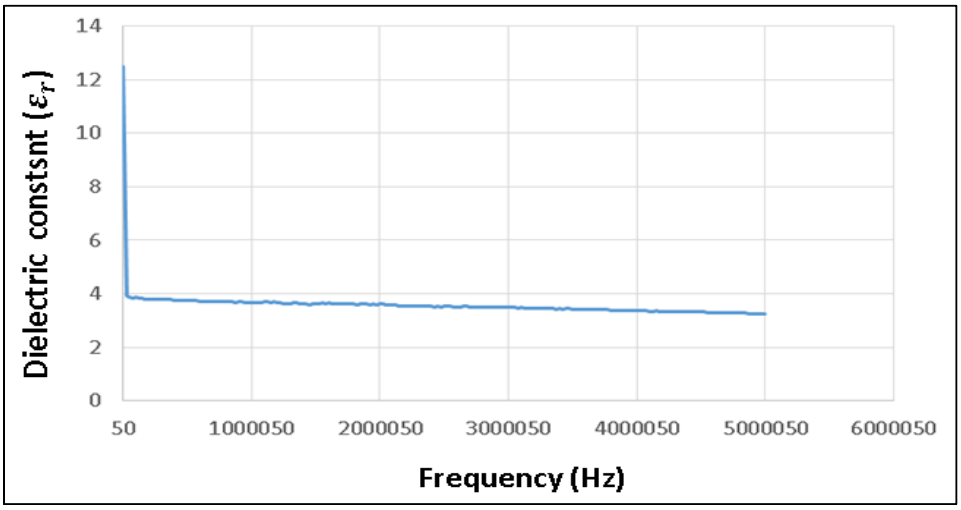


Figure 4: Variation of dielectric constant V_S frequency of [UPE + 2%wt BaTiO3]

2- Dielectric loss coefficient (ε_r''):

a- Effect of the addition rate:

Figure (5) illustrates how the addition rate of $BaTiO_3$ increases with frequency at the frequency (50Hz) and at the frequency (5MHz), increasing the values of the dielectric loss coefficient. Increased vacancy or pore formation and increased interface formation between the ceramic and the polymer result from increased percentages of ceramic material added to the polymer, which raises energy dissipation in those regions and raises the dielectric loss [9].

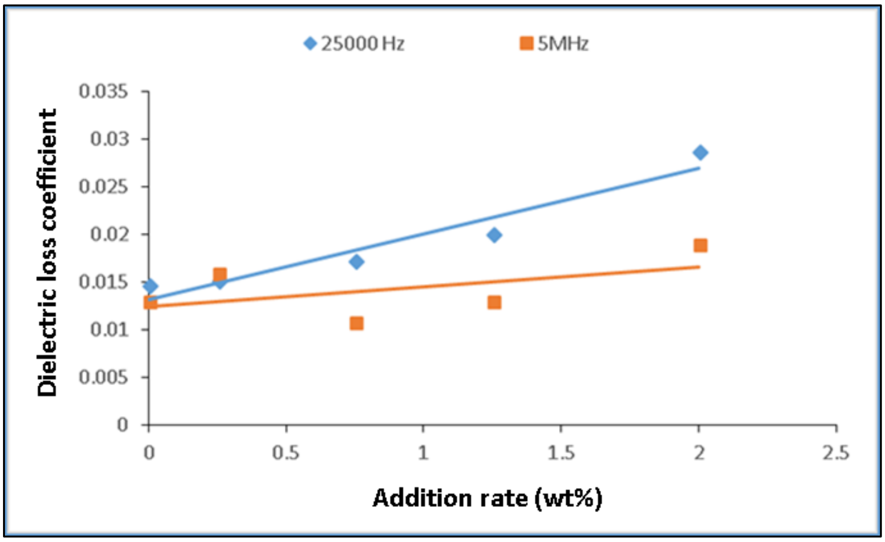


Figure 5: Variation of dielectric loss coefficient VS the addition rate at a frequency (25000Hz) and (5MHz)

b- Effect of electric field frequency:

Figures (6 & 8) make it abundantly evident that for all samples, the dielectric loss coefficient falls as the frequency of the electric field applied to the manufactured insulating material increases. Ionic conductivity and the homogeneous or heterogeneous nature of the material can both have an impact on the properties of a polymeric composite. the fundamental idea underlying the inverse relationship between frequency and dielectric loss, in which frequency increases overcome resistance [12]. The dielectric property of the insulating material weakens or attenuates as the dipoles inside absorb the electric field energy at low frequencies, which is when the dielectric constant is high. As a result, the material's dielectric loss coefficient rises and then decreases with increasing frequency. In some instances, we observe an increase in the dielectric loss as the frequency rises, followed by a return to a drop as the frequency rises. This is caused by the existence of the resonance phenomenon in the test device's electric circuit. [13]

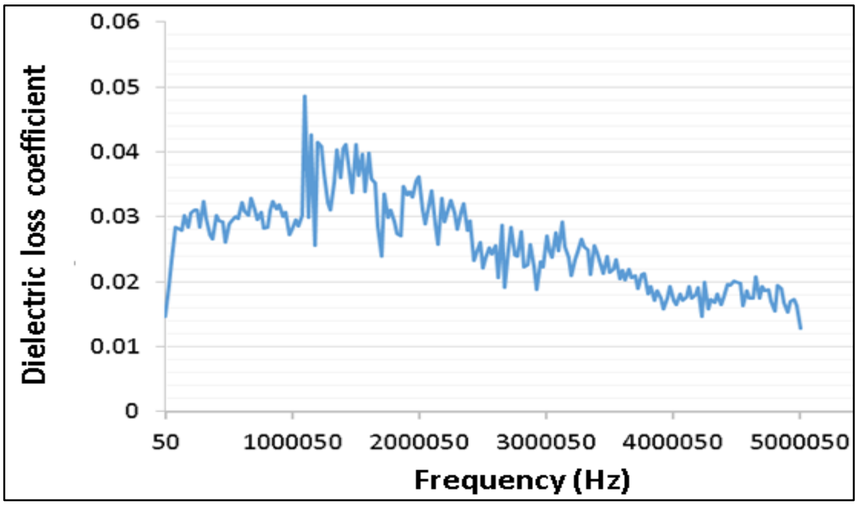


Figure 6: Variation dielectric loss coefficient VS frequency of [UPE].

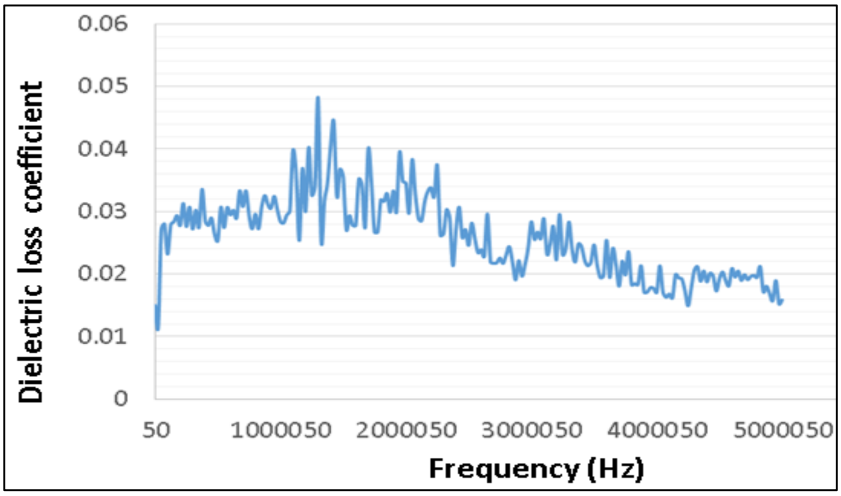


Figure 7: Variation dielectric loss coefficient VS frequency of [UPE+0.25 wt% BaTiO3]

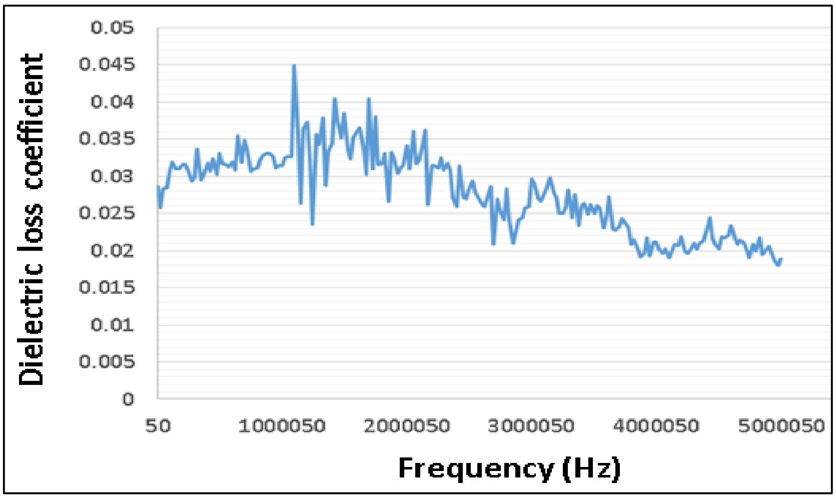


Figure 8 : Variation of dielectric loss coefficient VS frequency of [UPE+2wt% BaTiO3]

3- AC Electrical Conductivity (σa.c):

Figure (9) shows that for all samples, alternating electrical conductivity increases as frequency increases. This indicates that the frequency had a bigger impact on AC electrical conductivity values than the dielectric constant and dielectric loss coefficient. The charge carriers polarize and move as the frequency rises because they have the energy to do so, especially at high frequencies. It is important to note that the charge carriers move because of the frequency increase. Due to the effect of raising the frequency of the effective electric field, this movement is different from the nature of its movement in conductive materials and instead takes the form of transitions (non-continuous jumping) of charge carriers or reorientation between the levels of the local crystal boundaries [14]. The figure also shows that the alternating electrical conductivity of the samples disseminated by addition rates (0.25, 0.75, 1.25 wt%) is lower than that of the UPE sample and the sample that has been dispersed by (2 wt%). When the addition rate is increased to 2% wt, this causes an increase in the pores and interfaces in the composite material, which increases the accumulation of charges in those areas and the leakage current, and thus increases the leakage current. This is because the $BaTiO_3$ is characterized by the piezoelectric property, giving the composite material a high dielectrical constant, making it have a much lower electrical conductivity than the polymers ($\sigma_{a.c}$).

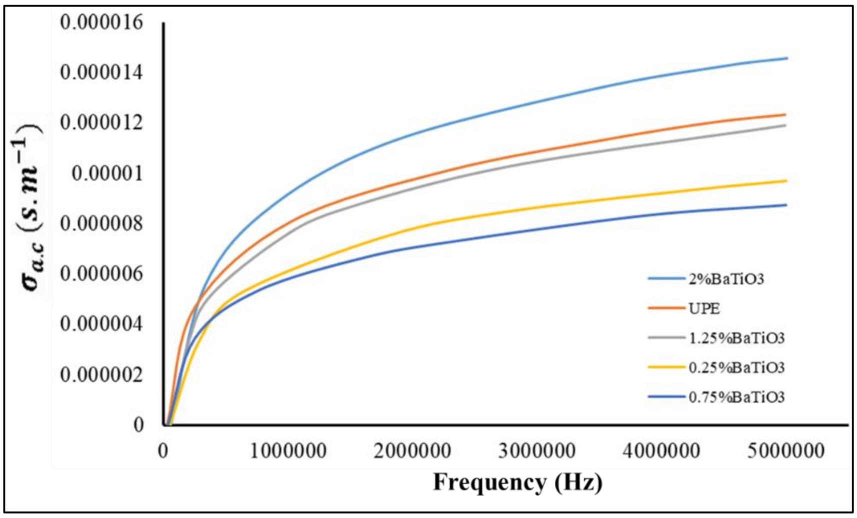


Figure 9: Variation of AC electrical conductivity (σa.c) VS frequency at laboratory temperature

4- Conclusions:

1. The dielectric constant and dielectric loss coefficient of the polymeric composites increase with an increase in the addition rate of BaTiO3 because of the increase in polarity caused by the increase in the number of dipoles per unit volume, whereas they decrease with an increase in the frequency of the applied electric field at the laboratory temperature.

2. The applied electric field has an impact on the piezoelectric composite material's alternating electrical conductivity because the conductivity rises with the frequency of the applied electric field.

3. Ultrasound is used to promote the homogeneity of the distribution of the ceramic powder particles within the polymeric matrix material.

Refrences:

[1] Christensen, Richard M. Mechanics of composite materials. Courier Corporation, 2012.

[2] Zaman, Haydar U., et al. "Morphology, mechanical, and crystallization behaviors of micro-and nano-ZnO filled polypropylene composites." Journal of Reinforced Plastics and Composites 31.5 (2012): 323-329.

[3]] Zaman, Haydar U., et al. "Morphology, mechanical, and crystallization behaviors of micro-and nano-ZnO filled polypropylene composites." Journal of Reinforced Plastics and Composites 31.5 (2012): 323-329.

[4] Smith, William Fortune. "Principles of materials science and engineering." (1986).

[5] Birčáková, Zuzana, et al. "Preparation and characterization of iron-based soft magnetic composites with resin bonded nano-ferrite insulation." Journal of Alloys and Compounds 828 (2020): 154416.

[6] Qi, H. J., K. Joyce, and M. C. Boyce. "Durometer hardness and the stress-strain behavior of elastomeric materials." Rubber chemistry and technology 76.2 (2003): 419-435.

[7] Khan, Muhammad Talha, and Syed Muzamil Ali. "A brief review of measuring techniques for characterization of dielectric materials." International Journal of Information Technology and Electrical Engineering 1.1 (2012): 1-5.

[8] Najim, Mojahid M. "Synthesis and study the structural and physical properties of Nano-BaTiO3." Department of Applied Sciences, University of Technology (2013)..

[9] Li, Y. C., Sie Chin Tjong, and R. K. Y. Li. "Dielectric properties of binary polyvinylidene fluoride/barium titanate nanocomposites and their nanographite doped hybrids." eXPRESS Polymer Letters 5.6 (2011).

[10] Upadhyay, Ravindra H., and Rajendra R. Deshmukh. "A new low dielectric constant barium titanate–poly (methyl methacrylate) nanocomposite films." Advances in Materials Research 2.2 (2013): 99.

[11] Schumacher, Benedikt, et al. "Temperature treatment of nano-scaled barium titanate filler to improve the dielectric properties of high-k polymer based composites." Microelectronic Engineering 87.10 (2010): 1978-1983.

[12] Lothongkam, Chaiyaporn. Dielectric strength behaviour and mechanical properties of transparent insulation materials suitable to optical monitoring of partial discharges. Bundesanstalt für Materialforschung und-prüfung (BAM), 2014.

[13] Yang, Ta-I., and Peter Kofinas. "Dielectric properties of polymer nanoparticle composites." Polymer 48.3 (2007): 791-798.

[14] Najim, Mojahid M. "Synthesis and study the structural and physical properties of Nano-BaTiO3." Department of Applied Sciences, University of Technology (2013).

Article review: Various Efficient Multifactor Methods for User Authentication

Rasha khalid Ibrahim [1]

Mays M. Hoobi [2]

Abstract

According to the wide advancements of the networks and computer applications, the cybersecurity become very important to protect data, cybersecurity refers to measures and controls that ensure the confidentiality, integrity and availability of the information, this includes everything from protecting physical information assets, to data security and computer safety practices. One of security principles a user authentication policy is a process that checking while someone is attempting to access services and applications if he is the same person who claim to be or not. Using a password-based authentication mechanism, the user must prove their identity by entering their password and username. The aim of this article is to look at previous researches experience in user authentication based on password and how this field of authentication can be stronger. In addition to the results of previous researches indicated the security level offered by using password and multifactor methods and how to make these methods more complexity and more secure against the attackers.

Keywords: *Brute Force Attack, Cryptography, Multi Factor Authentication, Password, PIN, User Authentication.*

http://dx.doi.org/10.47832/RimarCongress03-2

[1] College of Science, University of Baghdad, Baghdad, Iraq rasha.Khaled2201m@sc.uobaghdad.edu.iq

[2] College of Science, University of Baghdad, Baghdad, Iraq mays.m@sc.uobaghdad.edu.iq

1. Introduction

As computing systems get more powerful and massive data sets become more accessible, machine learning algorithms have produced significant advances across a wide range of industries. Computer security has been impacted by this progress, leading to a number of studies on learning-based security systems, including binary code analysis, vulnerability identification, and malware detection (Arp, et al., 2022). Cryptography is the study of methods for encrypting data using particular algorithms that make it unreadable to the human eye unless the recipient uses predefined algorithms to decrypt it (Qadir & Varol, 2019). Cryptography work by encryption and decryption. Encryption uses a specific method and a private key to convert the plaintext of readable data into a format that others cannot understand, or ciphertext. Decryption is a process of converting encrypted data in a form that is readable and understood by a human or a computer (Hendi, Dwairi, Al-Qadi, & Soliman, 2019) (Marqas, Almufti, & Ihsan, 2020). Cryptographic systems, which come in symmetric and asymmetric varieties, are used to offer security services that shield data from illegal applications. In symmetric systems, the cipher operation is performed using identical keys by the sender and the recipient. Asymmetric key cryptography, also referred to as public key cryptography, encrypts and decrypts data using two keys. (S.A & N.H.M, 2024)

Authorization, the function of specifying access rights to resources, is related to information security, computer security in general, and access control in particular. More formally, authorization means specifying an access policy. During operation, the system uses access control rules to determine whether access requests from (authenticated) consumers will be approved (granted) or rejected (denied).

Authentication is multi processes from user name and password to different kind of biometrics (ex: fingerprint…etc.) that gives assurance to authenticated clients to access the data and save their information in database to check them when they want to login. There are three factor authentication available, the first one represented by something the user knows, for example password, the second one is represented by something the user has, for example smart cards, and the last one represented by something the user is, for example biometric (behavioral or physiological) (Briceno, et al., 2019) Password authentication falls into the something you know category and is the most common form of authentication.

Something you know requires the user to answer some question assuming that only the valid user knows the correct answer (Shah & Kanhere, 2019).

A password attack is one of the various methods used to maliciously authenticate password-protected accounts. These attacks are usually facilitated through the use of software that speeds up the process of password cracking or guessing. There are different types of password attacks:

- Brute Force Attack: A brute force attack is a method of password assault in which hackers systematically attempt various login combinations in order to get unauthorized access to the data. In another word is typically a manually initiated process used to scan large ranges of IP addresses to find vulnerable accounts. The assault is uncomplicated and frequently use automated techniques, such as software, to attempt numerous permutations of alphanumeric characters (Alkhwaja, et al., 2023) (Bahaa Qasim M. AL-Musawi, 2024).

- Dictionary attack: This is a type of brute force password attack that uses a list of commonly used words and sentences as well as passwords to try to break in. Attackers cut down on the possible passwords to what are called "dictionary words" so they don't have to go through a long list (Alkhwaja, et al., 2023).

- Keylogger attack: A keylogger is a form of spyware that captures and logs the keystrokes performed by the user. Cybercriminals employ keyloggers to acquire sensitive data, such as credit card numbers and passwords. In the course of a password assault, a keylogger records not only the login and password but also the particular application or website that uses them, in addition to other private data. (Wajahat, Imran, Latif, Nazir, & Bilal, 2019).

- Credential stuffing: Attackers employ trial and error to obtain access in credential stuffing password attacks, which are similar to brute force attacks. But they employ credentials that have been stolen, not password guessing. Credential stuffing operates under the presumption that a large number of users reuse their passwords for numerous accounts on various platforms (Ba, Bennett, Gallagher, & Bhunia, 2021).

- Man in the middle: refers to a situation where there are three people: the victim, the attacker, and the third person the victim is trying to communicate. Cybercriminals often use fake emails to look like a trustworthy third-party during password attacks. For example, if a user is already logged in to a web server and has a valid session between them and the server, the attacker takes over that session, or "hijacks" it, and keeps connecting to the server as the user. (Mallik, 2019) (Reem Ismail, 2024).

- Traffic Interception: Threat actors employ traffic interception, a variation of the man-in-the-middle attack, to monitor and capture data by listening to network traffic. Unsecured Wi-Fi networks or communications without encryption, such as HTTP, are prevalent methods of accomplishing this (Birge-Lee, Wang, Rexford, & Mittal, 2019).

- Phishing refers to malicious assaults that aim to get sensitive financial or private information from internet users by using fraudulent websites that resemble real ones. Cybercriminals employ several methods to engage in phishing, such as sending phishing emails, performing man-in-the-middle attacks, and executing spear phishing (a sophisticated password attack that incorporates a voice call and a link). (Ba, Bennett, Gallagher, & Bhunia, 2021) (Mallik, 2019) (Alabdan, 2020) (Mahmood & Hameed, 2023).

- Password spraying: In password spraying, a lot of popular passwords are tried on a small group of user accounts or even on one account. This is another type of brute-force attack. When attackers spray passwords, they do very strange things to avoid being caught. Most of the time, they will do research early on to cut down on the number of logins tries and keep accounts from getting locked. (Alkhwaja, et al., 2023) (Crume, 2022).

- Collision attacks: A collision arises when two distinct inputs provide a same hash value. Hash functions are specifically engineered to reduce the likelihood of collisions, although they are not theoretically impervious to them (Mexriddinovich, 2023)

- The Stuxnet attack: In 2010, there was a cyberattack against the locations where Iran was conducting its nuclear enrichment program. Iran's nuclear program is experiencing disruptions, and the hack exposed the country's inadequate cybersecurity (Çetinkaya & Terzi, 2024).

- Social Engineering (SE) attacks: Just as real-world thieves take advantage of people's weaknesses, so do cybercriminals known as "social engineers," who employ a variety of methods and instruments to launch multiple attacks online (Abu Hweidi & Eleyan, 2023).

- Rainbow attack: It is a parsing attack on the rainbow crypto hash function. The attack involves creating a "rainbow table" of pre-computed hash values for a given set of inputs, which can then be used to efficiently determine which inputs are associated with a given hash value. (OA & AS, 2023)

- Third-party attack: When the activity coordinator receives and processes at least one activity message, extracting data from the message and adding it to a stream associated with one of the messages, involving at least one designated contact and an anonymous contact who is a user of the site. Additionally, the activity message must be in a consistent format. (Abrahami, Bloch, & Achsaf, 2023)

In addition, there are several criteria for strong password as follow: - (Alkhwaja, et al., 2023)

- Password length: longer than 8 character is batter.
- Combination of uppercase, lowercase, symbols and numbers.
- Not a word from dictionary or personal name.
- Not personal information.

2. literature review

This section explains several methods are used in number of important researches; these methods are listed as below:

In (Jarecki, Krawczyk, Shirvanian, & Saxena, 2018), this article aimed to addresses the weaknesses of currently deployed two-factor authentication (TFA) schemes by presenting a rigorous security model of two-factor authentication (TFA) schemes that captures well-defined security limits that can be maximized, and then presenting a practical TFA scheme that has been proven to achieve the robust security guaranteed by the procedures formalized the model, and eventually prototyped several ways to validate a user's possession of a secondary authentication factor. In this research a Two component Authenticated Key Exchange (TFA-KE) model, in which the user provides a password at the client terminal to authenticate with the server; the second component of authentication is demonstrating that the user is in possession of a personal device. The user's claim that the device equals the t-bit checksum provided by the device with the checksum provided by the client establishes device possession under the TFA-KE model. This implements an authenticated channel from the t-bit client user to the device, confirming that the same person controls the client and the device. TFA schemes can now be more secure and user-friendly because these channel authentication requirements are less stringent than those of the private channel needed by PIN-based TFAs.

In (Boopathi & Aramudhan, 2018), It is discovered that, as implied by its name, the two-stage authentication technique consists of two authentication phases. Two servers must be included in the protocol in order to achieve two-step authentication. Initialization, registration, login and authentication, and key creation are the processes that make up this work. Since the primary objective of this technique was to give increased strength during authentication, it was discovered that neither the password change phase nor the cancellation and re-registration phase were present. Master Server (MS) and Authentication Server (AS) are the names of the two servers that have been implemented in the new schemes. When in use, these servers enable complete control over user communications. In order to prevent the AS from learning about the information in the MS, the MS registers at the Registration Center (RC) during the registration phase implementation and maintains the credentials in a private way.

Two kinds of connections are established during the authentication and key generation phase: one between (MS) and (AS) and the other between RC. AS, the user, MS, and RC communicate with each other in addition. Hence, neither the MS nor the user establish a direct communication channel. This configuration, which prevents the AS from immediately obtaining the server details, can address the adversarial nature of the channel. See figure (1).

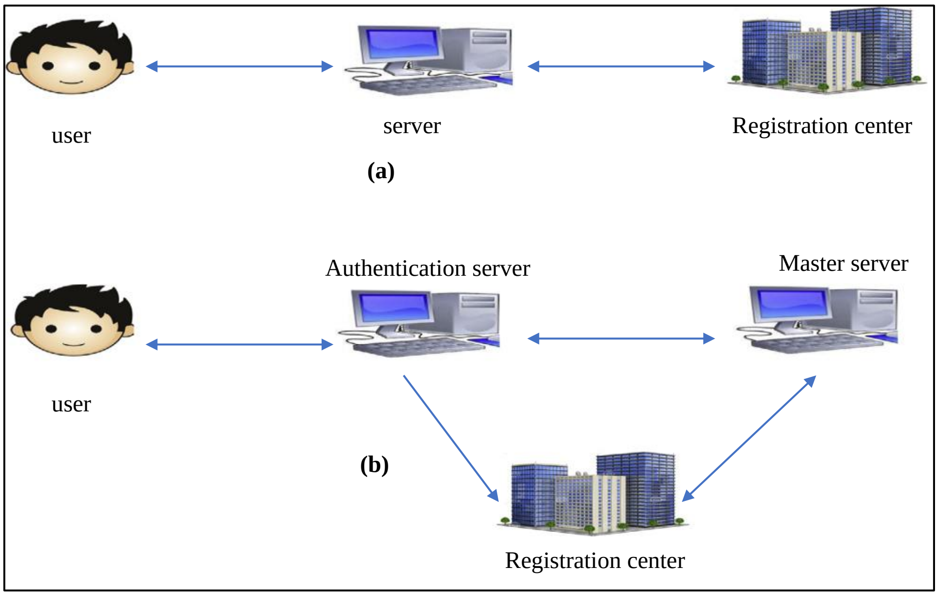


Figure (1) Communication links associated with (a) single stage authentication mechanism and (b) dual stage authentication mechanism.

In (Brumen, 2019), This article presents results of the security analysis of the Game Changer password system. Several games will be graphically displayed on the screen, and users will be able to choose one by first entering the password and playing the game by placing pieces on a board. For instance, the user sets up four chess numbers on the chessboard after selecting a game. The use of the chess game and the character positions serve as representations for the password. The limited search space and amount of password combinations that allow for very easy and cheap brute force attacks are the first problem with the suggested solution. The second problem is that consumers choose particular places and numbers over others. This narrows the search area, making it easier for attackers to launch high-probability strikes quickly. The problem of non-uniformity in places and numbers can be used by attackers to create custom dictionaries and perform dictionary-based attacks. This article explores the flaws and suggests a solution that generates better passwords. But it's important to consider the trade-off between attack flexibility and memorability. However, in this research the system could potentially be improved by the following:

1. Increasing the number of pieces
2. Increasing the number of positions (where possible)
3. Increasing the number of colors of boards (where possible)
4. Increasing the number of colors of pieces
5. Composing the password not only based on locations, but also on moves.

In (Son, Noh, Choi, & Yoon, 2019), This article provides a challenge-response authentication mechanism for a Programmable Logic Control (PLC) system used as a safety system control for the Advanced Power Reactor (APR) 1400 NPP. An underlying protocol that improves the integrity of security authentication is the challenge response authentication approach. Challenge response authentication can be carried out using a variety of techniques. This article simulates and develops the implementation of a one-time password (OTP) authentication method for nuclear control systems. Nuclear power plants (NPPs) have not yet been intended to utilize the most dependable response authentication methods, such as challenge response, in their instrumentation and control (I&C) systems. In this article, the process of developing a challenge response authentication mechanism and integrating it into the POSAFE-Q programmable logic control (PLC) system of the Advanced Power Reactor (APR) 1400 NPP is clarified. Reusing the password could be a potential threat when utilizing the authentication feature. The authentication system cannot distinguish between an attacker typing the password or the real user when frequently used authentication passwords are intercepted. The challenge response authentication mechanism is a way to stop these issues. The technology is a protocol that needs a valid response (response) and a question (challenge) from one party to the other in order to be authenticated. With the OTP approach, a random number is generated by the server from as random numbers are generated and sent to the client, the client uses the value to build an OTP and authenticate itself using the value it receives back. See figure (2).

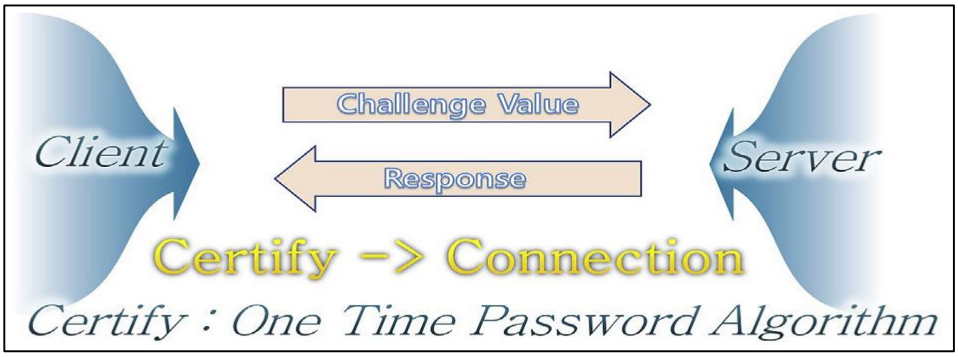


Figure (2) OTP challenge-response.

In (Juneja, 2020), Graphical passwords are currently being evaluated as a more dependable authentication system than text passwords. The purpose of these passwords was to enhance their longevity and memorability. Graphical passwords and image-based authentication mechanisms are implemented in a multitude of applications. However, these authentication methods have a problem managing graphic or pictorial data. When mapping a user-input picture or graphical password across a wider database, the authentication process is slowed down. The graphical image was represented using a schema that was proposed in this research, which was based on XML. The server processes the graphical form and verifies that the password image is a valid pattern by examining the stroke length and skewness when the user submits it. Several transformations are applied to the input graphic style to generate several versions of the graphic style. The collected pixel values from these techniques are stored in an XML-style database. The server employed the LSB steganography technique to modify the least significant bits in the input picture and subsequently presented the password image to the user. Each time the user inputs the password image, the password pattern is retrieved and mapped to the XML pattern database.

The model that is being presented is implemented using a desktop and mobile application. The comparative performance evaluation of the method demonstrates that it surpasses alternative image password setters.

Due to the extraction of all pertinent data from the query password pattern image, password mapping achieves a 100% accuracy. Additionally, the qualitative metrics that have been implemented serve to verify the model's improved dependability and robustness against the backdrop of a variety of factors. An integrated mixed media framework is included to improve the security aspect and accomplish safe authentication. To increase secrecy, the system incorporates server-side procedural changes at the media and pattern levels in addition to user passwords. The secure pattern that is created based on mouse or finger movements is applied to the image, and the input is obtained in the form of a password. To create a safe password, a multi-layer approach is implemented on the server side, including data masking and media transformation. Generating and setting up a strong password is one of the stages of the process, just like with any other authentication system. The newly enrolled user will be subject to the password creation framework. The user provides input in the form of a graphical pattern and password. Drawing a single curve with the least amount of constraint possible forms the basis of the password pattern. A legitimate pattern needs to work within the given constraints of draw time, coverage, and length, etc.

In (Singh & Raj, 2022)suggested utilizing a dynamic password policy and an enhanced hashing algorithm to address the issue of password leaks on well-known websites such as Linked-In, Adobe, Gmail, Yahoo, eHarmony, etc. Depending on the character frequency, an algorithm has been designed to construct password restrictions dynamically. The computation of the time complexity demonstrates how fast the method operates. An attacker will find it challenging to precisely choose the properties of the password database, as the method automatically produces password requirements. See Figures (3-4) that show how the password is stored in the database.

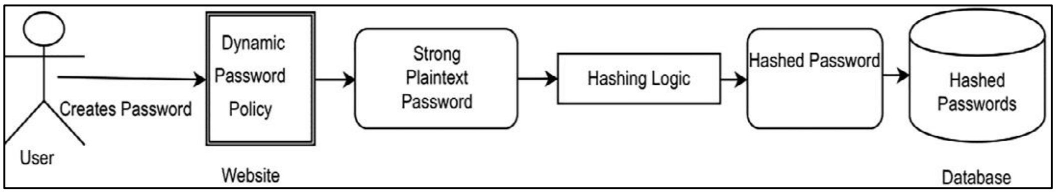


Figure (3) Storing password in the database.

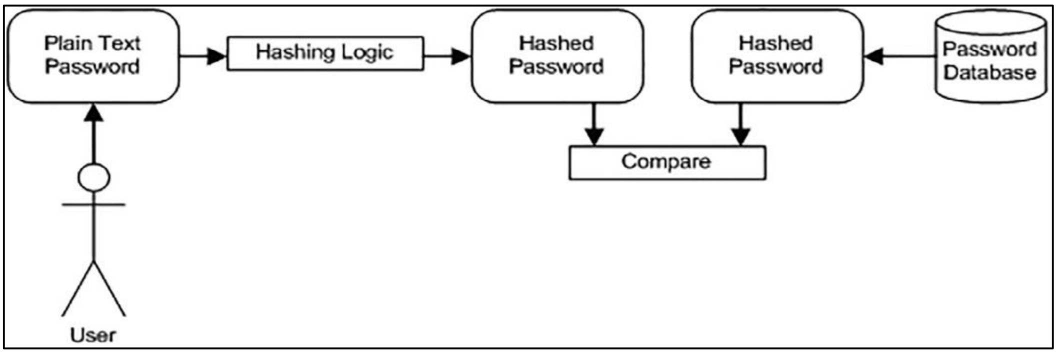


Figure (4) Comparing the hash of input password with the hash of the stored password in the database.

The user initially registers on the website, where they are required to provide a variety of information, including a username, a new password, and a security code. The main emphasis of the article is the password that the user chooses using the dynamic password policy that the algorithm generates. A password policy is a set of rules designed to encourage users to use strong passwords in order to increase security. Because the created password adheres to the dynamic policy, it is robust and complicated. A slow hash function known as a hash algorithm is used to hash a strong plain text password before storing it in a database.

In (Nag, Chandrakar, & Chandrakar, 2023)in this article the suggested scheme is tested using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The findings show that the strategy is impervious to man-in-the-middle and replay assaults, among other active and passive attacks. Better security and increased complexity in terms of communication, computation, and execution time are provided by the suggested protocol.

One of the safest and most efficient tools for patient-doctor contact offered by medical organizations is the Telecare Medical Information System (TMIS). People are generally worried about their well-being and desire to safeguard the confidentiality of their medical information. There are several two-factor authentication systems, typically consisting of a user ID and password. Additionally, there are three-factor authentication systems that incorporate all of the previous elements together with either biometrics or a smart card.

Just as necessary as the security, confidentiality, and integrity of system data is user and server authentication. To ensure that only verified users have access to resources and services, a user permission verification system must be in place.

This article developed a mechanism whereby users register to the server with their user ID and password for the Telecare medical information system. After gathering the credentials, the server provides the user with a smart card. The system does some math to determine whether a user is already enrolled when they input their smart card and credentials. The user may make use of the medical organization's services if granted permission. Since everything on the Internet is vulnerable to hacking, it is crucial for everyone to protect their personal information. A user's remote access to data, resources, and other services inside the healthcare system depends in large part on authentication.

suggested procedure, the user sends the medical server a registration request at the beginning, along with their user ID and password. The registration request will be denied if the matching user ID is already on file; if not, the user will receive one smart card. To use a number of features and services, the user needs to log in to the system. The user must use his smart card to reenter the user ID and password in order to access the system. In the event that the system's calculations are successful, the medical server provides the user with a session key for upcoming communications. After authenticating, the user can communicate with doctors using the shared session key. Thus, the patient can electronically submit his diagnosis and test results, and the doctor can look at the data, respond to the patient's inquiries, and write the prescription.

In (Khan, Din, & Almogren, 2023) This article suggests a new graphical authentication system that uses easy math operations, machine learning to recognize hand movements, and medical pictures for recall as well as other factors to register and identify users. The suggested approach aims to maintain a straightforward, robust, and memorable authentication procedure. A Post-Study System Usability Questionnaire (PSSUQ) is utilized to assess the suggested scheme by contrasting it with authentication methods based on patterns and PINs.

System quality showed a 16.7% improvement, information quality showed a 25% rise, interface quality showed a 40% increase, and overall quality indicated a 25% increase when comparing the treatment and comparison groups. The suggested approach effectively revives the usage of graphical passwords, particularly in the Internet of Things (IoMT) space, by creating a robust, satisfying, and easy-to-use authentication system.

The two primary subtasks of the proposed system will be authenticating an existing user and enrolling a new user. The suggested system will look for a user record when it boots up. The registration phase will commence with sub-phases if the record is absent, indicating that the user has not yet registered. Choosing secret details like a secret number, color, and click mode (double or single) is part of the first sub-stage.

The click positions will represent addition or subtraction operations, which will be used later in the login phase. After the user has successfully adjusted these settings, the device will enter the second sub-phase, which consists of handwriting tasks utilizing hand motions on the touch screen. The user will be requested to sketch various numbers multiple times, and the system will record and save each motion that corresponds to a certain number.

After completing a certain number of handwriting assignments, the user will be shown a randomly generated grid of images (5*4) that comprises pictures of various medical images, including MRIs, CT scans, and X-rays, etc.

It'll show up in the user interface. Given that medical professionals such as doctors and nurses are the system's intended users, these images will not only be pertinent, but also elicit some sort of emotional response related to their individual experiences. All of the user's secret data is encrypted and saved in the Firebase database when the user chooses three secret photos.

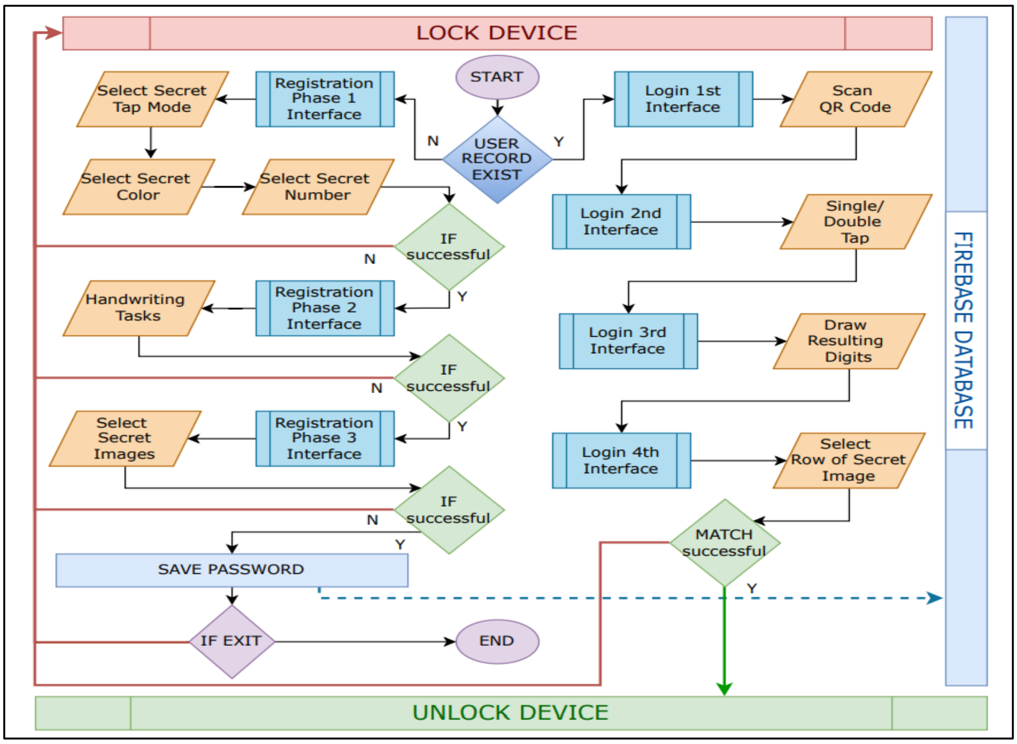


Figure (5) Flow diagram of the proposed architecture

In (Sadat, Lodin, & Ahmadzai, 2023)In this article, it is suggested to utilize a password-generating system that creates passwords depending on information entered by the user, such as location and time. The method comes up with passwords that are very strong, easy to remember, and can't be broken by dictionary or brute force attacks. The three-internet password-checking tools that were used to confirm the generated passwords showed that the method creates very strong passwords that are hard to crack. PHP is used to make the system work in an easy-to-use setting.

In the approach, the user provides their name, the name of a chosen city, and a certain time, which can be either the moment of password creation or any other preferred time. The initial two digits of the latitude and longitude data are utilized by the system to generate the password when the user selects a city. The concatenation of (Name + Latitude + Longitude + Time) will provide a password for the user that is highly secure, easy to remember, and uncomplicated to retrieve.

To retrieve a forgotten password, the user now only requires remembering the place (city name) and the time. The user can get the previous password that the system produced by entering their name, city, and time. After a while, users will want to rename the city to prevent hackers from learning the name of the city. Hackers will have a harder difficulty finding out the password if city and time data are combined with the username.

After the produced passwords were checked using three different online password checking tools, the results showed that the algorithm produces highly confidential passwords that are difficult to crack and take millennia to hack. Features of the proposed system: ease of remembering passwords, dealing with unconfirmed inputs, user safety, and resistance to attacks.

In (Gutub, 2024) A protection tool called count-based secret sharing (CBSS) is already out there and can be used to authenticate people who want to use collaborative trust access control. CBSS originally sets its master secret target key as an automatically selected secret random key to create private shares for all participants that fulfill the trap door function. Usually, CBSS does not provide user preferences when creating passwords to be entertained, which makes memory of recall somewhat challenging. This work solved this personal retention issue by optimizing a CBSS technique starting with the user's password choice, as is the case for extracting secret shares to produce the target key, therefore securing the cooperative cybersecurity system. Several algorithms were proposed to incorporate secret sharing of user preferences based on text and image alternatives, which were further verified by convenient authentication via personal email. Therefore, in order to increase the accountability of the IT process, it is necessary to divide the scheme into phases and ensure that more than one person is protecting the data in order for confidential sharing to be reliable, as shown in figure (6).

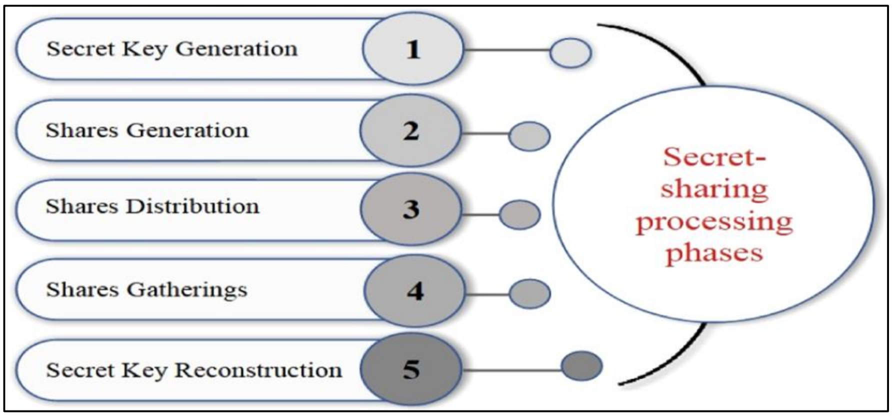


Figure (6) Processing phases of secret-sharing scheme.

The first stage in creating a target key (TK) is for the secret keeper or trader (dealer) to select an algorithmic randomization approach to establish the threshold (k). The target key is thus split into (n) shares controlled by (k <= n). Finally, the trader will allocate the (n) shares to each attendee. Nevertheless, it is anticipated that the recovery of this target key will be challenging as long as the contributions are not collected, as the number of contributions exceeds or equals the threshold

number k. In particular, the threshold (k) is the minimal number of target key shares that must be reconstructed.

The fundamental drawback of secret sharing systems is that the system determines individual passwords, therefore limiting users of flexibility of choice and resulting in great inconvenience for participants and/or password memory problems.

This article improves CBSS to swap steps one and two of fig. (6), enabling users to fully customize their password shares with intelligence and including email authentication to offer personal verification to the user following two-factor authentication. The traditional CBSS process is divided into five stages shown in fig. (6), Presuming the system executes the process of producing the confidential key, it proceeds to produce the shares. The article proposed the implementation of two-factor authentication (2FA) as a dependable and expeditious method to verify the integrity of crucial passwords and validate the identification of participants. The research presented five novel strategies for users to choose and remember their passwords while maintaining ambiguity to prevent attackers from guessing them. Participants select one of five techniques to generate the secret key that verifies identification using two-factor authentication (2FA) with a verification code obtained via personal email. Subsequently, in accordance with the user's request, the system enables participants to submit their own passwords, which are permitted to be in the form of images, thereby facilitating easier remembering.

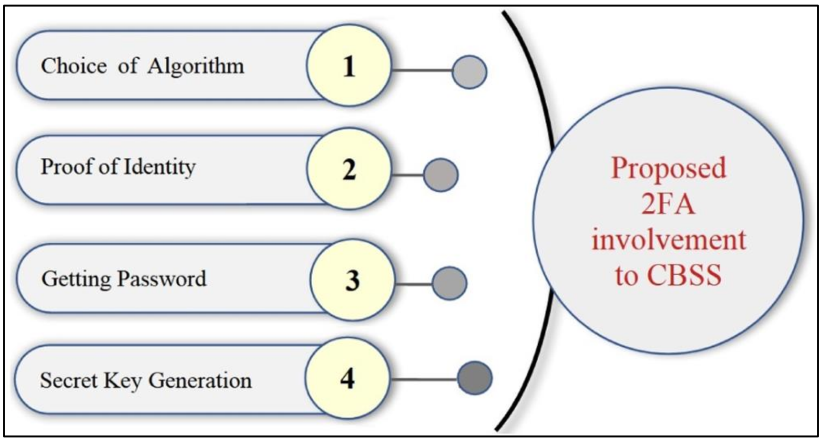


Figure (7) Proposed 2FA involvement in shares generation of CBSS.

It is clear from previous studies that password strength is directly related to user security, so there are different ways to make the password stronger and most complex to avoid hacking. And the strength of password is depended on the importance of the organization and the data that need to be secure. For more illustration of previous studies see Table-1.

Table 1: Previous Studies using Password User Authentication

No.	year	Title	attack	strategy
1	2018	Two-factor authentication with end-to-end password security	Dictionary attack	Use Two Factor Authenticated Key Exchange (TFA-KE) & SAS-MA (Short-Authentication-String Message Authentication)
2	2018	Secure server-server communication for dual stage biometrics–based password authentication scheme	collision attack	Using new scheme include two servers, Master Server (MS) and the Authentication Server (AS)connected to each other with Registration Center (RC)
3	2019	Security analysis of game changer password system	Brute force attack & dictionary attack	Use layering system &change in game designer as possible
4	2019	A practical challenge-response authentication mechanism for a Programmable Logic Controller control system with one-time password in nuclear power plants	Stuxnet attack	Use challenge response authentication
5	2020	An XML transformed method to improve effectiveness of graphical password authentication	Social engineering attack	Using XML pattern with LSB steganography

6	**2022**	Securing password using dynamic password policy generator algorithm	Brute force attack, rainbow table attack, dictionary attack, phishing attack & social engineering attack	Using hash function & dynamic password generation
7	**2023**	An Improved Two-Factor Authentication Scheme for Healthcare System	Man in the middle attacks	using user ID and password and Server gives the user a smart card
8	**2023**	Securing Access to Internet of Medical Things Using a Graphical-Password-Based User Authentication Scheme	Keylogger attack & Credential stuffing & Traffic interception & Password spraying	novel graphical authentication scheme that uses multiple factors to register and authenticate users using simple arithmetic operations, machine learning for hand gesture recognition, and medical images for recall purposes.
9	**2023**	Highly Secure and Easy to Remember Password-Based Authentication Approach	Dictionary and Brute force attacks	generates a password based on the user's input like, time and location data
10	**2024**	Adjusting counting-based secret-sharing via personalized passwords and email-authentic reliability	Third party attack	Using one of the five algorithms to generate the secret key proving identity via 2FA via verification code received by personal email

3. Conclusion:

When communicating across a network, authentication is always crucial. The first line of defense against an intrusive or unknown user accessing the system and services is authentication. Passwords are typically used by websites to verify a user's identity and grant access to resources that hold private data. Because most users don't choose extremely strong passwords, there is a risk that their information will be compromised. The main objective of previous research listed in the above section is to ensure the user authentication and confidentiality. The password policy needs to be more resistant to many types of attacks, like dictionary attacks, rainbow table attacks, brute-force attacks, etc. In addition, as a result of previous researches attempted to establish a secure environment for user authentication by using passwords and multifactor methods and dynamic password policies to mitigate vulnerabilities inherent in traditional password systems. The ultimate goal is to establish robust, user-friendly, and attack-resistant authentication frameworks.

References:

[1] Abrahami, Y., Bloch, K., & Achsaf, N. (2023). System and method for third party application activity data collection. Washington: U.S. Patent.

[2] Abu Hweidi, R., & Eleyan, D. (2023). Social engineering attack concepts, frameworks, and awareness: a systematic literature review. International Journal of Computing and Digital Systems, 13(1), 691-700.

[3] Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future internet, 12(10), 168.

[4] Alkhwaja, I., Albugami, M., Alkhwaja, A., Alghamdi, M., Abahussain, H., Alfawaz, F., & Min-Allah, N. (2023). Password cracking with brute force algorithm and dictionary attack using parallel programming. Applied Sciences, 13(10), 5979.

[5] Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., & Rieck, K. (2022). Dos and don'ts of machine learning in computer security. USENIX Security 22. Boston.

[6] Ba, M., Bennett, J., Gallagher, M., & Bhunia, S. (2021). A case study of credential stuffing attack: Canva data breach. International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas.

[7] Bahaa Qasim M. AL-Musawi. (2024). PREVENTING BRUTE FORCE ATTACK THROUGH THE ANALYZING LOG. Iraqi Journal of Science, 53(3), 663–667.

[8] Birge-Lee, H., Wang, L., Rexford, J., & Mittal, P. (2019). Sico: Surgical interception attacks by manipulating bgp communities. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.

[9] Boopathi, M., & Aramudhan, M. (2018). Secure server-server communication for dual stage biometrics–based password authentication scheme. Alexandria Engineering Journal, 57(2), 819-829.

[10] Briceno, M., Wilson, B., Kesanupalli, R., Baghdasaryan, D., Dholakia, R., Blanke, W., & Umap, A. (2019). Advanced authentication techniques and applications. Washington: U.S. Patent and Trademark Office.

[11] Brumen, B. (2019). Security analysis of game changer password system. International Journal of Human-Computer Studies, 126, 44-52.

[12] Çetinkaya, Ş., & Terzi, S. (2024). Analysing The Effects of Cyber Security on National Security. Güvenlik Çalışmaları Dergisi, 26(1), 38-51.

[13] Crume, J. (2022). Detection of and defense against password spraying attacks. Washington: U.S. Patent and Trademark Office.

[14] Gutub, A. (2024). Adjusting counting-based secret-sharing via personalized passwords and email-authentic reliability. Journal of Engineering Research, 12(1), 107-121.

[15] Hendi, A., Dwairi, M., Al-Qadi, Z., & Soliman, M. (2019). A novel simple and highly secure method for data encryption-decryption. International Journal of Communication Networks and Information Security, 11(1), 232-238.

[16] Jarecki, S., Krawczyk, H., Shirvanian, M., & Saxena, N. (2018). Two-factor authentication with end-to-end password security. International Conference on Practice and Theory of Public-Key Cryptography. Rio de Janeiro.

[17] Juneja, K. (2020). An XML transformed method to improve effectiveness of graphical password authentication. Journal of King Saud University-Computer and Information Sciences, 32(1), 11-23.

[18] Khan, M. A., Din, I. U., & Almogren, A. (2023). Securing access to internet of medical things using a graphical-password-based user authentication scheme. Sustainability, 15(6), 5207.

[19] Mahmood, A., & Hameed, S. (2023). A Smishing Detection Method Based on SMS Contents Analysis and URL Inspection Using Google Engine and VirusTotal. Iraqi Journal of Science, 64(10), 6276-6291.

[20] Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109-134.

[21] Marqas, R., Almufti, S., & Ihsan, R. (2020). Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. Journal of Xi'an University of Architecture & Technology, 12(3), 3110-3116.

[22] Mexriddinovich, A. Z. (2023). SAFEGUARDING DIGITAL SECURITY: ADDRESSING QUANTUM COMPUTING THREATS. The Role of Exact Sciences in the Era of Modern Development, 1(4), 1-7.

[23] Nag, P., Chandrakar, P., & Chandrakar, K. (2023). An Improved Two-Factor Authentication Scheme for Healthcare System. Procedia Computer Science, 218, 1079-1090.

[24] OA, M., & AS, B. (2023). SIMULATION OF THE RAINBOW ATTACK ON THE SHA-256 HASH FUNCTION. Journal of Theoretical and Applied Information Technology, 101(4).

[25] Qadir, A., & Varol, N. (2019). A review paper on cryptography. 7th international symposium on digital forensics and security. Barcelos.

[26] Qu, J. (2022). Research on password detection technology of iot equipment based on wide area network. ICT Express, 8(2), 213-219.

[27] Reem Ismail. (2024). A Secure Session Management Based on Threat Modeling. Iraqi Journal of Science, 54(4), 1176–1182.

[28] S.A, A., & N.H.M, A. (2024). Lightweight Block and Stream Cipher Algorithm: A Review. Journal of Applied Engineering and Technological Science (JAETS), 5(2), 860–874.

[29] Sadat, S. E., Lodin, H., & Ahmadzai, N. (2023). Highly secure and easy to remember password-based authentication approach. Journal for Research in Applied Sciences and Biotechnology, 2(1), 134-141.

[30] Saqib, M., Jasra, B., & Moon, A. (2022). A lightweight three factor authentication framework for IoT based critical applications. Journal of King Saud University-Computer and Information Sciences, 34(9), 6925-6937.

[31] Shah, S., & Kanhere, S. (2019). Recent trends in user authentication–a survey. IEEE access, 7, 112505-112519.

[32] Singh, A., & Raj, S. (2022). Securing password using dynamic password policy generator algorithm. Journal of King Saud University-Computer and Information Sciences, 34(4), 1357-1361.

[33] Son, J., Noh, S., Choi, J., & Yoon, H. (2019). A practical challenge-response authentication mechanism for a Programmable Logic Controller control system with one-time password in nuclear power plants. Nuclear Engineering and Technology, 51(7), 1791-1798.

[34] Wajahat, A., Imran, A., Latif, J., Nazir, A., & Bilal, A. (2019). A novel approach of unprivileged keylogger detection. International Conference on Computing, Mathematics and Engineering Technologies. Sukkur.

Article Review: Efficient Randomness Methods for Key Generation

Ali A. Mahdi [1]

Mays M. Hoobi [2]

Abstract

In today's tech-savvy world, it's super important to keep our digital conversations private and safe. That's where the magic of secure key generation comes in, especially in realm of encryption. Typically, crypto systems are all about strong key creation practices. But hey, there's a new player in town: chaotic maps. These bad boys thrive on unpredictability, which is perfect for cooking up secure keys.

This research dives deep into how using chaotic maps for key generation could seriously up the game for encryption security. We're talking a deep dive into the chaos theory and its buddy, cryptography. Main dish here is a thorough look at what's been written about using these wild, unpredictable maps to make keys. It highlights the freshest strategies and smarty-pants theories that help these methods tick, all aimed at crafting top-notch, secure solutions.

The goal, to ramp up encryption security. Plus, it really underlines how crucial chaotic maps are in churning out tough cryptographic keys. This work is stepping up to meet the demand for stronger, smarter key generation as we all dive deeper into our digital lives.

Keywords: *True Random Number Generator (TRNG), Pseudorandom Number Generator (PRNG), Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs), National Institute of Standards and Technology (NIST).*

http://dx.doi.org/10.47832/RimarCongress03-3

[1] College of Science, University of Baghdad, Baghdad, Iraq ali.abdulameer1201a@sc.uobaghdad.edu.iq

[2] College of Science, University of Baghdad, Baghdad, Iraq mays.m@sc.uobaghdad.edu.iq

1. Introduction

In this digital era, where everything from coffee makers to corporate data is connected, keeping unauthorized snoops out is more crucial than ever. Enter robust encryption methodologies—true game-changers boosting data security. A cornerstone of this security fortress is encryption key generation[1]. y harnessing solid cryptographic methods, we can shield data zipping across networks, safeguarding both secrecy and authenticity of digital chats and transactions.

The cyber threat landscape is a beast constantly evolving, always coming up with new ways to attack. That's why ongoing advancements in key generation are so vita [2]. At the heart of cryptographic systems, key generation creates keys that are secure and unpredictable—key to locking down sensitive data. These innovative techniques are our best bet against digital marauders and cyber threats [3]. Traditionally, keys needed to be random, and randomness was conjured up by Pseudo-random Number Generators (PRNGs). These depend on mathematical formulas to drum up semblances of randomness. Cryptographic operations need this unpredictability—not just for creating encryption keys but also for generating initialization vectors and nonce values that enhance encryption processes; Though PRNGs have been the go-to, they aren't foolproof. They've got their vulnerabilities, which can be like leaving your digital door slightly ajar. That's where Cryptographically Secure Pseudo Random Number Generators (CSPRNGs) step in[4]. These help in improving the security of the system by generating sequences that are unique, unexpected cryptanalysis-resistant.

Chaos theory and chaotic map both appear to be promising [5]. Characteristics of chaotic maps, which include their unpredictability and sensitivity to initial circumstances, align well with the aim of protecting data and increasing security. Strong cryptographic keys use conventionally used chaotic map techniques like Logistic Map, Baker's Map, Lorenz System, Henon Map, and Chen Map in the field of cryptography. All of these provide a foundation for applying chaos theory to the world of cryptography [6]. This review deals with the incorporation of conventional and hyper-chaotic map techniques for key generation in cryptography, along with its ability to surpass the cyber constraints of PRNGs and CSPRNGs. The subject includes a number of important analytical techniques used to judge how well chaotic map-based key creation works. The methods mentioned, such as statistical analysis as well as modeling of cryptographic analysis, allow valuable information about the cryptographic power of the produced keys, thus ensuring the greatest security standards [7].

Importance as digital systems grow more complex, the potential for cyberattacks increases. To respond, this research explores chaotic maps as a way to generate cryptographic keys with greater randomness and security. By improving key generation methods, the study aims to help strengthen digital defenses, ensuring that our sensitive information stays safe in an ever-evolving online world[8].

2. True Random Number Generators

A true random number generator (TRNG) uses an unpredictable source to generate randomness. They are capable of producing numbers without the use of algorithms because they make random numbers out of naturally unpredictable physical events.. Predictable random number generators (RNGs) provide vulnerabilities that may be exploited to breach devices and compromise data. In order to be efficient, random numbers must possess the qualities of being unexpected and statistically independent, meaning they are not influenced by any previously created random numbers. Also, they ensure that there is no need for an initial seed value to identify the sequence of numbers [9].

Mathematically, it can be represented as:

$R = f\,(\textit{physical event})$

where R is the random output.

3. Pseudo-Random Number Generators

A pseudorandom number generator (PRNG) is a mathematical algorithm that generates a predictable, repeating series of integers based on an initial value known as the seed. These generators cannot be shown to be really random. PRNGs exhibit ideal equilibrium between 0's and 1's without any bias, but they also possess significant long-range correlations that weaken cryptographic security and might manifest as unforeseen mistakes in Monte Carlo computations and modeling. It provides the sequence with the illusion of randomness solely until the seed and algorithm are disclosed [10]. Distinct features of PRNGs include generating numbers with minimal computational sources and dependency on seed-based generation [11], [12].

It can be mathematically expressed as

$$X_{n+1} = f(X_n)$$

Where f is the deterministic function.

4. Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs)

CSPRNGs use advanced algorithms to generate keys that are highly indistinguishable from genuine randomness with the concept of secrecy and unpredictability [13]. It means that you cannot predict the next number by liking any element in the series, nor can you use any part of the generated sequence to guess past or future numbers. They require only a few computational resources despite their high efficiency and may produce keys rapidly. This is based on the initial introduction of a high-entropy seed that injects the entropy into the system [14]. Thus, CSPRNGs make it impossible to predict the future output, fulfilling the fundamental goal of security and safety [15]. In mathematical terms, it looks like:

$$Unpredictability\colon\ H(X_{n+1} \mid X_n, X_{n-1}, \dots, X_1) \approx H(X_{n+1})$$

$$Forward\ Secrecy\colon H(X_1, X_2, \dots, X_{n-1} \mid X_n) \approx H(X_1, X_2, \dots, X_{n-1})$$

Where H denotes the entropy, representing the uncertainty or randomness within the sequence X, and n is the position in the sequence.

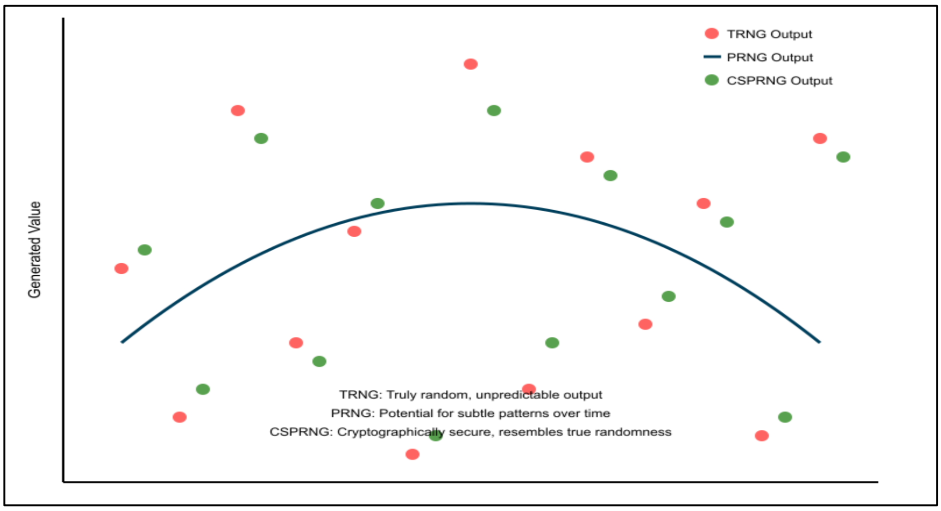


Figure 1: Comparison of CSPRNG, PRNG, and TRNG Output Patterns

5. Chaos: Unraveling Complexity in the Natural and Digital Worlds

Chaos theory is the mathematical and mechanical study of ostensibly unpredictable or arbitrary behavior in systems governed by deterministic laws [16]. According to the chaos theory, even the slightest variance in the initial conditions can produce significantly highly diverse results. Chaos theory offers a valuable theoretical framework for comprehending the dynamic growth of industries and the intricate interconnections among industry participants.

Industries may be seen and represented as intricate, ever-changing systems that display both unpredictability and a hidden structure [17]. The word "deterministic chaos" is more precise since it combines two concepts that are generally seen as incompatible, resulting in a contradiction. The first characteristic is that of randomness or unpredictability. The second concept pertains to the phenomenon of deterministic motion [18]. Chaotic systems provide the groundwork for the development of encryption techniques in the field of cryptography, which use the innate complexity and unpredictable nature of chaos to improve security. Initially, the Lorenz System and the Logistic Map were the focused applications of chaos systems in cryptography despite them being simple [4]. For achieving the highest level of security, cryptography is now looking forward to hyperchaotic systems because their operations are even more complex, featuring more than one positive Lyapunov exponent. They provide an extra layer of security because of the higher-dimensional behavior of hyperchaotic systems such as Coupled Map Lattices or Pricewise Linear Chaotic Maps [19], [20]. Cryptographic assessment of chaotic systems demands advanced analytic techniques. These tools check produced sequences' complexity and unpredictability to meet cryptographic application requirements. Chaotic map-generated sequences are often tested for randomness and unpredictability using statistical test suites such as the NIST Special Publication 800-22 [21]. This evaluates the sequences for cryptographic key creation.

6. Traditional Methods in Chaotic Map

these maps provide complex dynamic behavior from simple non-linear mathematical models. They showcase a combination of both unpredictability and chaos [22], [23]. There are several types of chaotic maps.

a. Logistic Map.

These maps show how complexity can come from simplicity. Their dynamic behavior is a cornerstone in the study of chaos theory applications. The following equation represents the logistic map:

$$x_{n+1} = rx_n(1 - x_n)$$

where the population at generation *n*, and *r* is a parameter controlling the system's rate of reproduction[24].

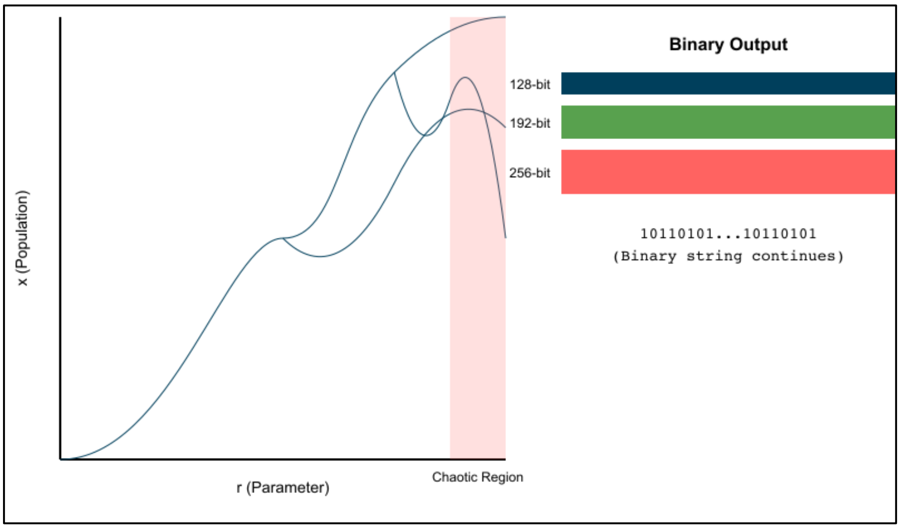


Figure 2: Logistic Map for Generating Binary Numbers

b. Hénon Map

It is a two-dimensional discrete-time dynamical system. It has the dinstict feature of creating complicated patterns despite of it being simple. it is a tool of interest for researchers due to the non-linear dynamics and complexity enabling to generate keys providing a secure system [21], [25]. Hénon Map is described by following set of equations:

$$x_{n+1} = 1 - ax_n^2 + y_n$$
$$y_{n+1} = bx_n$$

where a and b are parameters that dictate the behavior of the map, with typical values being a=1.4 and b=0.3 to ensure chaotic behavior.

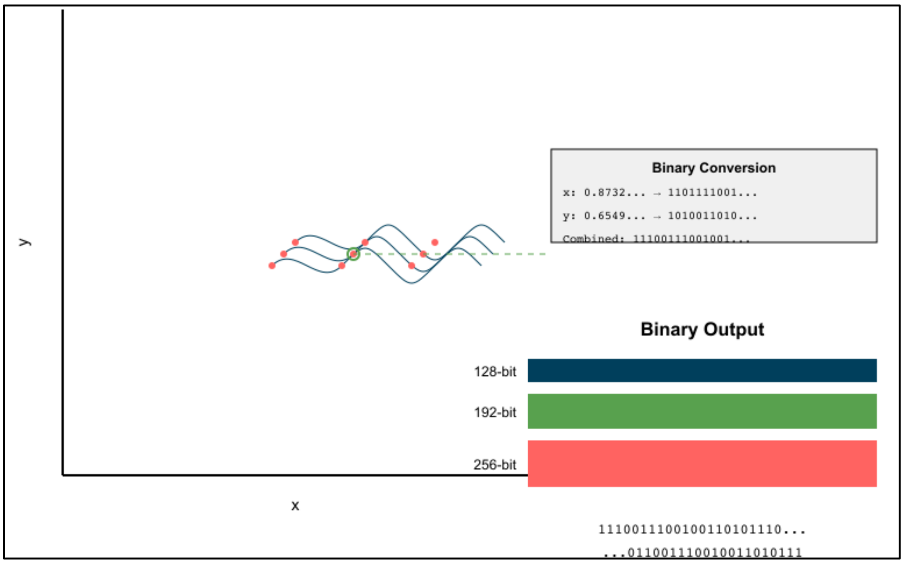


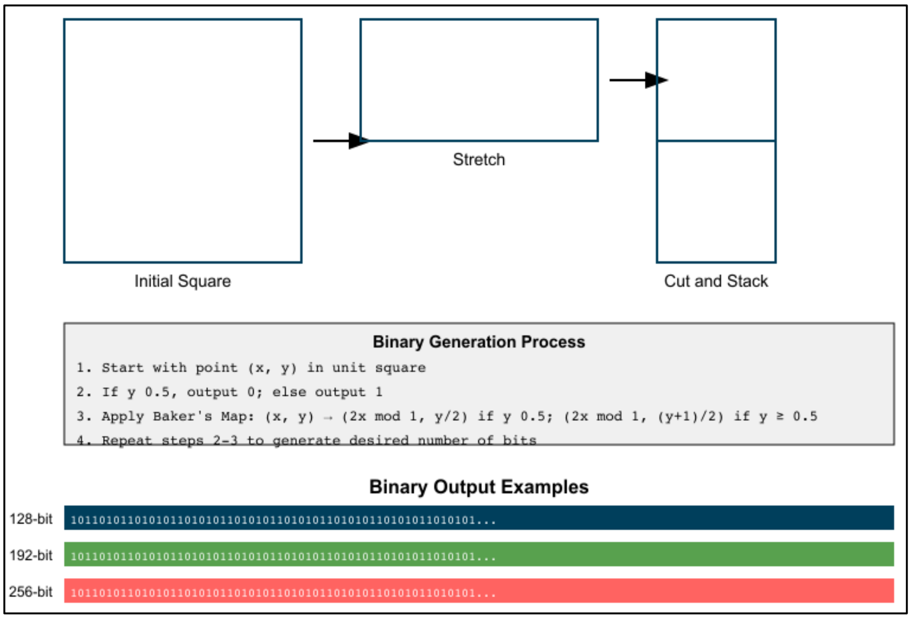
Figure 3: Hénon Map for Generating Binary Numbers

c. Baker's Map

In the field of dynamical systems analysis, baker's map exhibits chaotic behavior. It operates on the unit square and maps points inside the square back onto itself. The name of this process is derived from a technique used by bakers to manipulate dough. In this technique, the dough is divided into two halves, which are then placed on top of each other and firmly pushed together. Baker's map works on the basis of unpredictability and mixing in communication systems thus producing secured results [26], [27]. Mathematically Baker's map is described by the following equation and follows linear transformation such as:

$$(x', y') = \begin{cases} \left(2x, \dfrac{y}{2}\right) & \text{if } 0 \leq x < \dfrac{1}{2} \\ \left(2x - 1, \dfrac{y+1}{2}\right) & \text{if } \dfrac{1}{2} \leq x \leq 1 \end{cases}$$

Where x checks if x is less than 0.5, where true, the point is considered to be in the left half of the square, else x equal or more than 0.5 point is in the right half.



Binary Generation Process

```
1. Start with point (x, y) in unit square
2. If y 0.5, output 0; else output 1
3. Apply Baker's Map: (x, y) → (2x mod 1, y/2) if y 0.5; (2x mod 1, (y+1)/2) if y ≥ 0.5
4. Repeat steps 2-3 to generate desired number of bits
```

Binary Output Examples

```
128-bit 101101011010101101010110101011010101101010110101011010101...
192-bit 101101011010101101010110101011010101101010110101011010101...
256-bit 101101011010101101010110101011010101101010110101011010101...
```

Figure 4: Baker's Map for Generating Binary Numbers

d. Lorenz System

Lorenz System is based on three different equations called differential equations. On if the feature of Lorenz system is that a small change can drastically change the outcomes. It is widely used in meteorology, mathematics and chaos theory. It displays deterministic, non-periodic series [22], [28].

The Lorenz System equations are as follows:

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = x(\rho - z) - y$$
$$\frac{dz}{dt} = xy - \beta z$$

where σ, ρ, and β are parameters related to the physical properties of the system, with common values being σ =10, ρ =28, and β=$\frac{8}{3}$ for the chaotic regime.

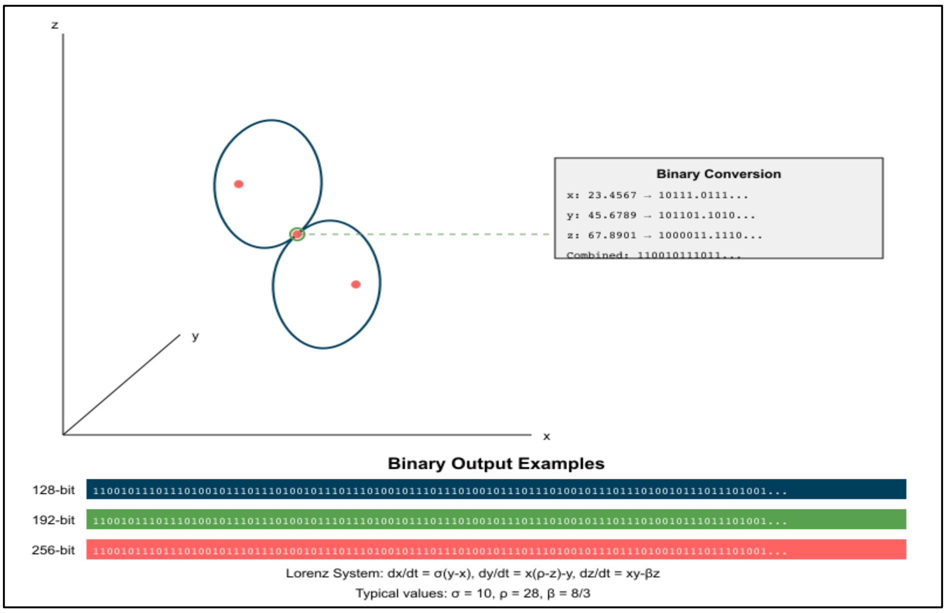


Figure 5: Lorenz system Binary Number Generator

e. Chen Map

Chen Map is similar to Lorenz system with some distinct features. Guarong Chen introduced it in 1990s and known for its chaotic and hyperchaotic characteristics. its application includes communication systems and encrypted data[29], [30]. The equations for the Chen System are:

$$\frac{dx}{dt} = a(y - x)$$
$$\frac{dy}{dt} = (c - a)x - xz + cy$$
$$\frac{dz}{dt} = xy - bz$$

where *a*, *b*, and *c* are system parameters that determine the behavior of the system, with common values being *a*=35, *b*=3, and *c*=28 to ensure chaotic dynamics.

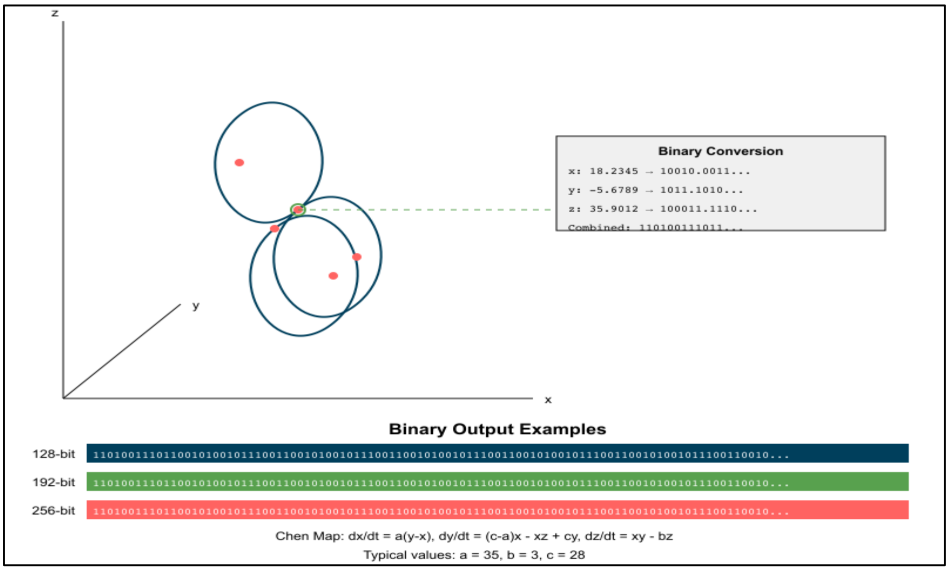


Figure 6: Chen Map Binary Number Generator

f. Tent Map

It is named after its graph that looks like tent-shaped when plotted. The highlights of tent map are simple, linear and 1-D map having chaotic characteristics. It is used in the understanding of bifurcation and high sensitivity to initial conditions along with the illustration of the concepts of chaos theory [22], [31].

The equation for the Tent Map is given by:

$$\begin{cases} 2x_n & \text{if } 0 \le x_n < \dfrac{1}{2} \\ 2(1-x_n) & \text{if } \dfrac{1}{2} \le x_n \le 1 \end{cases}$$

This function doubles the value of *xn* for inputs in the first half of the interval and doubles the distance of *xn* from 1 for inputs in the second half, thereby creating a "tent" shape.

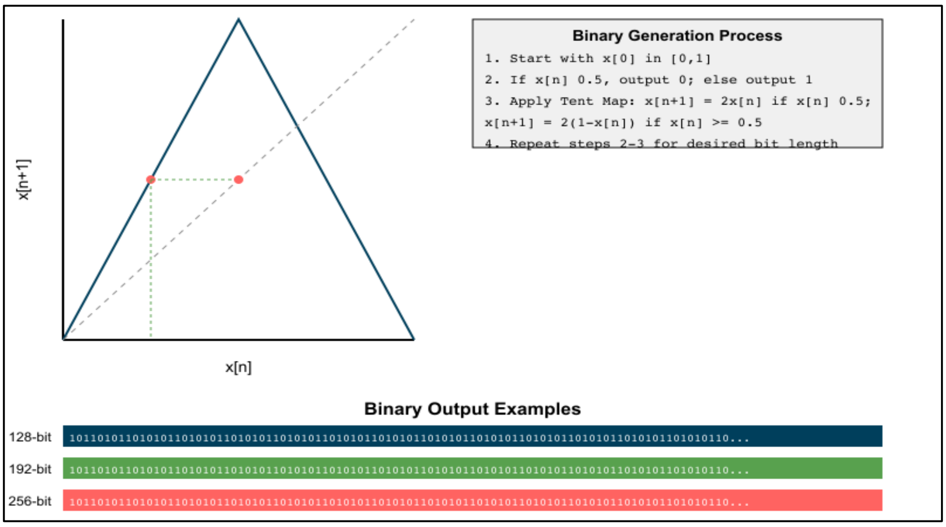


Figure 7: Tent Map for Generating Binary Numbers

g. Sine Map

It is used in generating bifurcation diagrams and helps in studying the transition to chaos from simpler. It uses a sine function over unit interval to exhibits non linearity in the chaotic system. [22], [32].

The equation for the Sine map is:

$$x_{n+1} = r\sin(\pi x_n)$$

Where *xn* is the state at iteration *n*, *r* is a parameter controlling the system's behavior, and the sine function modulates the input, producing a non-linear feedback loop that can result in chaotic behavior for certain values of *r*.

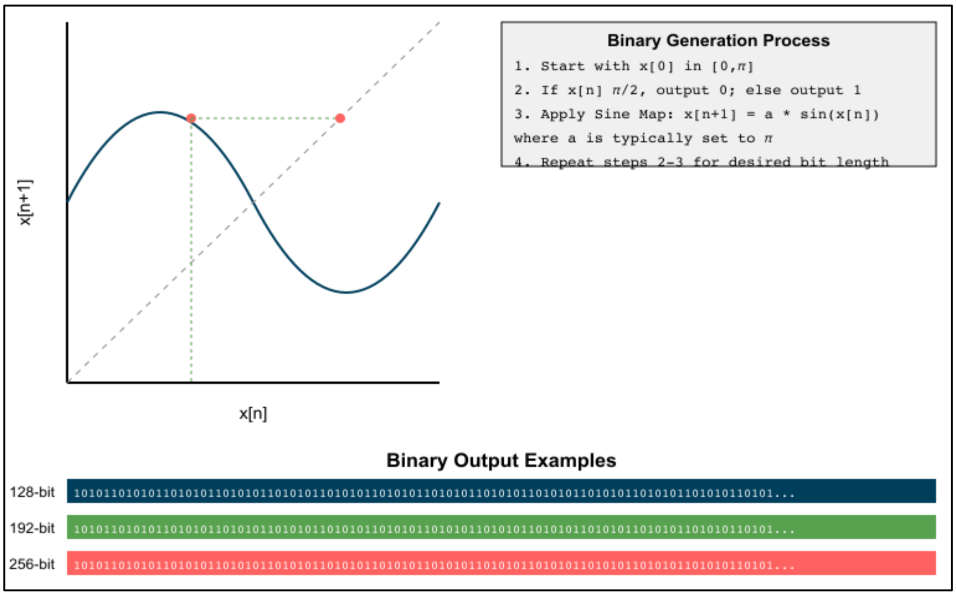


Figure 8: Sine Map for Generating Binary Numbers

h. Ikeda Map

The Ikeda map is used in the modeling of optical recording media, specifically crystals. Previous numerical results have demonstrated that the Ikeda map displays highly intricate dynamical behavior under specific parameter values. This behavior is characteristic of chaotic systems, which are highly sensitive to initial conditions [23], [33].

The equation for the Ikeda Map is:

$$\begin{aligned} x_{n+1} &= A + B(x_n\cos t_n - y_n\sin t_n) \\ y_{n+1} &= B(x_n\sin t_n + y_n\cos t_n) \\ t_n &= T - \frac{\kappa}{1 + x_n^2 + y_n^2} \end{aligned}$$

Where A, B, T, and κ are parameters of the system, with A and B affecting the scaling and T, κ influencing the phase shift.

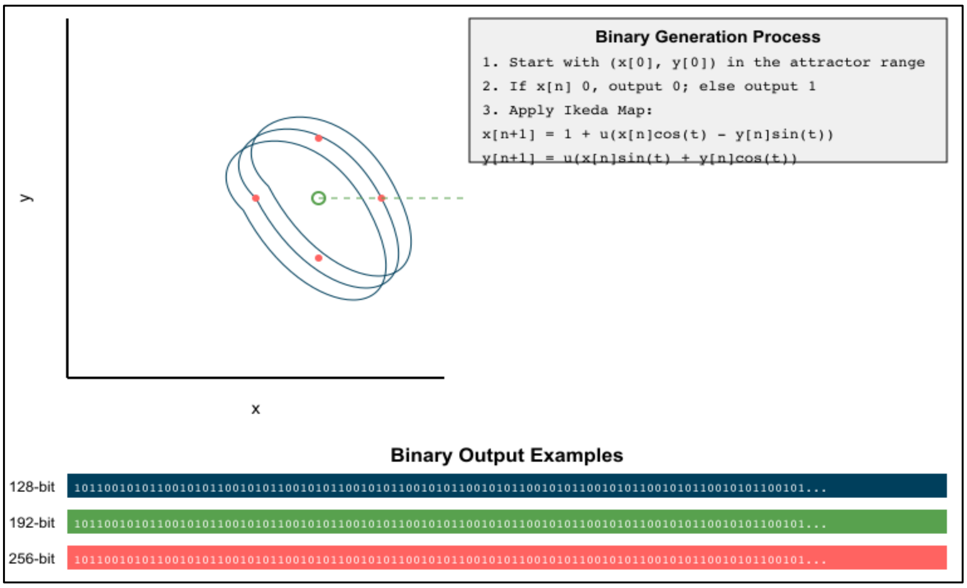


Figure 9: Ikeda Map for Generating Binary Numbers

i. Chirikov Standard Map

The standard map, also known as Chirikov Standard Map is a precise representation of several physical systems, either exact or approximate. It models the example of a kicked rotor. The Chirikov standard map is a map that preserves the area for two canonical kinematic variables, namely momentum and coordinate. The map was first suggested by Bryan Taylor and subsequently discovered independently by Boris Chirikov as a means to explain the dynamics of magnetic field lines. The standard map and H´enon's area-preserving quadratic map are well researched examples of chaotic Hamiltonian dynamics [34], [35].

The equation for the Chirikov Standard Map is:

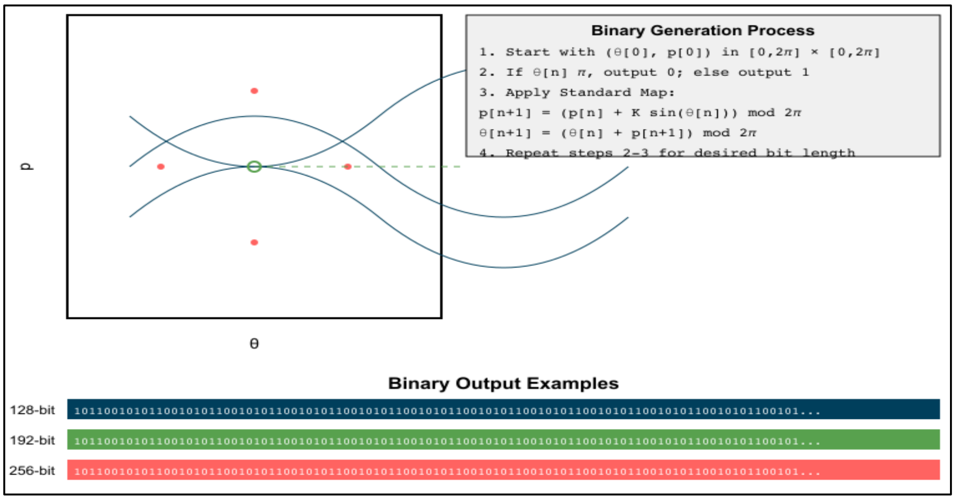
$$p_{n+1} = p_n + K\sin(\theta_n)(mod2\pi)$$
$$\theta_{n+1} = \theta_n + p_{n+1}(mod2\pi)$$

where

θn = Angle

pn =Angular momentum at iteration n

K = Parameter that controls the strength of the perturbation



Binary Generation Process

```
1. Start with (θ[0], p[0]) in [0,2π] × [0,2π]
2. If θ[n] π, output 0; else output 1
3. Apply Standard Map:
p[n+1] = (p[n] + K sin(θ[n])) mod 2π
θ[n+1] = (θ[n] + p[n+1]) mod 2π
4. Repeat steps 2-3 for desired bit length
```

Binary Output Examples

```
128-bit 101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101...
192-bit 101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101...
256-bit 101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101...
```

Figure 10: Chirikov Standard Map for Generating Binary Numbers

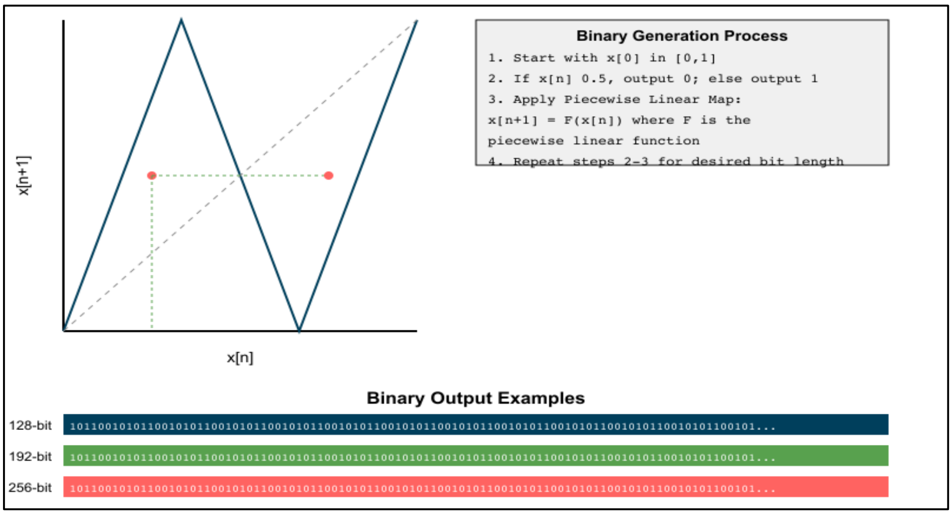
j. Piecewise Linear Chaotic Maps

Piecewise Linear Chaotic Maps (PWLCM) are the simplest among the chaotic maps. it is a straightforward chaotic system often used for the generation of pseudorandom numbers (PRN). The finite precision effect in the digital implementation of PWLCM diminishes the unpredictability of the pseudorandom number [6], [36].

Its equation is represented as follows:

$$\begin{cases} a_1 x_n + b_1 & \text{if } x_n < c \\ a_2 x_n + b_2 & \text{otherwise} \end{cases}$$

The variables a_1, a_2, $b_1$and $b_2$determine the slopes and intercepts of the linear segments, whereas c indicates the point at which the function transitions from one linear behavior to another.



Binary Generation Process

```
1. Start with x[0] in [0,1]
2. If x[n] 0.5, output 0; else output 1
3. Apply Piecewise Linear Map:
x[n+1] = F(x[n]) where F is the
piecewise linear function
4. Repeat steps 2-3 for desired bit length
```

Binary Output Examples

```
128-bit 101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101...
192-bit 101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101...
256-bit 101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101...
```

Figure 11: Piecewise Linear Chaotic Map for Generating Binary Numbers

7. Hyperchaotic Systems

Hyperchaotic systems deals with even more complex systems than regular chaotic systems. The important highlight is that it contains more than one positive Lyapunov exponent. They are used in several fields including communication, cryptography and complex simulations. Its types include:

a. Hyperchaotic Lorenz System

The Hyperchaotic Lorenz System is an advanced version of Lorenz system, leading more complexity and security because of increase in the unpredictability. In this system an increase in the dimensionality is visible [16], [20].

The equations for a generalized Hyperchaotic Lorenz System, introducing additional components for hyperchaotic behavior, are:

$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = rx - y - xz$$
$$\frac{dz}{dt} = xy - bz + w$$
$$\frac{dw}{dt} = -\gamma w + xz$$

where σ, r, b, and γ are parameters, and w is an additional variable that introduces extra complexity, contributing to the system's hyperchaotic nature.

b. Hyperchaotic Chen System

It is also an advanced form of Chen system, having more than one Lyapunov exponent and shows more chaotic behavior by the introduction of additional non-linearities[30], [37], [38]. The equations for a typical Hyperchaotic Chen System might include an additional variable and modified parameters to induce hyper chaos:

$$\frac{dx}{dt} = a(y - x)$$
$$\frac{dy}{dt} = (c - a)x - xz + cy$$
$$\frac{dz}{dt} = xy - bz$$
$$\frac{dw}{dt} = -dz + xy$$

where a, b, c, and d are system parameters, and the addition of the variable ww extends the system to exhibit hyperchaotic behavior.

c. Hyperchaotic Coupled Map Lattices (CML)

They show hyperchaotic behavior by coupling chaotic maps across the lattice due to this Hyperchaotic CML achieves higher dimensional chaos in network-like structure and features several positive Lyapunov exponents [39], [40]. The equation for this system is stated below.

$$x_i^{n+1} = (1-\epsilon)f(x_i^n) + \frac{\epsilon}{2}[f(x_{i-1}^n) + f(x_{i+1}^n)]$$

Where

x_i^n = The state of the *i*-th map at time *n*

f= The chaotic map function (e.g., logistic map)

ϵ = Coupling strength between the maps.

d. Hyperchaotic Neural Networks

Traditional neural networks are incorporated with new models of dynamics that lead to hyperchaotic behavior neural networks having multiple positive Lypunov exponents. Hyperchaotic Neural Networks extend traditional neural network models by incorporating dynamics that lead to hyperchaotic behavior, characterized by multiple positive Lyapunov exponents. Their application covers secure communications, hyper chaotic pattern recognition These networks combine the complex, adaptive learning capabilities of neural and unpredictability for improved security networks with the unpredictable, sensitive dynamics of hyperchaotic systems [5], [41].

General form of set of equations is complex due to the variability but a simple version is stated below:

$$\frac{\mathrm{dx_i}}{\mathrm{dt}} = -\alpha \mathrm{x_i} + \sum_{j=1}^{N} \mathrm{w_{ij}}\phi(\mathrm{x_j}) + \mathrm{I_i}, \mathrm{i} = 1,2,\dots,\mathrm{N}$$

where *xi* represents the state of the *i*-th neuron, α is a decay parameter, *wij* are the synaptic weights from neuron *jj* to neuron *i*, $\phi(\cdot)$ is a nonlinear activation function, and *Ii* is the external input to the *i*-th neuron. This framework can be extended with additional equations or variables to introduce hyperchaotic behavior.

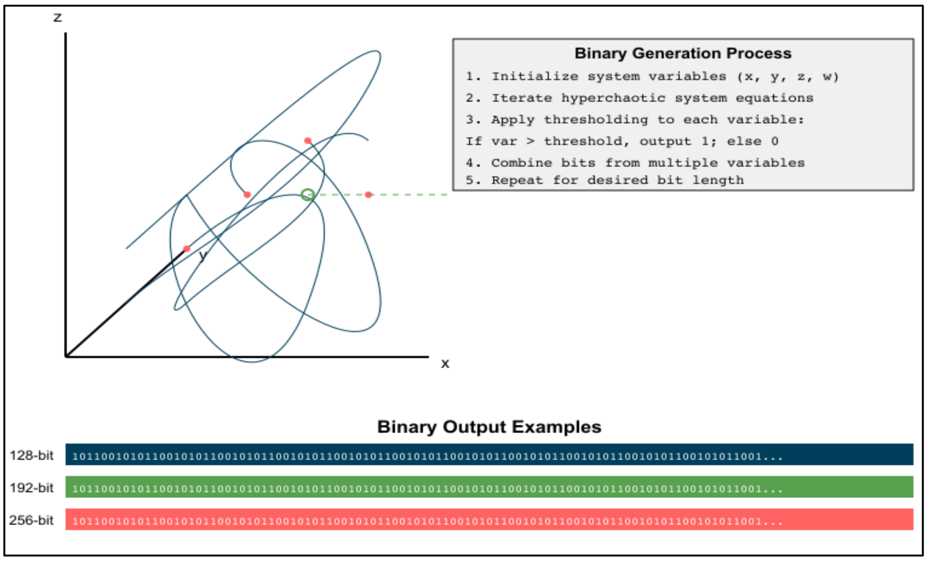
e. X-D Hyperchaotic Systems

X-D Hyperchaotic Systems depict X-dimensional state space allowing them for hyperchaotic behavior and includes multiple positive Lyapunov exponents. for the manifestation of hyperchaotic behavior, which includes more than one positive Lyapunov exponent. this is ideal for applications that require extensive security and safe communication [21], [42], [43].

4D Hyperchaotic System equation is as follows:

$$\frac{dx}{dt} = f(x, y, z, w)$$
$$\frac{dy}{dt} = g(x, y, z, w)$$
$$\frac{dz}{dt} = h(x, y, z, w)$$
$$\frac{dw}{dt} = k(x, y, z, w)$$

where *f*, *g*, *h*, and *k* are nonlinear functions of the system's state variables *x*, *y*, *z*, and *w*.



```
1. Initialize system variables (x, y, z, w)
2. Iterate hyperchaotic system equations
3. Apply thresholding to each variable:
If var > threshold, output 1; else 0
4. Combine bits from multiple variables
5. Repeat for desired bit length
```

```
128-bit 1011001010101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101010110010101011001...
192-bit 1011001010101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101010110010101011001...
256-bit 1011001010101100101010110010101011001010101100101010110010101011001010101100101010110010101011001010101100101010110010101011001...
```

Figure 12: Hyperchaotic Systems for Generating Binary Numbers in General

8. Hybrid Chaotic System

They combine the dynamics of two or more chaotic maps to get the benefit of both the systems in order to enhance the cyber security and prevent from the attacks of malware. In hybrid synchronization of chaotic systems, one component of the system achieves synchronization while the other component achieves anti-synchronization, resulting in the coexistence of full synchronization (CS) and anti-synchronization (AS) inside the system. The simultaneous presence of CS (Cryptographic Systems) and AS (Authentication Systems) is very advantageous in ensuring secure communication and disorderly encryption schemes [44], [45], [46]. The Hybrid chaotic system types:

a. Hybrid Lorenz-Rossler System

As the name suggests, it is a hybrid system that combines the characteristics of both the systems, Lorenz and Rossler system. The technique for achieving synchronization between two chaotic systems is attainable in certain chaotic systems. This enables the new pathways to explore chaos theory. It merges the butterfly effect of Lorenz and dynamic effects of Rossler system [47], [48], [49]. It is represented through equation:

$$\frac{dx}{dt} = -\sigma x + \sigma y$$
$$\frac{dy}{dt} = rx - y - xz$$
$$\frac{dz}{dt} = xy - bz + a(z - c)$$

Here, σ, r, b, a, and cc are parameters derived from both the Lorenz and Rossler systems, illustrating how elements from each can be integrated. The exact formulation can vary based on the specific objectives of the hybrid system design.

b. Hybrid Hénon-Logistic Map

The Hybrid Hénon-Logistic Map Systems are like the all-stars of chaotic systems, blending the intricate dance of the Hénon Map with the wild mood swings of the Logistic Map. This combo pack not only brings more chaos to the party but also expands the types of chaotic behaviors we can study. By merging the spatial twists and turns of the Hénon Map with the unpredictable timing of the Logistic Map, this hybrid creates a powerhouse tool for diving deep into the weird and wonderful world of non-linear dynamics[50], [51], [52].

A conceptual representation of the Hybrid Hénon-Logistic Map might be expressed as:

$$x_{n+1} = 1 - ax_n^2 + y_n + r(1 - x_n)x_n$$
$$y_{n+1} = bx_n$$

where a and b are the parameters of the Hénon Map, and r adjusts the influence of the Logistic Map, integrating the effects of both systems into a unified dynamic model.

c. Chaotic Neural Network

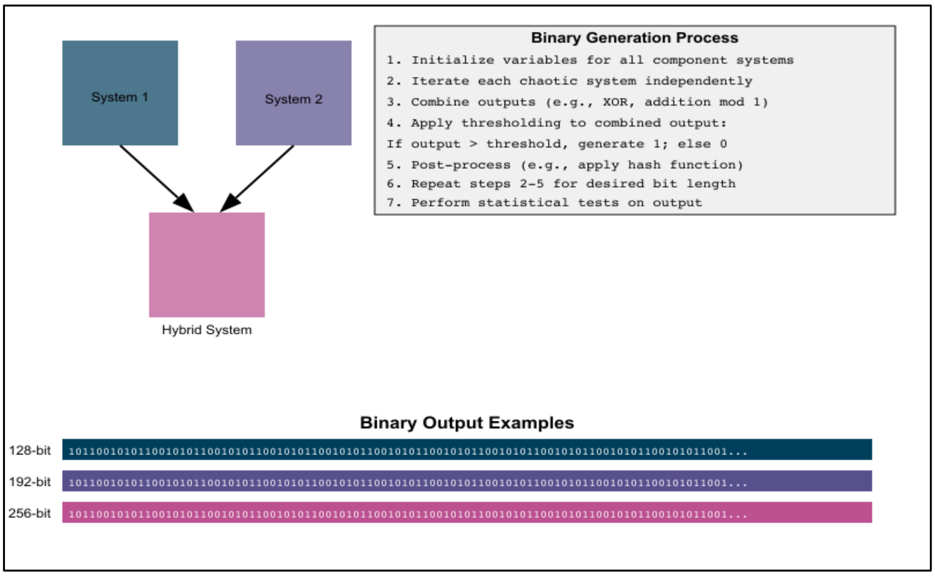
The Hybrid Chaotic Neural Network is a cutting-edge creation that marries the adaptability and learning prowess of neural networks with the wild unpredictability of chaotic systems. Picture a neural network—those layers of artificial neurons learning patterns and making predictions. Now, imagine injecting the erratic pulse of chaotic dynamics straight into this network's veins. That's what we're talking about here.

These networks aren't just your average smart systems; they take things up a notch. By embedding chaotic maps or behaviors into the neural architecture itself, these networks become super sensitive to even the tiniest changes in initial conditions and parameters. It's like they have a hyper-awareness of their environment, which can dramatically influence their computations and outputs[25], [45], [46].

A conceptual equation for a Hybrid Chaotic Neural Network could be framed as:

$$x_i^{(n+1)} = \sigma\left(\sum_{j=1}^{N} w_{ij} f\left(x_j^{(n)}\right) + \theta_i + h\left(g\left(x_i^{(n)}\right)\right)\right)$$

Where x_i^n is the state of neuron *i* at time step *n*, w_{ij} are the synaptic weights, θ_i is the bias, σ is the activation function, *f* represents the chaotic map integrated into the network, *g* is a transformation function, and *h* adds an additional layer of chaotic behavior, potentially through another chaotic map or mechanism



Binary Generation Process

```
1. Initialize variables for all component systems
2. Iterate each chaotic system independently
3. Combine outputs (e.g., XOR, addition mod 1)
4. Apply thresholding to combined output:
If output > threshold, generate 1; else 0
5. Post-process (e.g., apply hash function)
6. Repeat steps 2-5 for desired bit length
7. Perform statistical tests on output
```

Binary Output Examples

```
128-bit 101100101011001010110010101100101011001010110010101100101011001010110010101100101011001010110010101100101011001...
192-bit 101100101011001010110010101100101011001010110010101100101011001010110010101100101011001010110010101100101011001...
256-bit 101100101011001010110010101100101011001010110010101100101011001010110010101100101011001010110010101100101011001...
```

Figure 13: Hybrid Chaotic System for Generating Binary Numbers for Generating Binary Numbers in General

9. Related Work

The growing proliferation of cyber dangers has rendered powerful cryptographic systems indispensable for networking and data exchange. Chaotic maps are being emphasized as one of the major approaches for generating cryptographic keys among many methodologies. This section of the study examines current works that have made major contributions to the area of key generation based on chaotic maps, with the aim of improving cybersecurity[53].

Ghayad et al. [54] introduced a novel random key generator form by combining the Two-Dimensional Hénon map and the Two-Dimensional rational Map. The fundamental procedure of the proposed generator involved transforming the output of the two chaotic maps into 64-bit values and combining them using the XOR operation and other mathematical processes. The NIST test group examined the random sequences generated by the key and also used conventional statistical techniques for analysis.

Wang et al. [55] studied that in several practical applications, such as chaotic secure communication and chaotic pseudorandom sequence generators, a significant quantity of chaotic systems were found to be essential. Due to the absence of a systematic construction theory, the creation of chaotic systems mostly relies on the comprehensive exploration of systematic parameters or starting values, particularly for a category of dynamical systems that include concealed chaotic attractors. The study examined a specific category of chaotic maps known as quadratic polynomial chaotic maps and presented a comprehensive approach for creating such maps. The polynomial chaotic maps described in the study adhered to the Li-Yorke definition of chaos. This approach effectively regulated the magnitude of chaotic time series with precision. By conducting an examination of the fixed points' existence and stability, it was proven that quadratic polynomial maps of this kind were incapable of possessing concealed chaotic attractors.

Huang et al.[29] introduced a novel system that combined the three-dimensional Chen chaotic system with a chaotic technique. The study demonstrated that this new system met the criteria for chaos as defined by Wiggins. The complexity tests explained that the output of this new system surpasses the complexity of any dimensional variable in the Chen system. A novel Pseudorandom Bit Generator (PRBG) that was built and a coding procedure was used to standardize the sequences. The results showed that the produced PRBS exhibited excellent randomization properties and robustness against various assaults, while also achieving high practical speed.

The digital information is efficiently delivered over various communication channels with great speed. The digital realm is rapidly advancing and has become a crucial component of our everyday existence. Regarding the matter at hand, pertaining to the confidentiality of this digital information. One of the essential problems is that information is sent across an unsecured route of communication. The digital information is stored in many web databases. The study of Tariq et al.[28] analyzed the Logarithmic based picture encryption system and examined any possible vulnerabilities in its key security by using a public key to get the private key.

Furthermore a method based on chaos that offers enhanced security was proposed in the study. The Lorenz system was used in a projected mechanism that was highly responsive to beginning circumstances and chaotic parameters. The suggested approach was then verified by using existing security performance standards. In order to assess the level of security against various cryptographic assaults, statistical studies such as entropy and correlation between pixels, as well as differential analyses including the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) were assessed. To counter brute force assaults, key sensitivity analysis and key space analyses were also conducted. The suggested encryption system was examined for randomness using entropy and NIST randomness suit tests. In addition, a comparative analysis of our modified confidentiality scheme with current benchmarks was carried out, which indicated that encryption approach in the study was very suitable for ensuring the security of digital multimedia.Study of Li et al.[56] presented a predictive analytic method based on deep learning (DL) to assess the security of a non-deterministic random number generator (NRNG) that utilizes white chaos. The temporal pattern attention (TPA)-based deep learning (DL) model was used to study and learn from the data obtained from both phases of the non-linear random number generator (NRNG): the chaotic output data of an external-cavity semiconductor laser (ECL) and the final output data of the NRNG. The findings of the ECL stage indicated that the model effectively identified underlying correlations resulting from the time-delay signature. Upon the implementation of optical heterodyning on two chaotic External Cavity Lasers (ECLs) and minimum further processing, the model failed to identify any patterns in the relevant data. It showed that the NRNG has robust resistance against the prediction model. Before these works, the model's strong predictive capacity was examined and shown by applying it to a random number generator (RNG) that utilized the linear congruential technique. The study indicated that the deep learning-based prediction model is anticipated to provide an effective enhancement for assessing the security and quality of random number generators.

In a study by Sudeepa et al.[57], the researchers explored the use of a Linear Feedback Shift Register (LFSR) to generate a non-binary pseudo-random key sequence. To extend the length of the sequence beyond the typical maximum length of an LFSR, they developed a hybrid model that combined an LFSR with a Genetic Algorithm (GA). The primary goal of this approach was to surpass the inherent length limitations of a standalone LFSR.The researchers performed statistical tests to evaluate the randomness of the key sequence generated by their hybrid model. Subsequently, the generated key sequences were employed for cryptographic applications, and their performance was assessed. The study's findings concluded that the proposed method successfully produced key sequences that exceeded the maximum length achievable by a conventional LFSR.Furthermore, the statistical tests confirmed the homogeneity and independence of the data within the generated key sequences. The results demonstrated that these longer key sequences exhibited suitable characteristics for cryptographic purposes. Notably, the study highlighted that increasing the length of the key sequence can effectively strengthen the underlying cryptographic technique.

In their study, Moysis et al. [58] proposed a variant of the traditional logistic map by incorporating fuzzy triangular numbers. The analysis of this modified map involved examining its Lyapunov exponent and bifurcation diagrams. Compared to the traditional version, this variant exhibited increased complexity, displaying phenomena such as ant monotonicity and crisis behavior.

Subsequently, the researchers utilized this modified logistic map to address the challenge of generating pseudo-random bit sequences. They employed a straightforward method to produce the bit sequence from the map's output. The generated random bit generator underwent statistical testing by the National Institute of Standards and Technology (NIST) and successfully passed these tests

To further validate their approach, the researchers applied the generated bit sequence for image encryption purposes. It is well-established that the entropy of an encrypted image should approximate a value of 8 for optimal security. In their experiments, the original image had an information entropy of 7.4450, while the encrypted version exhibited an entropy of 7.9670. This higher entropy value for the encrypted image, being closer to the target of 8, suggested that the encrypted information was more secure against entropy-based attacks.

The study by Moysis et al. demonstrated the potential of incorporating fuzzy logic concepts into chaotic maps, resulting in enhanced complexity and improved performance for applications such as pseudo-random bit generation and image encryption. Data encryption greatly benefits from the application of chaotic dynamics, as demonstrated by Lawnik et al[17] in their study on the M-map. This research delves into the M-map’s dynamics, analyzing its fixed points, bifurcation diagram, and Lyapunov exponents. The findings reveal that the map displays robust chaos, indicated by Lyapunov exponent values ranging from ln2 to ln4, which underscores its potential for secure encryption algorithms. The study goes further by introducing a new image encryption technique that incorporates cyclically shifting S-boxes to manipulate pixel positions, enhancing security by reducing predictability. This method also strategically places encrypted pixels at the start or end of the cipher image to maximize entropy and minimize correlation between adjacent pixels.

The effectiveness of this approach is evidenced by the impressive encryption metrics reported: entropy values nearing 8, pixel correlation values approaching zero, and high rates of pixel change (NPCR) and average intensity change (UACI). These metrics confirm the encryption's strength, making the M-map a promising tool for cryptography, especially in securing digital images against unauthorized access.

According to the study of Menon et al.[59] this research employed a unique 2D chaotic function that demonstrated a consistent branching pattern over a wide variety of parameters and demonstrated significant degrees of chaotic activity. This function was used to create a random sequence, which was then employed to encrypt the input data. The suggested approach employed a genetic algorithm to optimize the parameters of the map in order to improve the security of any given textual data. many evaluations confirmed a sufficiently vast key space and the presence of many global optima, highlighting the requirement and security offered by the proposed system.

Rahman et al. [60] aimed to address the delay latency needed for safe encryption and decryption, the suggested technique recommends modifying both the key-origination matrix and the S-box. It is likely that the time it takes to send a plain-text message is proportional to the length of the message, but the length of the message is not proportional to the likelihood of a letter being in the message. The current endeavor in the study is to understand how the increase in seeming disorder leads to the desired activation of the key before transmitting a message. Several initiatives have emerged advocating for the use of lightweight block ciphers as a viable alternative for safeguarding the Internet of Things. Currently, it has been possible to envision the privacy-preserving aspects of smart and sensor-oriented appliances as a widely applicable framework. Various methodologies are prone to inefficiency when it comes to achieving the appropriate level of security, given the ease and simplicity of the procedure.

Enhancing the well-recognized symmetric key and block-dependent technique by including either a chaos-driven logistic map or an elliptic curve has shown significant promise for ensuring confidentiality in real-time communication. The logistic maps are known for their unpredictability and randomness, which make them suitable for dynamic key propagation in synchronization with chaos and scheduling techniques to ensure data integrity. Any little changes in encryption keys might result in significant deviations and could compromise data secrecy. In the future, there may be a need to minimize the time it takes to send data between participating nodes, which might provide a hurdle. Massive MIMO is a very promising technique for the implementation of fifth and subsequent generations of mobile communication networks. Generalized Spatial Modulation (GenSM) in huge MIMO systems offers significant promise in terms of increasing channel capacity, reducing bit error rate, and improving spectral efficiency. The main considerations in the implementation of these networks are on their security. Physical layer security (PLS) is a developing solution for security issues in future networks, serving as a substitute for standard cryptographic security procedures. This kind of security architecture is based on the information-theoretic features of wireless networks. In the age of powerful eavesdroppers with sophisticated technologies like quantum computing, it provides enhanced security.

The current PLS key generation approaches are compromised in terms of secrecy because of the slow and inefficient communication channel settings. The study of Tamilselvan et al.[61] presented a method for generating encryption keys at the physical layer using deep learning. The method utilized a neural network that is modeled using Chua's chaotic dynamics. The suggested approach has the capability to generate keys that are very safe. The study introduced a new and innovative transmitter and receiver system with dual key functionality for PLS. The study was conducted using the secrecy parameters of secrecy rate and secrecy outage probability to assess the performance of the proposed system. The simulation results confirmed the superiority of the proposed approach over the Chaotic Antenna index Three-dimensional Modulation and Constellation Points Rotated (CATMCPR) method and traditional massive MIMO. Additionally, the simulation findings indicated a substantial decrease in Eve's eavesdropping capability when compared to the most advanced systems. Conversely, Bob's resources are seeing substantial improvement. Eve has a significant Bit Error Rate (BER) when the Signal-to-Noise Ratio (SNR) reached 42 dB. In contrast, the CATMCPR technique and the Bean Division Multiple Access (BDMA) based PLS have a similar range of SNR values, with the CATMCPR method having a range of 36 dB and the BDMA based PLS having a range of

28 db. As a result, the proposed system had a secrecy rate that was three times greater than standard massive MIMO and about a 15% improvement compared to the CATMCPR approach.

Wei et al.[62] in their study presented a technique for generating chaotic keys utilizing QAM constellation points in an OFDM-PON system. The purpose of this approach was to dynamically modify the security key. The suggested technique involved prearranging key generation rules between the transmitter and receiver, with the created key being linked to the features of the most recent uplink user data. Instead of using the security key for transmission, appropriate parameters were used. Research showed that this strategy effectively increased the challenge for unauthorized attackers attempting to capture user data and strengthens its resistance against exhaustive attempts. Furthermore, it was occluded that using this method did not have any notable effects on computational complexity or transmission performance. altering the criteria for generating keys, it has been made possible to assess the correlation between the size of the key space acquired and the amount of storage space required for keys at both the sender and recipient.

Security is the primary focus in communication during this age of digital technology. An innovative key generation method was suggested by Nalini et al.[63] for the purpose of picture encryption. The proposed study utilized a hyper chaotic map and DNA sequences for its execution. The Beta chaotic function was used to achieve hyper chaotic behavior, and scrambling had been further utilized to intensify chaos, hence enhancing key security. The scrambled picture faced DNA addition and complement processes, which enhanced the level of complexity of the system. Ultimately, the cryptographic key was produced by the use of SHA256, enabling its application in the encryption of images. Multimodal sensing was used to augment security and precision. The simulation findings demonstrated that the key obtained via the utilization of a hyper-chaotic functionality and DNA addition was exceedingly sensitive and secure. Various techniques were used to assess the robustness of the produced key, hence demonstrating the algorithm's resistance to key sensitivity analysis, entropy of information analysis, and correlation coefficient analysis.

Shah et al.[64] proposed an approach that employed 3-D chaotic sequences to rearrange the audio data points in order to accomplish the diffusion feature. In the confusion module, the audio data sequence was originally separated into 8-bit and 7-bit sequences. Afterwards, the individual sequences were replaced with distinct replacement boxes of high quality. These substitution boxes were created via a Mobius transformation over Galois fields. The proposed encryption technique was used on a range of audio files with varying sizes and character compositions. The testing findings have shown that the suggested technique was capable of ensuring the security of all types of audio data.

According to the study of Saber et al., [10] discussed that The Lemniscate chaotic map (LCM) offered a broad spectrum of control parameters, eliminating the need for several iterations and demonstrated exceptional effectiveness in the process of carrying out randomization test. This study introduced a low power hardware model of LCM, known as practical lemniscate chaotic map (P-LCM), which utilized trigonometric identities to simplify the standard model and decreased its complexity. The hardware model wass created and implemented on the field programmable gate array (FPGA) board, namely the Spartan-6 SLX45FGG484-3. The suggested model demonstrated a significant decrease of 48.3% in resource utilization and a 34.6% decrease in power consumption compared to the standard LCM. In addition, we provided a novel pseudo-random number generator that utilized a low power P-LCM model. Randomization experiments were conducted to evaluate the effectiveness of the proposed encryption system. Implementation findings demonstrated a significant 33% decrease in power usage when using the “Practical" model as opposed to the "conventional" approach.

Many scholars and institutes have recognized the significance and advantages of cryptography in enhancing the efficiency and efficacy of many areas of secure communication. The study of Al-Hassani[65] utilized an innovative approach to create a safe data cryptosystem by using chaos theory. The algorithm generated a 2-Dimensional key matrix with the same dimensions as the original image. The matrix was filled with random numbers obtained from a 1-Dimensional logistic chaotic map using given control parameters. The fractional parts of these numbers were then converted into a set of non-repeating numbers using a function. The process executed resulted in a large number of unpredictable probabilities, equal to the factorial of the number of rows multiplied by the number of columns. The values of numbers were subjected to double layers of permutation, including both rows and columns, for a predetermined number of stages. Next, the key matrix was XORed with the original picture, providing a robust method for encrypting data in many file formats such as text, image, audio, video, and more. The results demonstrate that the suggested encryption method shows great potential when evaluated on over 500 image samples, based on security metrics. The histograms of the encrypted images are significantly flatter compared to the original images. However, the average Mean Square Error is quite high at 10115.4, and the Peak Signal to Noise Ratio is very low at 8.17. Additionally, the correlation is close to zero and the entropy is approximately 8 (7.9975).

Erkan et al. [19] introduce a image encryption scheme leveraging a chaotic log-map deep convolutional neural network (CNN) model for key generation and bit reversion operations, aimed at bolstering security against a variety of cryptographic attacks and enhancing encryption performance. Through comprehensive analysis across several metrics—key space, key sensitivity, information entropy, histogram correlation, and resistance to differential, noisy, and cropping attacks—the scheme's robustness and efficiency in protecting images are demonstrated. The scheme's resilience is underscored by its performance against diverse attacks, affirming its high security for image encryption. Key space analysis reveals that a key length exceeding 10120, derived from deep CNN-generated SHA 512, ensured security, effectively negating brute-force attack feasibility. Key sensitivity analysis showcased the scheme's acute sensitivity to key variations, with a mean distinctive level of 99.6164% across different keys, indicating robust diversity performance. Information entropy analysis further validated the encrypted images' randomness, achieving near-maximum entropy values.

The research work of Churchill et al.[66] elaborated A novel data-driven numerical framework recently created for the learning and modeling of unknown dynamical systems utilizing either fully- or partially-observed data. The technique employed deep neural networks (DNNs) to create a model for the flow map of the unidentified system. This research utilized the framework to analyze chaotic systems, namely the renowned Lorenz 63 and 96 systems. With the primary objective to thoroughly evaluate the forecasting accuracy of this technique. One notable characteristic of chaotic systems observed was that even the tiniest disturbances resulted in significant (but limited) variations in the solution paths. This raised doubts about the reliability of long-term forecasts using the approach, or any other data-driven methods, since the precision of the local model would gradually decline and resulted in significant inaccuracies at individual data points. In this study, several qualitative and quantitative methods were used to ascertain the acquisition of chaotic dynamics. The mentioned analyses included phase graphs, histograms, autocorrelation, correlation dimension, approximation entropy, and Lyapunov exponent. By using these metrics, it was demonstrated that the DNN learning approach, which relied on flow maps, effectively represented chaotic systems. The DNNs have access to just a portion of the state variables. The model was able to properly reproduce the chaotic behavior of the whole system.

In the study conducted by Zhang et al.[67] it has been proposed that deep learning-based physical-layer secret key generation (PKG) has been used to overcome the imperfect uplink/downlink channel reciprocity in frequency division duplexing (FDD) orthogonal frequency division multiplexing (OFDM) systems. Current efforts have focused on key generation for users in a specific environment where the training samples and test samples followed the same distribution, which was unrealistic for real-world applications. The research formulated the PKG problem in multiple environments as a learning-based problem by learning the knowledge such as data and models from known environments to generate keys quickly and efficiently in multiple new environments. Specifically, it was investigated that deep transfer learning (DTL) and meta-learning-based channel featured mapping algorithms for key generation. The two algorithms used different training methods to pre-train the model in the known environments, and then quickly adapted and deployed the model to new environments. Simulation and experimental results showed that compared with the methods without adaptation, the DTL and meta-learning algorithms both improved the performance of generated keys. In addition, the complexity analysis showed that the meta-learning algorithm can achieve better performance than the DTL algorithm with less cost, thus enhancubg cryptographic security.

Irfan et al. [68]demonstrated that by using the suggested CoC, the RLM may be modified to produce pseudorandom integers that are cryptographically safe. The RLM had a vast and disordered range of parameters and demonstrated a positive Lyapunov exponent. However, its non-uniform probability distribution of trajectories rendered it unsuitable for cryptographic purposes. Therefore, the use of CoC in RLM results in an output sequence that is evenly distributed. The proposed design of the CSPRNG underwent evaluation utilizing the NIST 800-22 tests. The correlation, key-sensitivity, and key-space statistical analysis demonstrated that the extensive parameter space of RLM provided a sufficiently long key length and key space to effectively withstand all known assaults. Therefore, suggested modified RLM (MRLM) had the potential to be used in diverse cryptographic applications such as image processing, telemedicine, electronic payment systems, computing, text encryption, personal information security, biometrics, and military applications, among others.

Al-Saadi et al.[46] targeted a hybrid chaotic key generator (HCKG) that utilized the 3D Lorenz and 2D Henon maps to produce a highly randomized key. This key is then combined with the LED to provide a strong degree of encryption on devices with limited resources.

To enhance the complexity of the ciphertext, simple procedures were used to derive subkeys from the HCKG every four rounds. These subkeys were then XORed with the state. In addition, using the HCKG with subkeys enable to reduce the overall number of LED rounds from 32 to 24, therefore minimizing computational expenses while still maintaining a robust degree of security.

The National Institute of Science and Technology (NIST) test suite confirmed that the proposed LED-HCKG exhibited a significant performance improvement of around 0.3283 compared to LED in terms of data integrity and confidentiality.

Li et al.[41] delves into the use of artificial neural networks (NNs) as models of chaotic dynamics. The research validated the effectiveness of neural networks (NN) in replicating chaotic behavior. It demonstrated that a concise NN trained on a limited number of data points, can successfully recreate odd attractors, make predictions beyond the bounds of the training data, and properly estimate local divergence rates. These geometric procedures demonstrated topological mixing and chaos, clarifying why neural networks are inherently well-suited to simulate chaotic processes.

Table 1: The Studies in Chaotic Map

	Year	**Author(s)**	**Aim of Study**	**Key Results**
1.	**2019**	Ghayad et al.	To design a new random key generator using a combination of the Two-Dimensional Hénon Map and Two-Dimensional Rational Map, enhancing encryption security.	- Successfully passed NIST tests, indicating high randomness. -Demonstrated a large keyspace capable of resisting brute-force attacks. -Showed high key sensitivity and security against differential attacks. -Favorable speed performance for encryption applications.
2.	**2019**	Wang et al.	Introduce a method for constructing quadratic polynomial chaotic maps with controllable amplitude for cryptographic applications.	- Systematic method for creating new chaotic maps. - Proved the absence of hidden chaotic attractors. - Demonstrated effectiveness through examples and simulations. - Extended methodology to high-degree polynomial chaotic maps.
3.	**2019**	Huang et al.	To develop a PRBG using a three-	- Generated sequences with high complexity and good randomness.

			dimensional Chen chaotic system mixed with chaotic tactics for cryptographic security.	- Successfully passed NIST test suite for randomness. - Proposed coding algorithm ensures sequence uniformity. - Demonstrated potential for secure cryptographic applications.
4.	**2020**	Tariq et al.	To analyze and enhance the security of a logarithmic public key encryption algorithm by integrating a chaotic Lorenz system.	- Successfully passed NIST randomness tests - Demonstrated high randomness and large keyspace. - Showed strong resistance to differential attacks (high NPCR and UACI scores) - Competitive speed performance for practical applications
5.	**2020**	Li et al.	To analyze the security of an NRNG using white chaos with a DL-based predictive analysis.	- Detected correlations in ECL stage data, indicating potential security risks. - Found no patterns after optical heterodyning, showing strong NRNG security. - Highlighted the effectiveness of DL in RNG security evaluation.
6.	**2020**	Sudeepa et al.	Enhance big data security with a novel key generation model using permutation function and chaotic selection.	- Successfully passed NIST tests, indicating high randomness. - Demonstrated potential for use in cryptological encryption and data hiding. - Efficiency of chaotic systems in enhancing key security highlighted.
7.	**2020**	Moysis et al.	Enhance the logistic map's chaotic behavior using fuzzy numbers for secure pseudorandom	- Increased map complexity and higher Lyapunov exponent. - RBG passed NIST randomness tests.

			number generation and image encryption.	- High security of encrypted images confirmed by statistical analyses.
8.	**2020**	Lawnik et al.	Introduce and analyze the M-map for chaos-based cryptography, developing a new image encryption algorithm.	- Robust chaos without periodic windows. - Proposed encryption algorithm shows high security based on entropy, correlation, NPCR, and UACI analyses. - Demonstrated superiority of M-map over traditional chaotic maps in cryptography.
9.	**2020**	Menon et al.	Propose a text encryption method using a 2D chaotic function optimized with a genetic algorithm.	- Effective generation of random sequences for encryption. - Optimization of chaotic map parameters for enhanced security. - Demonstrated robustness through chaotic behavior analysis. - Offers a novel encryption method leveraging chaos theory and genetic algorit
10.	**2021**	Rahman et al.	To enhance AES-driven IoT security with a new key generation technique using chaos theory and the logistic map.	- Introduced 3DKGM for complex key generation. - Preserved data integrity in sensitive IoT applications. - Empirical evaluations justify improved security strength. - Addressed and proposed solutions for latency challenges in encryption/decryption processes.
11.	**2021**	Tamilselvan et al.	To develop a CDNN-based PLS protocol for GenSM aided massive MIMO systems, enhancing key generation for 5G security.	- Significantly increases secrecy rate. - Introduces deep learning techniques for information reconciliation and privacy amplification.

				- Achieves superior performance against eavesdropping, with a notable improvement over conventional and CATMCPR methods. - Proposes a novel dual key transmitter and receiver for enhanced PLS.
12.	**2021**	Wei et al.	To propose a dynamic chaotic key generation method for OFDM-PON systems, enhancing security against eavesdropping and exhaustive attacks.	- Enhanced security and resistance to attacks. - Maintained computational efficiency and transmission performance. - Demonstrated high sensitivity to initial conditions and parameter changes for secure key generation. - Provided a method for balancing key space and storage requirements.
13.	**2021**	Nalini et al.	To develop a secure key generation algorithm for image encryption using hyper-chaotic maps and DNA sequences.	- High sensitivity and protection of the generated keys confirmed by various analyses. - Utilization of multimodal biometrics for enhanced security and accuracy. - Proved resistance to attacks, suitable for securing digital communication.
14.	**2021**	Shah et al.	To introduce a novel 3-D chaotic system for digital audio security and propose a lossless audio encryption scheme.	- Demonstrated enhanced chaotic behavior and dynamic properties. - Successfully encrypted various audio files, showing robustness against attacks. - Comprehensive security analysis validated the scheme's effectiveness and security.

15.	**2021**	Saber et al.	Develop a low power P-LCM and introduce a PRNG based on it for cryptographic applications.	- Achieved significant reductions in power consumption and resource use on FPGA. - Developed PRNG passed NIST SP800-22 randomization tests. - Demonstrated the potential for chaotic maps in low power cryptographic applications.
16.	**2022**	Al-Hassani	To propose a novel cryptosystem using chaotic logistic maps for generating a 2D key-matrix image, enhancing file encryption security.	- High MSE and low PSNR values confirm strong encryption. - Near-zero correlation and entropy close to 8 indicate high randomness and security. - Demonstrated robustness and versatility across various image samples.
17.	**2022**	Erkan et al.	To introduce a secure image encryption scheme based on a chaotic logarithmic map and deep CNN for key generation.	- Passed multiple security analyses with high marks, indicating strong encryption. - Demonstrated resistance to brute-force, differential attacks, and more. - Showed competitive speed, suitable for practical applications.
18.	**2022**	Churchill et al.	To develop a framework for modeling unknown dynamical systems, particularly chaotic systems, using DNNs based on fully or partially observed data.	- Successfully modeled chaotic dynamics with limited observations. - Used comprehensive measures to validate the effectiveness of DNN models. - Showed potential for predicting high-dimensional chaotic systems with sparse data.
19.	**2022**	Zhang et al.	To enhance PKG in FDD-OFDM systems using DTL and meta-learning, addressing	- Introduced DTL and meta-learning for efficient key generation.

			the challenge of channel reciprocity across multiple environments.	- Demonstrated significant performance enhancements in new environments. - Conducted complexity and security analyses, validating the approach's feasibility and robustness. - Practical validation through experimental evaluation, showcasing real-world applicability.
20.	**2022**	Irfan et al.	To generate cryptographically secure random numbers using a modified robust logistic map with control of chaos.	- Successfully passed NIST 800-22 tests, indicating suitability for cryptographic applications. - Enhanced binary distribution balance through CoC, improving cryptographic security. - Demonstrated the effectiveness of chaotic systems in cryptographic key generation.
21.	**2023**	Al-Saadi et al.	Enhance LED security for resource-constrained devices using a hybrid chaotic key generator based on 3D Lorenz and 2D Henon maps.	- Significant performance improvement in data integrity and secrecy. - Reduced total encryption rounds from 32 to 24, minimizing computational costs. - Successfully passed NIST tests, demonstrating unpredictability and robustness. - Increased ciphertext complexity and vast keyspace, enhancing security against attacks.
22.	**2023**	Ziwei Li and Sai Ravela	To theoretically explore and demonstrate how neural networks can model chaotic	- Efficiently emulated chaos with limited training data. - Introduced a geometric interpretation of neural network operations essential for chaos.

			dynamics from a geometric perspective.	- Demonstrated topological mixing in neural networks as a basis for chaos. - Showed that low complexity in neural networks is effective for modeling chaotic systems.

10. Conclusion

The comprehensive review of chaotic map-based cryptographic key generation techniques underscores the significant advancements and innovative approaches developed to enhance digital security. The studies reviewed reveal a diverse array of methods leveraging chaos theory and its inherent unpredictability to fortify cryptographic systems against increasingly sophisticated cyber threats. Notably, the integration of chaotic maps, whether traditional or hyper-chaotic, has emerged as a pivotal strategy in generating robust cryptographic keys, demonstrating superior performance in terms of randomness, unpredictability, and resistance to cryptanalytic attacks.

refine how chaotic maps produce cryptographic keys, ultimately improving both security and reliability. Its insights have broad relevance, from protecting personal data and financial transactions to securing countless connected devices. By making secure encryption more accessible and effective, the research supports a safer, more trustworthy digital environment for everyone.

The employment of chaotic dynamics, characterized by sensitivity to initial conditions and deterministic chaos, aligns perfectly with the cryptographic need for keys that are both secure and efficient. Moreover, the exploration of hybrid chaotic systems and the adaptation of neural networks to model chaotic behavior further illustrate the field's direction towards employing *complex systems to achieve higher security standards. These methodologies not only enhance the cryptographic key generation process but also contribute to the broader discourse on securing digital communication and data integrity in an era marked by pervasive cyber vulnerabilities.

References

[1] N. Allahrakha, “Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age,” Legal Issues in the Digital Age, vol. 4, no. 2, pp. 78–121, 2023, doi: 10.17323/2713-2749.2023.2.78.121.

[2] J. Kaur and K. R. Ramkumar, “The recent trends in cyber security: A review,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, pp. 5766–5781, 2022, doi: 10.1016/j.jksuci.2021.01.018.

[3] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, “A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security,” Comput Secur, vol. 128, p. 103123, 2023, doi: 10.1016/j.cose.2023.103123.

[4] Z. M. Gao, J. Zhao, and Y. J. Zhang, “Review of chaotic mapping enabled nature-inspired algorithms,” Mathematical Biosciences and Engineering, vol. 19, no. 8, pp. 8215–8258, 2022, doi: 10.3934/mbe.2022383.

[5] U. Bhat and S. B. Munch, “Recurrent neural networks for partially observed dynamical systems,” Phys Rev E, vol. 105, no. 4, 2022, doi: 10.1103/PhysRevE.105.044205.

[6] T. Saito, “Piecewise linear switched dynamical systems: A review,” Nonlinear Theory and Its Applications, IEICE, vol. 11, no. 4, pp. 373–390, 2020, doi: 10.1587/nolta.11.373.

[7] A. H. Khaleel and I. Q. Abduljaleel, “Chaotic Image Cryptography Systems: A Review,” Samarra Journal of Pure and Applied Science, vol. 3, no. 2, pp. 129–143, 2021, doi: 10.54153/sjpas.2021.v3i2.244.

[8] N. F. Hassan, A. Al-Adhami, and M. S. Mahdi, “Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps,” Baghdad Journal of Science, vol. 63, no. 2, pp. 830–842, 2022, doi: 10.24996/ijs.2022.63.2.36.

[9] H. Wu et al., “Design and implementation of true random number generators based on semiconductor superlattice chaos,” Microelectronics J, vol. 114, no. January, p. 105119, 2021, doi: 10.1016/j.mejo.2021.105119.

[10] M. Saber and M. M. Eid, “Low power pseudo-random number generator based on lemniscate chaotic map,” International Journal of Electrical and Computer Engineering, vol. 11, no. 1, pp. 863–871, 2021, doi: 10.11591/ijece.v11i1.pp863-871.

[11] S. Krishnamoorthi, P. Jayapaul, R. K. Dhanaraj, V. Rajasekar, B. Balusamy, and S. H. Islam, “Design of pseudo-random number generator from turbulence padded chaotic map,” Nonlinear Dyn, vol. 104, no. 2, pp. 1627–1643, 2021, doi: 10.1007/s11071-021-06346-x.

[12] R. B. Naik and U. Singh, “A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption,” Annals of Data Science, vol. 11, no. 1, pp. 25–50, 2022, doi: 10.1007/s40745-021-00364-7.

[13] L. Baldanzi et al., “Cryptographically secure pseudo-random number generator IP-core based on SHA2 algorithm,” Sensors (Switzerland), vol. 20, no. 7, 2020, doi: 10.3390/s20071869.

[14] Y. Cao et al., “Entropy Sources Based on Silicon Chips: True Random Number Generator and Physical Unclonable Function,” Entropy, vol. 24, no. 11, 2022, doi: 10.3390/e24111566.

[15] S. Krishnamoorthi, P. Jayapaul, and V. Rajasekar, “A modernistic approach for chaotic based pseudo random number generator secured with gene dominance,” Sadhana - Academy Proceedings in Engineering Sciences, vol. 46, no. 1, 2021, doi: 10.1007/s12046-020-01537-5.

[16] D. He, R. Parthasarathy, H. Li, and Z. Geng, “A Fast Image Encryption Algorithm Based on Logistic Mapping and Hyperchaotic Lorenz System for Clear Text Correlation,” IEEE Access, vol. 11, no. June, pp. 91441–91453, 2023, doi: 10.1109/ACCESS.2023.3305637.

[17] M. Lawnik and M. Berezowski, “New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography,” Symmetry (Basel), vol. 14, no. 5, 2022, doi: 10.3390/sym14050895.

[18] J. S. Muthu and P. Murali, “Review of Chaos Detection Techniques Performed on Chaotic Maps and Systems in Image Encryption,” SN Comput Sci, vol. 2, no. 5, 2021, doi: 10.1007/s42979-021-00778-3.

[19] U. Erkan, A. Toktas, S. Enginoğlu, E. Akbacak, and D. N. H. Thanh, “An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN,” Multimed Tools Appl, vol. 81, no. 5, pp. 7365–7391, 2022, doi: 10.1007/s11042-021-11803-1.

[20] B. Ge, G. Chen, X. Chen, and Z. Shen, “Efficient Hyperchaotic Image Encryption Algorithm Based on a Fast Key Generation Method and Simultaneous Permutation-Diffusion Structure,” Security and Communication Networks, vol. 2022, 2022, doi: 10.1155/2022/2237525.

[21] A. E. Hampton and J. D. Meiss, “The three-dimensional generalized Hénon map: Bifurcations and attractors,” Chaos, vol. 32, no. 11, 2022, doi: 10.1063/5.0103436.

[22] Z. M. Gao, J. Zhao, and Y. J. Zhang, “Review of chaotic mapping enabled nature-inspired algorithms,” Mathematical Biosciences and Engineering, vol. 19, no. 8, pp. 8215–8258, 2022, doi: 10.3934/mbe.2022383.

[23] R. B. Naik and U. Singh, “A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption,” Annals of Data Science, vol. 11, no. 1, pp. 25–50, 2022, doi: 10.1007/s40745-021-00364-7.

[24] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, “Designing Substitution Box Based on the 1D Logistic Map Chaotic System,” IOP Conf Ser Mater Sci Eng, vol. 1076, no. 1, p. 012041, 2021, doi: 10.1088/1757-899x/1076/1/012041.

[25] P. Parida et al., “Elliptic curve cryptographic image encryption using Henon map and Hopfield chaotic neural network,” Multimed Tools Appl, vol. 82, no. 22, pp. 33637–33662, 2023, doi: 10.1007/s11042-023-14607-7.

[26] Y. Luo, J. Yu, W. Lai, and L. Liu, “A novel chaotic image encryption algorithm based on improved baker map and logistic map,” Multimed Tools Appl, vol. 78, no. 15, pp. 22023–22043, 2019, doi: 10.1007/s11042-019-7453-3.

[27] A. Chamoli, J. Ahmed, M. A. Alam, and B. Alankar, “INTELLIGENT SYSTEMS AND APPLICATIONS IN A Diffusion Model Based on the Features of the 3D Chaotic Baker Map for Image Encryption,” Intelligent Systems and Applications, vol. 11, pp. 173–180, 2023.

[28] S. Tariq, M. Khan, A. Alghafis, and M. Amin, “A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation,” Multimed Tools Appl, vol. 79, no. 31–32, pp. 23507–23529, 2020, doi: 10.1007/s11042-020-09134-8.

[29] X. Huang, L. Liu, X. Li, M. Yu, and Z. Wu, “A new pseudorandom bit generator based on mixing three-dimensional chen chaotic system with a chaotic tactics,” Complexity, vol. 2019, 2019, doi: 10.1155/2019/6567198.

[30] K. M. Hosny, S. T. Kamal, and M. M. Darwish, “Novel encryption for color images using fractional-order hyperchaotic system,” J Ambient Intell Humaniz Comput, vol. 13, no. 2, pp. 973–988, 2022, doi: 10.1007/s12652-021-03675-y.

[31] S. Kanwal et al., “An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices,” Sensors, vol. 22, no. 12, 2022, doi: 10.3390/s22124359.

[32] H. Zhu, Y. Zhao, and Y. Song, “2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption,” IEEE Access, vol. 7, pp. 14081–14098, 2019, doi: 10.1109/ACCESS.2019.2893538.

[33] M. Bucolo, A. Buscarino, L. Fortuna, and S. Gagliano, “Multidimensional Discrete Chaotic Maps,” Front Phys, vol. 10, no. April, pp. 1–10, 2022, doi: 10.3389/fphy.2022.862376.

[34] W. S. Lee and S. Flach, “Deep learning of chaos classification,” 2020.

[35] A. Tutueva, D. Pesterev, A. Karimov, D. Butusov, and V. Ostrovskii, “Adaptive Chirikov Map for Pseudo-random Number Generation in Chaos-based Stream Encryption,” Conference of Open Innovation Association, FRUCT, pp. 333–338, 2019, doi: 10.23919/FRUCT48121.2019.8981516.

[36] D. W. Ahmed, T. M. Jawad, and L. M. Jawad, “An effective color image encryptionscheme based on double piecewise linear chaotic map method and RC4 algorithm,” Journal of Engineering Science and Technology, vol. 16, no. 2, pp. 1319–1341, 2021.

[37] C. Zhao, T. Wang, H. Wang, Q. Du, and C. Yin, “A Novel Image Encryption Algorithm by Delay Induced Hyper-chaotic Chen System,” Journal of Imaging Science and Technology, vol. 67, no. 1, pp. 1–15, 2023, doi: 10.2352/J.ImagingSci.Technol.2023.67.1.010501.

[38] L.-J. Ouyang, B.-Q. Xie, and B. Ding, “Analytical Studies on Approximate Lag and Anticipating Synchronization in Two Unidirectionally Coupled Hyperchaotic Chen Systems without Time Delay,” Applied Sciences, vol. 13, no. 21, p. 11949, 2023, doi: 10.3390/app132111949.

[39] R. Smidtaite, J. Ragulskiene, L. Bikulciene, and M. Ragulskis, “Hyper Coupled Map Lattices for Hiding Multiple Images,” Complexity, vol. 2023, 2023, doi: 10.1155/2023/8831078.

[40] S. kumar, R. kumar, S. kumar, and S. Kumar, “Cryptographic construction using coupled map lattice as a diffusion model to enhanced security,” Journal of Information Security and Applications, vol. 46, pp. 70–83, 2019, doi: 10.1016/j.jisa.2019.02.011.

[41] Z. Li and S. Ravela, “Neural Networks as Geometric Chaotic Maps,” IEEE Trans Neural Netw Learn Syst, vol. 34, no. 1, pp. 527–533, 2023, doi: 10.1109/TNNLS.2021.3087497.

[42] N. T. Nguyen, T. Bui, G. Gagnon, P. Giard, and G. Kaddoum, “Designing a Pseudorandom Bit Generator with a Novel Five-Dimensional- Hyperchaotic System,” IEEE Transactions on Industrial Electronics, vol. 69, no. 6, pp. 6101–6110, 2022, doi: 10.1109/TIE.2021.3088330.

[43] C. Chen, K. Sun, and S. He, “A class of higher-dimensional hyperchaotic maps,” Eur Phys J Plus, vol. 134, no. 8, 2019, doi: 10.1140/epjp/i2019-12776-9.

[44] M. Hamdi, J. Miri, and B. Moalla, “Hybrid encryption algorithm (HEA) based on chaotic system,” Soft comput, vol. 25, no. 3, pp. 1847–1858, 2021, doi: 10.1007/s00500-020-05258-z.

[45] V. Chikkareddi, A. Ghosh, P. Jagtap, S. Joshi, and J. Kanzaria, “Hybrid Image Encryption Technique Using Genetic Algorithm and Lorenz Chaotic System,” ITM Web of Conferences, vol. 32, p. 03009, 2020, doi: 10.1051/itmconf/20203203009.

[46] H. M. Al-Saadi and I. S. Alshawi, “Efficient and secure hybrid chaotic key generation for light encryption device block cipher,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 31, no. 2, pp. 1032–1040, 2023, doi: 10.11591/ijeecs.v31.i2.pp1032-1040.

[47] B. Kharabian and H. Mirinejad, “Synchronization of Rossler chaotic systems via hybrid adaptive backstepping/sliding mode control,” Results in Control and Optimization, vol. 4, no. May, p. 100020, 2021, doi: 10.1016/j.rico.2021.100020.

[48] B. Emin and Z. Musayev, “Chaos-based Image Encryption in Embedded Systems using Lorenz-Rossler System,” Chaos Theory and Applications, vol. 5, no. 3, pp. 153–159, 2023, doi: 10.51537/chaos.1246581.

[49] V. Kumar and A. Girdhar, “A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach,” Multimed Tools Appl, vol. 80, no. 3, pp. 3749–3773, 2021, doi: 10.1007/s11042-020-09854-x.

[50] Y. Chen, S. Xie, and J. Zhang, “A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map,” Entropy, vol. 24, no. 2, pp. 1–28, 2022, doi: 10.3390/e24020287.

[51] M. Heshmat, “Video Encryption Technique Based on Hybrid Chaotic Maps and Multi-Operation keys,” Information Sciences Letters, vol. 11, no. 6, pp. 2197–2207, 2022, doi: 10.18576/isl/110627.

[52] S. M. Ali Ebrahim, “Hybrid Chaotic Method for Medical Images Ciphering,” International Journal of Network Security & Its Applications, vol. 12, no. 6, pp. 1–14, 2020, doi: 10.5121/ijnsa.2020.12601.

[53] N. H. M. A. Omar Khalid Dheyab, “Secure File Storage in Cloud Computing Based On Hybrid Cryptosystem Algorithm,” Solid State Technology, no. Vol. 63 No. 6 (2020), 2020.

[54] N. H. Ghayad and E. A. Albahrani, “A Combination of Two-Dimensional Hénon Map and Two-Dimensional Rational Map as Key Number Generator,” 1st International Scientific Conference of Computer and Applied Sciences, CAS 2019, no. 2, pp. 107–112, 2019, doi: 10.1109/CAS47993.2019.9075731.

[55] C. Wang and Q. Ding, “A class of quadratic polynomial chaotic maps and their fixed points analysis,” Entropy, vol. 21, no. 7, 2019, doi: 10.3390/e21070658.

[56] C. Li et al., “Deep learning-based security verification for a random number generator using white chaos,” Entropy, vol. 22, no. 10, pp. 1–15, 2020, doi: 10.3390/e22101134.

[57] K. B. Sudeepa, G. Aithal, V. Rajinikanth, and S. C. Satapathy, “Genetic algorithm based key sequence generation for cipher system,” Pattern Recognit Lett, vol. 133, pp. 341–348, 2020, doi: 10.1016/j.patrec.2020.03.015.

[58] L. Moysis et al., “Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption,” Entropy, vol. 22, no. 4, 2020, doi: 10.3390/E22040474.

[59] U. Menon, A. Hudlikar, and A. R. Menon, “A Novel Chaotic System for Text Encryption Optimized with Genetic Algorithm,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 10, pp. 34–40, 2020, doi: 10.14569/IJACSA.2020.0111005.

[60] Z. Rahman, X. Yi, I. Khalil, and M. Sumi, “Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security,” Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, vol. 402 LNICST, pp. 177–193, 2021, doi: 10.1007/978-3-030-91424-0_11.

[61] C. Ismayil Siyad and S. Tamilselvan, “Chaotic deep neural network based physical layer key generation for massive MIMO,” International Journal of Information Technology (Singapore), vol. 13, no. 5, pp. 1901–1912, 2021, doi: 10.1007/s41870-021-00751-6.

[62] H. Wei et al., “Chaotic key generation and application in OFDM-PON using QAM constellation points,” Opt Commun, vol. 490, no. March, p. 126911, 2021, doi: 10.1016/j.optcom.2021.126911.

[63] N. M.K and R. K.R, "Secured Key Generation for Biometric Encryption using Hyper-chaotic Map and DNA Sequences," SSRN Electronic Journal, no. Icicnis, pp. 585–595, 2021, doi: 10.2139/ssrn.3769813.

[64] D. Shah, T. Shah, I. Ahamad, M. I. Haider, and I. Khalid, "A three-dimensional chaotic map and their applications to digital audio security," Multimed Tools Appl, vol. 80, no. 14, pp. 22251–22273, 2021, doi: 10.1007/s11042-021-10697-3.

[65] M. D. Al-Hassani, "A Novel Technique for Secure Data Cryptosystem Based on Chaotic Key Image Generation," Baghdad Science Journal, vol. 19, no. 4, pp. 905–913, 2022, doi: 10.21123/bsj.2022.19.4.0905.

[66] V. Churchill and D. Xiu, "Deep Learning of Chaotic Systems From Partially-Observed Data," Journal of Machine Learning for Modeling and Computing, vol. 3, no. 3, pp. 97–119, 2022, doi: 10.1615/jmachlearnmodelcomput.2022045602.

[67] X. Zhang, G. Li, J. Zhang, A. Hu, and X. Wang, "Enabling Deep Learning-based Physical-layer Secret Key Generation for FDD-OFDM Systems in Multi-Environments," vol. XX, no. Xx, pp. 1–16, 2022, doi: 10.1109/TVT.2024.3367362.

[68] M. Irfan et al., "Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM)," Electronics (Switzerland), vol. 9, no. 1, 2020, doi: 10.3390/electronics9010104.

Studying Cloud Computing Offloading Using Machine Learning Strategies

Hiba A. Tarish [1]

Alaa Q. Raheema [2]

Abstract

Sophisticated messaging networks require many advances in source priority applications that can be suggested to multiple clients. Although peripheral equipment is increasingly "used," nearby and accessible supplies cannot cope with the necessities of such applications. Figure 5 shows various kinds of shapes used to stabilize the internal alloy cells of the honeycomb model candidate for use in the experimental design. The idea of offloading cloud computing, such as reconstructing edge computing capabilities near branch machines at the edge of the network, has been recommended. In this study, an analysis will be presented on how well the edge and/or cloud integrates with the task offloading problem. Particular emphasis is placed on training the AI using optimal command moves that can be used to achieve the goals, imperatives, and various dynamic states of the start and end execution technique. A virtual environment will be simulated for the most important offloading operations to the cloud network along the application of machine learning techniques to classify the most important commands and instructions within the network to harmonize them with the units and parties of the cloud computer network. The classification efficiency of the data models used and the unpacking of tasks reached 99%, with an error rate not exceeding 0.15%.

Keywords: *Smart Homes, Artificial Intelligence, Intensity Sensors, Light Sensors, Shrewd Applications, Brilliant Home, Artificial Neural Networks (ANN) Internet of Things (IoT).*

http://dx.doi.org/10.47832/RimarCongress03-4

[1] Civil Engineering Department, University of Technology Baghdad, Iraq
hiba.A.tarish@uotechnology.edu.iq

[2] Civil Engineering Department, University of Technology Baghdad, Iraq
40345@uotechnology.edu.iq

1. Introduction

Because of the fast improvement of remote correspondence innovations, expanded reality, voice acknowledgment, picture acknowledgment, and mobile medical care are only a couple of the undeniably asset escalated and latency-sensitive applications and administrations that have arisen. These mobile applications have essentially expanded the interest for cloud-based registering and stockpiling resources for remote gadgets, normally given by cloud servers. Nonetheless, when errands are offloaded to the cloud, there is a ton of transmission inactivity since cloud servers are ordinarily sent over significant distances. As a result of this, mobile edge figuring, or MEC, is viewed as a powerful methodology for managing this issue. By conveying disseminated processing capacities at the edge of the far off association, MEC's focal standard is met. Remote gadgets can alleviate the issue of inadequate computational resources, speed up calculations, and ration energy by offloading them to edge servers. Perhaps of MEC's most significant innovation, calculation offloading, resolves the issues of restricted resources and low handling efficiency by appointing calculation serious assignments to MEC has at the network's edge. The course of errand offloading is affected by a few things, including the nature of remote correspondence and the resources accessible for calculation. In any case, forceful offloading of computational undertakings to edge servers will go along info transfer capacity in the network framework. The serious congestion in the uplink remote channel will essentially expand the transmission delay. Figure 1 shows a worked on variant of the Framework model for a MEC network with various WDs [1-3].

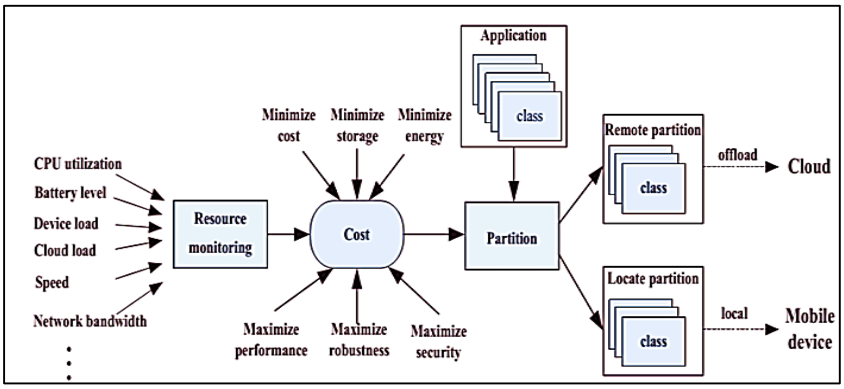


Figure 1: Cloud computing Offloading mechanism structure.

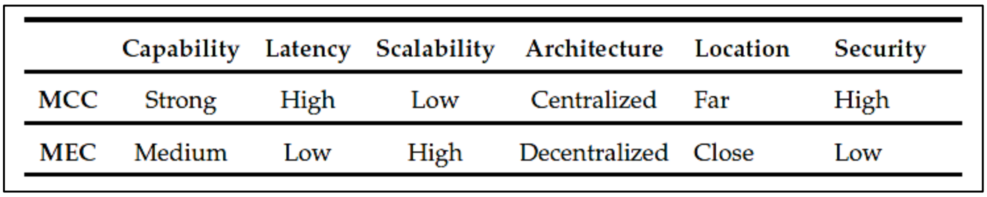
The vital issue of edge offloading is the means by which to settle on the most ideal choice. Calculation offloading and resource allocation are normally planned as blended whole sum programming nonlinear programming issues together. Heuristic or guess algorithms are the groundwork of most of the ongoing arrangements. Such arrangements, then again, depend on exact numerical models and master information. At the point when the MEC climate transforms, it frequently takes another begin to change the numerical models, which prompts wasteful offloading choices. These approaches have a generally elevated degree of computational intricacy. Therefore, fostering a period differing MEC network that utilizes a calculation of low intricacy stays a test. Offloading choices have as of late seen broad reception of deep learning. Deep learning offers a promising answer for the previously mentioned challenges on the grounds that a neural network is a black-box model that doesn't require exact master information or exact numerical models. Along steady experimentation, deep reinforcement learning figures out how to take care of intricate issues like chess, astute robot control, and computer games. Computational offloading in light of deep Q-learning (DQL) [4-7], which discretizes the state/activity space and uses web based figuring out how to upgrade choices with respect to computational offloading and framework resource optimization, as of now gets the most exploration consideration. Anyway, the discretization of consistent factors restricts the introduction of DQL and isn't sensible for overseeing high-layered movement spaces. Moreover, most of these methodologies depend on static, intelligent MEC conditions that give adequate preparation tests to neural networks. While joining to another scene, it is hard to assemble adequate preparation tests once the MEC scene has changed. Notwithstanding, given the dynamic idea of the offloading task, it is as yet worth researching how to combine with little examples to another scene rapidly. [5-10].

The literature contains a couple of studies on dynamic MEC networks. Huang and others [11-15] utilized time-differing remote channel gains and weight factors of computational tasks to create dynamic MEC situations and recommended a meta-learning-based calculation offloading (MELO) calculation to deliver a general model that can be quickly adjusted to new task situations involving few preparation tests in MEC situations. Wang and others [12-18] suggested a meta-reinforcement learning-based strategy to increment preparing efficiency and reduction test dependence and built dynamic task situations with various geographies. Unfortunately, the framework's energy utilization to accomplish low latency is overlooked in this exploration. Furthermore, the computational offloading calculation's meta-learning-based preparing operation is tedious. Furthermore, another model should be created to calculate the gradient at each preparation.

1.1. Offloading in Cloud Computing Networks

A means of giving computing resources and administrations is cloud computing (CC). A one-request foundation that empowers clients to get to computational resources at any time and from any location is alluded to as this. Organizations and clients the same advantage from CC in three fundamental ways: 1) huge computing resources are promptly accessible upon request; 2) capacity constantly and discharge depending on the situation; and 3) worked on administration and maintenance abilities are given. Along the Web, CC offers clients various applications as administrations. We can give Windows Sky blue and Amazon Web Administrations (AWS) as instances of public CC. Windows Sky blue is a cloud platform that is open and versatile. It offers a few administrations for creating, conveying, and running web applications and administrations in cloud data focuses [16]. As an illustration of a public computing instrument, AWS offers two models to clients: programming as a help and foundation as a help. These administrations license the client to use virtualized resources including server ranches. To use unconcerned computing dreams, the computational cloud executes an assortment of administration models [15, 16]. By and large, sending parts of computationally requesting applications to a far off server is known as "computational offloading." For mobile applications, a few calculation offload frameworks with various methodologies have as of late been suggested. To put it another way, offloading, otherwise called accelerating, is the method involved with moving computing tasks to PCs or frameworks that are made to do specific tasks more quickly than programs running on a broadly useful computer chip could. Thus, offloading is the most common approach of moving whole mobile applications or simply aspects of them to the cloud for quicker calculation [17-20]. Regularly, requests from clients running applications that point of interaction with the server utilizing frameworks are taken care of by specific servers (normally running a virtual machine). These servers choose to offload in view of various measures to lessen power utilization and additionally further develop execution. While utilizing frameworks and the cloud, security, execution, bandwidth, and cost ought to be generally considered for a successful offloading operation. The shortfall of a standard offloading framework, cross-platform compatibility, various network conditions, latency, and operating costs like bandwidth and capacity are extra obstructions. Also, in Table 1, a comparison of MEC and MCC has presented [18-20].

Table 1: MCC with MEC comparison [20]



	Capability	Latency	Scalability	Architecture	Location	Security
MCC	Strong	High	Low	Centralized	Far	High
MEC	Medium	Low	High	Decentralized	Close	Low

1.1.1. The Markov Decision Process Data Dump

Also called Finite Horizon Markov Decision Process (FHMDP). On the basis of the Finite Horizon Markov Decision Operation, we present two mobile data offloading strategies in this section. Our goal is to make it as cheap as possible to communicate mobile data with varying delay sensitivity across a variety of wireless networks, including the cellular network, the WiFi network, and D2D communication [16-22].

1.1.2. System Structure

Our model to further develop mobile cloud data offloading is introduced in this part. One could consider in such model that mobile devices could get to cloud administrations along different remote networks. (1) Remote network WiFi APs interface remote cloud foundation through a wired network and give MS pioneering WiFi communication, like WLAN; (2) A remote network For MS, cell base stations give consistent cell communication, for example, 4G, and associate by means of wired network to the cloud; (3). The D2D network MHs, like MHs An and B in Fig. 2.5. Furnish MS with crafty D2D communication and associate through WiFi or cell communication to local WiFi APs or BSs. Mobile partners are chosen to act as data suppliers for mobile endorsers in our data offloading model. Utilizing a micropayment plan or offering members a lower cost for the help, MNOs can urge MHs to participate in data offloading. In this section, we select the miniature installment conspire [18-23], in which MHs can participate in data offloading and get rewards. MNO decides the cost of communicating a data unit i.e., (4) Subsequent to declaring the cost to mobile clients, MNO chooses MHs from those clients who will participate in data offloading and acknowledge the cost. It is critical to take note of that this part doesn't zero in on a far reaching examination of this operation. A progression of data units make up the mobile data that MS gets from the cloud. MNO has proactively decided the data units. Data conveyance involves sending data to MS ahead of the cutoff time D, where K is the overallsum of data units and D is the greatest measure of time for data transmission. At the point when non-communicated data size k, i.e., the data size which has not been identified by MS is zero preceding D, the data conveyance is finished. Commonly, MS gets generally mobile data along cell communication without WiFi APs or MHs. Nonetheless, MS can decide to get a portion of the data in our model by means of neighboring WiFi or D2D communication, which might provide higher data rates at lower communication charges [18-25].

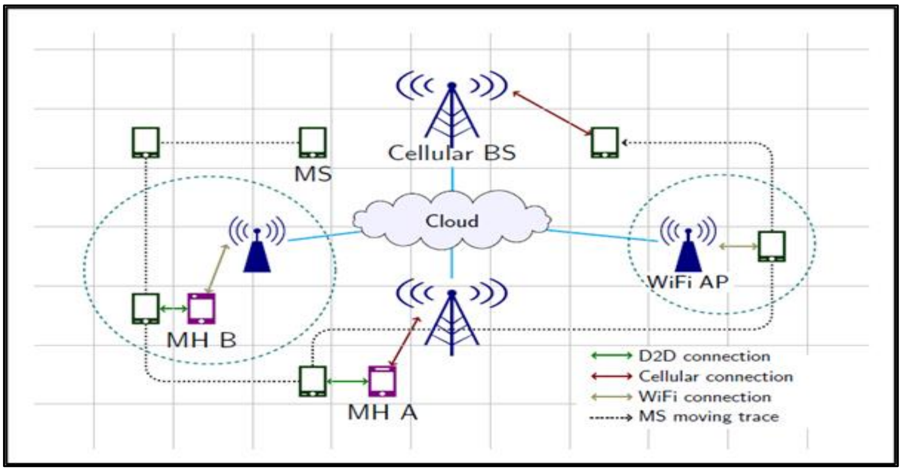


Figure 2: The Offloading model for portable scheme [22].

MNO decides, in light of data qualities and network execution, whether to send data by means of the cell network or offload it to WiFi and D2D networks after getting a data conveyance request from MS. The delay normal for compact data — whether or not it is delay open minded — decides the chance of offloading. MNO can delay data transmission to improve the probability of offloading on the off chance that data is delay-open minded. Since versatile data is delay-sensitive, MNOs will not have the option to offload compact data from cell networks as frequently otherwise. Furthermore, cell data offloading could abbreviate conveyance times for MNOs assuming WiFi and D2D network data rates are higher than cell network data rates. The primary thought behind data offloading is to search for chances to utilize WiFi and D2D networks by using the versatility of compact clients and the delay resistance of convenient data. We expect that MS could get at least one data unit from a cell, WiFi, or D2D network inside a time allotment T. At the start of each time allotment, an offloading choice, otherwise called choosing a network, is made. The time at which the choice to offload is made is indicated by d; The expression for it is choice age. Subsequently, a network is picked at every choice age to work during the time allotment [28]. MNO perceives the current plan cases, like the location of MS, the size of the non-communicated data, and the locations of conceivable MHs, at every choice age. MNO calculates the communication cost for potential networks in view of the perceived design state. The MNO then chooses whether to offload data to a different network, (for example, the WiFi or D2D network) or to communicate data over the cell network. To formulate this issue, we propose a Finite Skyline Markov Choice Cycle in this part. The objective is to offload however much versatile data as could be expected with the WiFi network and D2D communication to decrease communication costs and meet delay limitations. While pursuing sequential choices, for example, remote network determination, the Markov choice operation is a successful model. With a finite amount of choice ages, FHMDP is a Markov choice cycle [84]. FHMDP will design data offloading choices at every choice age on the grounds that every data conveyance task should be finished by a specific date. The FHMDP arranging stage can be utilized in the remote cloud to alleviate MS's significant weight of overseeing complex data offloading. It is critical to take note of that the base station and the WiFi APs are both stationary, while the MHs are moving inside the base station's inclusion region. Because of their versatility, MHs can be viewed as a supplement to WiFi APs..

1.2. Problem Statement

The problem of offloading portable data is formulated as an FHMDP problem in this section. The notations used throughout this chapter are displayed in Table 2.3. Portable data is initially delivered to one or more MSs in our model via WiFi and cellular networks. D2D communication also allows any MH that carries a copy of the data to opportunistically transmit it to MSs. MNO will select a remote network for each MS at each decision epoch D2D = f_1; data of size K must be transmitted by deadline D for each MS according to the presentstate of the structure [18-23].

$$. d \in D = \{1, \dots, D\} \tag{1}$$

In fact, the mathematics of this strategy is very difficult and complex, as it depends on the theories of probability and statistics, and therefore we will try to reduce mathematical complexity as much as possible by providing an explanation and clarification of the idea and methods used while shortening the mathematical difficulties as much as possible. The following is the definition of the model state for multiple MSs and MHs:

$$\mathrm{s} = (\mathcal{M}, \mathcal{H}) \tag{2}$$

where the sets of states for MSs and MHs are $\mathcal{M}$ and $\mathcal{H}$, respectively. In other words and More precisely;

$$\mathcal{M} = \left\{\mathrm{m_i}, \mathrm{i} \in \{1, \dots, \mathrm{M}\}\right\} \tag{3}$$

contains all MS states in which;

$$\mathrm{m_i} = (\mathrm{l_i}, \mathrm{u_i}, \mathrm{k_i}) \tag{4}$$

Such that, mi , hints at the potential state of MS i; the position of MS, i is indicated by li, the client's kind by ui, and the data's size by ki. Also, $\mathcal{H}$, represents the set that contains all the positions of MHs, such that:

$$\mathcal{H} = \left\{\mathrm{l_j}, \mathrm{j} \in \{1, \dots, \mathrm{N}\}\right\} \quad (5)$$

Such that the position of MH j is l_{j} .

We simplify by omitting the subscripts i and j of the state components l, u, and k in the following section. $l \in \mathcal{L}$ is the state parameter $\mathcal{L} = \{1, \dots, L\}$; The index of the grid (or position) is $\mathcal{L}$, where L is the sum of grids that MSs might reach before D. We assume that the cellular network can cover all grids seamlessly. At decision epoch d, all grids are divided into four distinct categories based on the sum of WiFi or D2D connections that are possible. The grids that are only covered by the cellular network are shown in $\mathcal{L}_d^1$, the grids that are covered by both the cellular and WiFi networks are shown in $\mathcal{L}_d^2$, the grids that are covered by both the cellular network and D2D communication are shown in $\mathcal{L}_d^3$, and the grids that are covered by both the cellular network and D2D communication are shown in $\mathcal{L}_d^4$. $\mathcal{L}_d^2$, $\mathcal{L}_d^3$, and $\mathcal{L}_d^4$. change over decision epoch d because of the mobility of MHs. The state parameter $u \in \mathcal{U} = \{1, \dots, U\}$; The portable client kind (loose delay or tight delay, for example) is represented by $\mathcal{U}^1$, and the sum of various client kinds is represented by $\mathcal{U}$. We think that various kinds of clients have various delay needs, which means that various deadlines will apply. We consider two sets of client kinds, each with distinct QoS demands, to simplify the model. More specifically, set $\mathcal{U}^1$ contains delay-sensitive client kinds; Set $\mathcal{U}^0$ contains the other kinds, such as software updates. Therefore, U = $\mathcal{U}^0 \cup \ \mathcal{U}^1$, [20-30]

We divide the data that needs to be sent into K equal parts; the state variable k $\in \mathcal{K} = \{1, \dots, K\}$; The sum of data parts that still need to be sent is called $\mathcal{K}$. The data delivery operation is complete if k = 0 when $d \in D$ occurs.

The action space of MNO in the portable data offloading model is then presented, following the definition of the FHMDP model state. MNO selects one of the data transmission offloading actions at each decision epoch. The action space contains four actions that correspond to four decisions about offloading. Formally, $a \in \mathcal{A}$ action equals $\mathcal{A}$={1,2,3,4};: (1) The waiting action is a = 1.

MS will hold off until it is possible to receive data from the D2D or WiFi networks; (2) (cellular action) a = 2; 3) (WiFi action) a = 3 Moreover, a equals 4 (D2D action): MS can, respectively, receive data from a WiFi network, a cellular network, and a D2D connection.

D2D action occurs when MS is able to access a nearby MH, and WiFi action occurs when MS is in WiFi coverage. As a result, the possible actions are influenced by the state parameter

l. Additionally, we notice that the portable client kind u has an effect on the possible actions; for instance, the D2D action is not possible for delay sensitive data due to the low data rate. $\mathcal{A}$ (l; u) ⊆ $\mathcal{A}$. The following is the definition of $\mathcal{A}$, which represents the set of actions that are possible at grid *l* for data of kind *u* , [20-30]:

$$\mathcal{A}(l.u) = \begin{Bmatrix} \{1,2\} & l \in \mathcal{L}_d^1, u \in \mathcal{U} \\ \{1,2,3\} & l \in \mathcal{L}_d^2, u \in \mathcal{U} \\ \{1,2,4\} & l \in \mathcal{L}_d^3, u \in \mathcal{U}^0 \\ \{1,2,3,4\} & l \in \mathcal{L}_d^4, u \in \mathcal{U}^0 \end{Bmatrix} \qquad (6)$$

1.3. Computing Structures

The computing structure is divided into three basic catigories: Local Computing Edge Computing Communication Structure which might be explained as below.

1.3.1. Local Computing

If the agent decides to operate the mission, $u_m(t)$, at MD, m, at slot t, then the mission will be queued up and processed at subsequent slots for the client, m. We use $\varphi_m^{loc}(t)$ to specify the time slots sum before $u_m(t)$ might be completed, and $\varphi_m^{loc}(t)$ shows whenever the mission is finished or thrown. If it is not finished by the deadline, the following is how $\varphi_m^{loc}(t)$ is calculated for task $u_m(t)$:

$$\varphi_m^{loc}(t) = \max_{t' \in \{0,1,,t-1\}} L_m^{loc}(t') - \mathrm{t} + 1 \qquad (7)$$

It goes without saying that the preceding tasks, $u_m(t)$, are dependent on $\varphi_m^{loc}(t)$, and once all of them have been completed or dropped, um(t) will be processed at t + on t+$\varphi_m^{loc}(t)$. In addition, the overallcalculation delay between reaching the MD, m, and being finished or dropped Is represented by on $L_m^{loc}(t)$; It is estimated to be [22-35]:

$$L_m^{loc}(t) = min \begin{Bmatrix} t + \varphi_m^{loc}(t) + \dfrac{\lambda_m(t)}{\frac{f_m \mu}{\xi_m}} - 1, \\ t + \pi_m - 1 \end{Bmatrix} \qquad (8)$$

Where f_m represents the MD capacity of CPU processing, *m*, and x_m represents the CPU cycles, MD, *m*, needed for processing unit information [20-26].

1.3.2. Edge Computing

One could define L_{edge}, $L_{m,n}^{edge}(t)$, $u_m(t)$ to indicate when a task is executed or dropped by the service when it is offloaded to ED n for processing. Until the task processing is finished, the figure of Ledge $L_{m,n}^{edge}$ (t) is unclear due to the queue dynamic of ED n and the MD, m. Let m, n, and *t* denote the point at which the task begins to be processed:

$$L_{m,n}^{edge}\ (t)\ = max\left\{t, \max_{t'\in\{0,1,,t-1\}} L_{m,n}^{edge}\ (t') + 1\right\} \tag{9}$$

It is assumed that the MEC servers have sufficient computing power. As a result, the servers can handle a variety of tasks sent from various MDs. That is to say, there will be no waiting in the queue because the tasks will be carried out as soon as they reach the MEC servers.

1.3.3. Communication Structure

In this study, we assume that portable devices communicate over orthogonal channels in a remote network. Let P represent the client's transmission power, and denote $h_{m,n}$ as the uplink channel gain between the client m and the ED n. The following formula is used to determine the model to offload um(t)'s uplink transmission rate in bits per second:

$$r_{m,n}^{trans}(t)\ = Wlog\left(1+\frac{h_{m,n}^2 P}{\sigma^2}\right) \tag{10}$$

Such that σ^2 is the noise power at the edge server and W is the bandwidth of the channel. We denote $\varphi_m^{trans}(t)$ to define the sum of time slots that the task, $u_m(t)$, will wait for transmission after being placed in the transmission queue at time slot t; When the task has been completely transmitted or dropped if it has not been transmitted by the deadline, the $L_m^{trans}(t)$ symbol is used. The following is how $\varphi_m^{trans}(t)$ is calculated for task $u_m(t)$:

$$\varphi_m^{trans}(t)\ = \max_{t'\in\{0,1,,t-1\}} L_m^{trans}(t') - \mathrm{t} + 1 \tag{11}$$

Moreover, $L_m^{trans}\ (t)$, is evaluated as below:

$$L_m^{trans}\ (t)\ = min\left\{\begin{matrix} t, \varphi_m^{trans}(t) + \dfrac{\lambda_m(t)}{r_{m,n}^{trans}(t)} - 1, \\ t+\pi_m - 1 \end{matrix}\right\} \tag{12}$$

Task data and calculation results are transferred between MDs and EDs as part of the offloading operation. We disregard the transmission delay between the BS and MEC servers because wire lines ensure much faster transmission speeds than remote channels [22-35].

2. Literature Review

The latest articles as well as exploration articles lodging the name of the review are recorded as underneath: (In 2013) Roberto B. Al [11] managed offloads from portable devices to a remote or close by cloud, and the emphasis was on offloads on a case by case basis rather than permanent offloads on remote machines in the cloud, where some offloads should be possible on neighboring devices as per demands, where the trial was directed On the round of chess, the outcomes depended on energy and time essentially on the level of intricacy in the tasks and the limit of the gadget utilized, and the initial steps of the arrangement were: automating the choice as per the required intricacies and estimating it with the limit of the objective gadget and lessening the general utilization of resources. In (2014) Shuguang Deng et. al [12] study was finished on cloud computing improvement cycles and how to control compelled resources by permitting them to offload computational parts, complete demands, and settle on offload choices. Genetic Algorithm (GA) was utilized to arrive at the best outcomes to meet the needs, and the outcomes were practically amazing notwithstanding the intricacy of the algorithm. 2014, Mohammad Shiraz. et. al [13] studied mobile computing and the latest advancements in this field, and the starter discoveries are that smart mobile devices (SMDS) are still of low limit. This is on the grounds that AMDS utilizes smartphone applications to offload the cloud (MCC) widely, and the outcomes are that assuming dynamic data is migrated to the cloud, a great deal of force and transmission is saved in the network. In (2015) Bowen Zhou et. al., [14] presented a concentrate on Mobile Cloud Computing (MCC) and showed the significance gained during those years. A functioning prototype of the custom cloudlet framework is suggested and an algorithm is adjusted to the needs to choose to drop the stacking and dumping site as indicated by the hardware needs. Genuine tests were directed to evaluate the presentation of the algorithm and accomplish execution improvement. In (2015) Xu Chen et. al.,. [15] They led a concentrate on multi-cloud offloading for clients in cloud computing, embraced a strategy to understand the offloading in a dispersed manner, determined the offloading algorithm that can accomplish balance, and suggested a conscious offloading algorithm. In (2015) Xu Chen. et. al., [16] composed a review that incorporates the possibility that cloud computing is a high level and highly effective methodology that can be taken to build the capacities of mobile devices and proposes the best for the circulation cycle by formulating a decentralized record that can pursue choices in the mobile conveyance operation. The suggested mechanism accomplished viable outcomes as well as expanding the volume of the framework. In (2016) Songtao Guo et. al., [17] They directed a concentrate on mobile cloud computing (MCC), as it has a great potential to upgrade mobile devices and save energy by eliminating resource-escalated calculation tasks, and the (eDors) dynamic dump algorithm was utilized to diminish energy utilization by utilizing a document to decrease efficiency, the consequences of energy cost were (EEC) is successful inside expectations by improving the computer processor clock in light of dynamic voltage and frequency. In (2017), Daniela Mazza., et. al., [18] directed a review that showed that the extension of civilization and the expansion in population made the world a smart city, and this additional a weight on engineers to create smart applications that serve this objective, yet another imperfection showed up here concerning resources and spots. The capacity to stay up with this turn of events, which made us critically need to tackle this emergency utilizing cloud computing and how to control dumping processes by zeroing in on a brought together burden mechanism in communications and computing resources that are mutually figured out how to adjust the heap between various elements in the climate. In (2018) ,Dianchao Zheng., et. al., [19] led a concentrate on the computational force of mobile devices and decreased power utilization and release for cloud computing, and an algorithm was recommended in a dynamic climate as an irregular game containing Nash equilibrium (NE), and the algorithm was simulated to guarantee the viability of the email algorithm and the outcomes showed a benefit in execution. In (2020) B. Wang, et al., [20] led a review to address the resource lack of smart devices considering the fast improvement of programming with dumping tasks, deciding the overall setting of execution of each task, booking tasks, evaluating resource needs, decentralizing stacking and info reserving, and utilizing numerous clouds in a cloud layer, It is a study search. In (2020), Ali Charkaram., et al., [21] directed a concentrate on smart devices, IoT networks, and various applications like VR, UR, and GPS frameworks that need increasingly more extra room and resources. Unloading is a promising method for taking care of such an issue by moving the code or part of it to local servers wealthy in resources. Classification has been divided into three fundamental regions; Markov chain, Markov process, and secret Markov models. Furthermore, they made tables to think about the outcomes and the issue was the irregular dumps. In (2020), Adam Parker., et al., [22] introduced a concentrate on Sensor Networks (WSN) by following the Q-Directing algorithm zeroing in on the versatility of the Network (WSN) with the expansion of the EAQCO algorithm and this expansion prompted the improvement in both investments. The aftereffect of the investigations was that the EAQCO algorithm is helpful when time, energy, and computational capacity are basic factors. In (2020), Jaydip Kumar., et.

al., [23], recommended a vowing against unpredictable cut of the high techniques for info security therefore, the whole development has been gotten. Such an article affirmed that inadequate recording is harmed by a significant amount of people of the relation for premium for the hazes high info rate. As needs be, there is an interest to accomplish the info that could as texture, voice, video, and so forth.. Various strategies coordinated by the controllers for acquiring the cloud info. In (2021), Sheng Zhi Hoang., et al., [24] led a concentrate on the accessibility of multi computing, that is, the sending of sophisticated servers in the network limits, and this helped in mitigating resource limitations and offloading weighty tasks, and they created utilizing deep reinforcement learning techniques. The innovation has kept resources productive and conveyed tasks among high-end servers to support limit. In (2021), Shuchen Zhen, et al., [25] led a strategic investigation to concentrate on edge computing task offloading. An AI approach was utilized in view of the examination of curved and sunken properties utilizing an iterative optimization algorithm. The tests performed well to diminish the energy utilization of the computation dump, and the model had high efficiency and a high degree of exactness. In (2021), Saif ALjanabi, et. al., [26] They did a concentrate on the fast improvement of devices and the Web of Things (IOT), and they found that they need to furnish these devices with high capacities, and this is what makes it pricey, so they made a half and half innovation among haze and cloud (HFCO) in which it is chosen to offloading to a cloud server or to local fluffy hubs The issue was formulated Markov choice (MDP) strategy, and utilizing (Q-Learning) algorithm to settle the model and pick the offload technique, and the outcomes were superb in the field of lessening the deferral, adjusting the heap and expanding the execution of tasks .In 2018, Y. Simulated intelligence, M. Peng, and K. Zhang, et. al., [27], reviewed the improvement of conveyed handling so as to stay mindful of the information and its implementation by utilizing a focal far off server against the web association. A client could set aside cash by utilizing appropriated figures since there is no great explanation for them to purchase their own product and hardware. Regardless, dispersed registration truly disapproves of protections, similar to security techniques and the misfortune and theft of information. Clients use attacks to bypass a part of cloud organizations' safety efforts, like authenticity, receptiveness, and mystery. This study gives an outline of a portion of the issues and its ongoing plans. W. Z. Khan, et al. in 2019 et., al., [28] inspected a thorough layout of the right now existing piece for appropriated figuring security issues and blueprints. The writers of this article recommend a design for appropriated enrolling security near the end. This study gives an outline of various dangers and plans for the appropriated registration climate with regards to security and assurance of client explicit information in the cloud. The circulated figuring layers plans are additionally the subject of the review zeroing in on the security need. Involving protection demands in VANET, L. Mendiboure, M.- A. Chalouf, and F. Krief present a quick and dreadful graph of first class security in 2019 [29]. What's more, a depiction of the various VANET attacks considering the correspondence structure stages is given in this review, similar to the short strategies that are recommended in the article to satisfy these demands. What's more, the various VANET adversaries that can be utilized against aggressors are talked about here. In light of everything, the objective of this paper is to give valuable information about VANET security and confirmation with the goal that it very well may be utilized as an instrument to help specialists in this field in creating safe protection saving strategies for VANET. In 2019, M. Maray and others et. al., [30], introduced a study that initially digs into the plan of the conveyed handling, then examines the most normally seen security concerns associated with utilizing the cloud and a couple of manages any consequences of these worries. Security is one of the main parts of disseminated registration because of the responsiveness of client info.

Investigating accessible project offloading strategies in IoT cloud networks and channel interference problems. Also, studying the characteristics of the communication channel and external signals with various frequencies that are responsible for this problem. The study aims to effectively change the characteristics of the transmitter and receiver signal in cloud networks to get rid of the interference problem..

3. Methodology

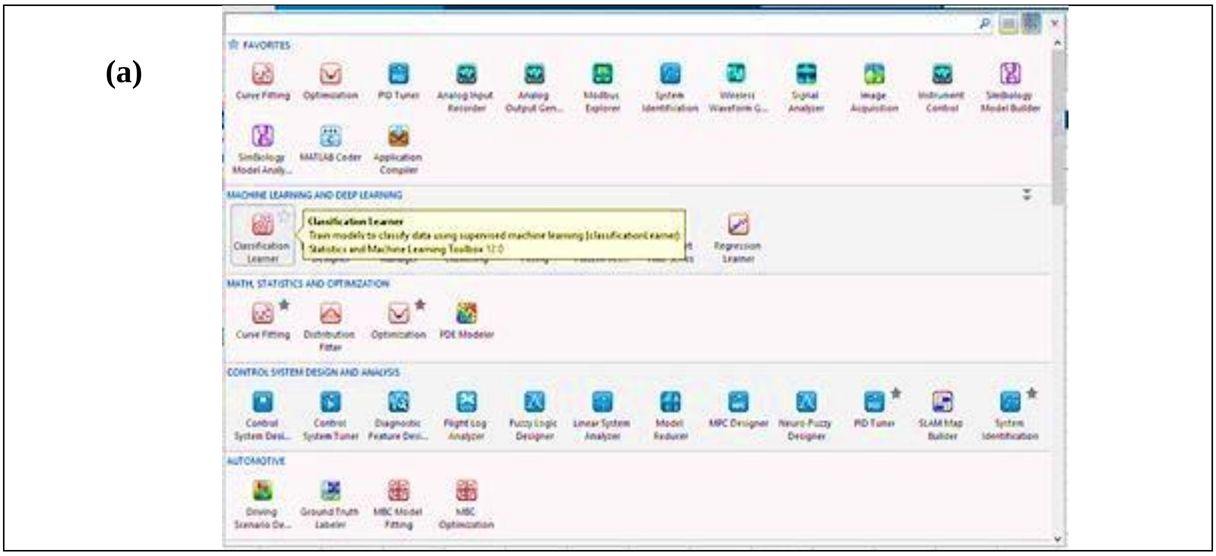
In this part, the representation and simulation of the recommended cloud network offloading model that is customized to be employed to address the study problem will be presented. In this recommended model, we try to address the problem of offloading multiple network tasks along the operation of smart sensors, their readings, and the necessary energy consumption by implementing smart techniques to inspect and control the readings and estimates from these smart sensors along the cloud network. First, the dataset stacked from sites and have been exhibited in Figure 3.

Table 2: Dataset of the recommended cloud computing offloading scheme.

NETWORK STATE									STATE
Security	Delay	Mobility	Data Size	Model	Position	Capability	Scalability	Coverage Area	Category
2	1	0	2	0	2	2	2	2	1WiFi
2	1	0	2	1	2	2	2	2	1WiFi

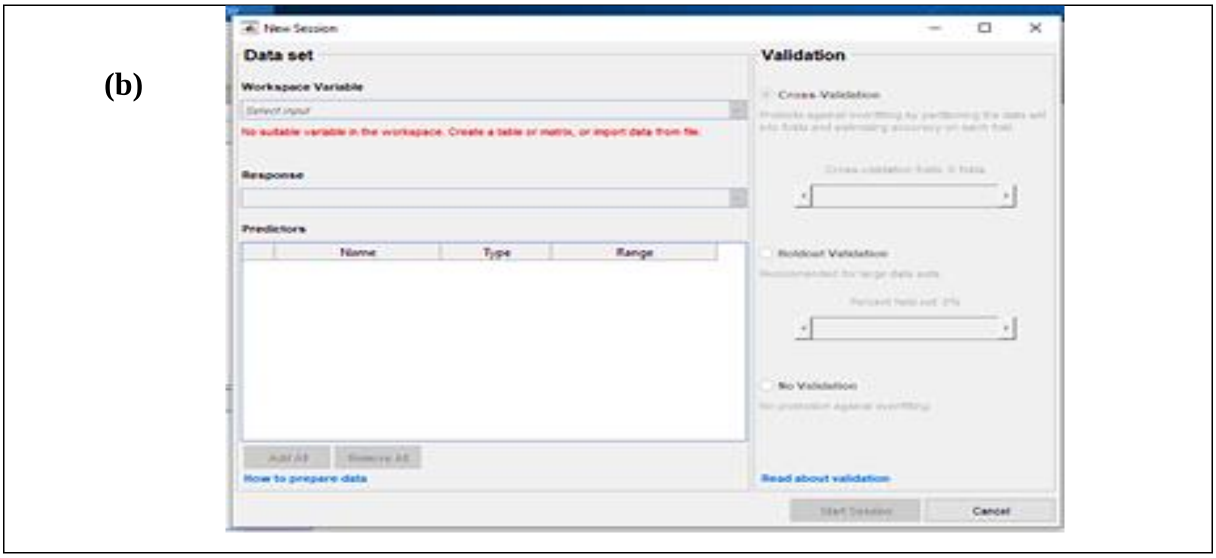
1	2	3	1	0	2	2	2	1	2D2D
2	1	1	2	1	2	2	2	2	1WiFi
2	1	1	2	0	2	2	2	2	1WiFi
1	2	3	1	0	2	2	2	1	2D2D
3	3	1	0	2	3	3	1	0	3MCC
1	2	3	1	1	2	2	2	1	2D2D
3	3	0	0	2	3	3	1	0	3MCC
3	3	0	1	2	3	3	1	0	3MCC
1	1	1	1	1	1	2	3	1	4MEC
3	3	1	0	2	3	3	1	0	3MCC
3	3	1	1	2	3	3	1	0	3MCC
3	3	0	0	2	3	3	1	1	3MCC
2	1	1	2	0	2	2	2	2	1WiFi
3	3	1	0	2	3	3	1	1	3MCC
3	3	1	1	2	3	3	1	1	3MCC
1	1	0	0	1	1	2	3	0	4MEC
1	1	0	1	1	1	2	3	0	4MEC
1	1	1	0	1	1	2	3	0	4MEC
2	1	1	2	0	2	2	2	2	1WiFi
1	1	0	0	1	1	2	3	1	4MEC
3	3	1	0	2	3	3	1	1	3MCC
1	1	1	0	1	1	2	3	1	4MEC
1	2	3	1	1	2	2	2	1	2D2D

The datasets have been prepared and modeled in order to justify the recommended model demands and objectives. Such that, they consist of coloumns representing the offloading case or state indication (such as; mobility, coverage area, delay, data size, model, position, capability, scalability, and security) or each kind or network category as shown in Table 2. the offloading case or state will be indicated such that; Low=1, Medium=2, High=3, and Non=0, for each network kind. All the possible situations of the offloading case or state have been regarded and the dataset has been loaded to MatLab2020b simulation program using the importing data utility. Figure 3.1 shows the dataset loading screen shoot after imported to the program. Thus, the imported offloading datasets, as depicted in Figure 3, represent readings of the offloading states for each network category, including all possible combinations that have been provided and recorded. The next step is to adapt these readings to the MatLab2020b programming format to make the necessary encryptions and processing simpler. In fact, when the classifier learner utility is employed, the MatLab2020b software provides powerful machine learning algorithms like fine trees, SVMs, and KNNs. Figure 4 introduces a screen shoot of the classifier student utility used to carry out the recommended AI calculations.



Classification Learner
Train models to classify data using supervised machine learning (classificationLearner)
Statistics and Machine Learning Toolbox 12.0

Figure 3: ?????????????????????????



Data set

Workspace Variable

Select input

No suitable variable in the workspace. Create a table or matrix, or import data from file.

Response

Predictors

	Name	Type	Range

How to prepare data

Validation

○ Cross-Validation

Protects against overfitting by partitioning the data set into folds and estimating accuracy on each fold.

Cross-validation folds: 5 folds

○ Holdout Validation

Recommended for large data sets

Percent held out: 25%

○ No Validation

No protection against overfitting

Read about validation

Figure 4: Results of the classifier learner utility utilized to implement the suggested machine learning algorithms, (a) Applications starting screen, (b) Classification learner utility window.

By considering Figure 4, one might observe the starting window utilized to open the classification learner utility from the application option provided be MATLAB2020b programming language. Moreover, the classification learning tool window has been illustrated in Figure 4. (b), such that all the necessary machine learning techniques are possible. Next, the flow chart of the suggested cloud computing offloading model methodology will be depicted in Figure 5.

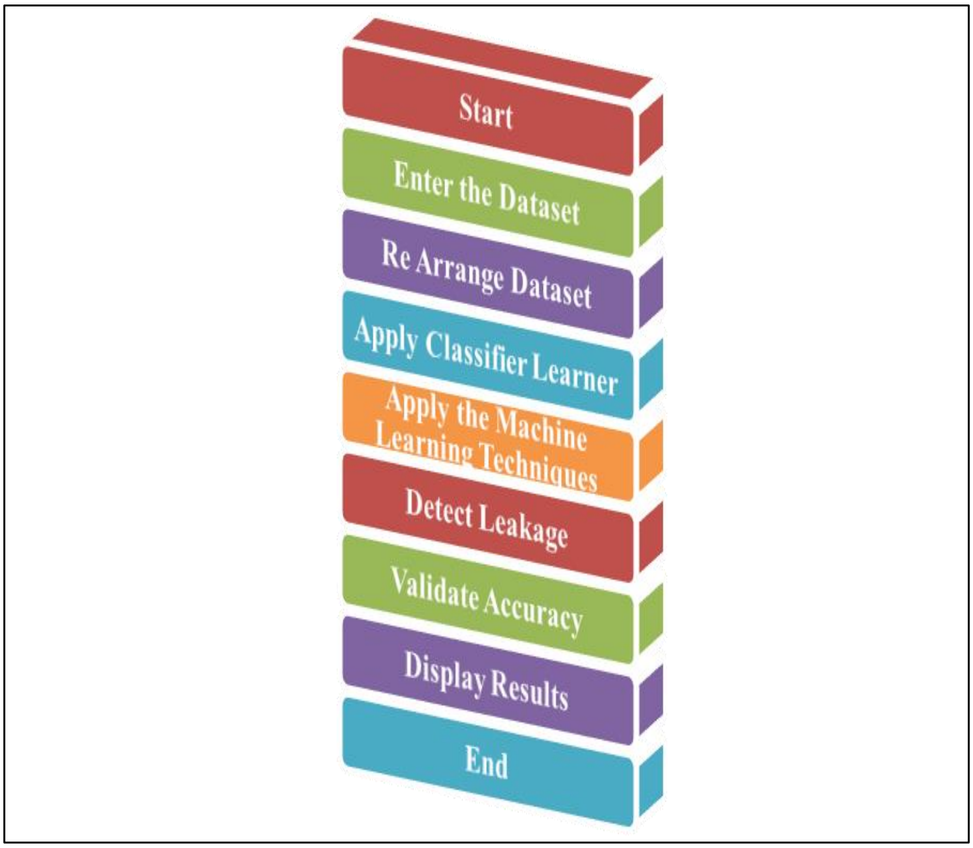


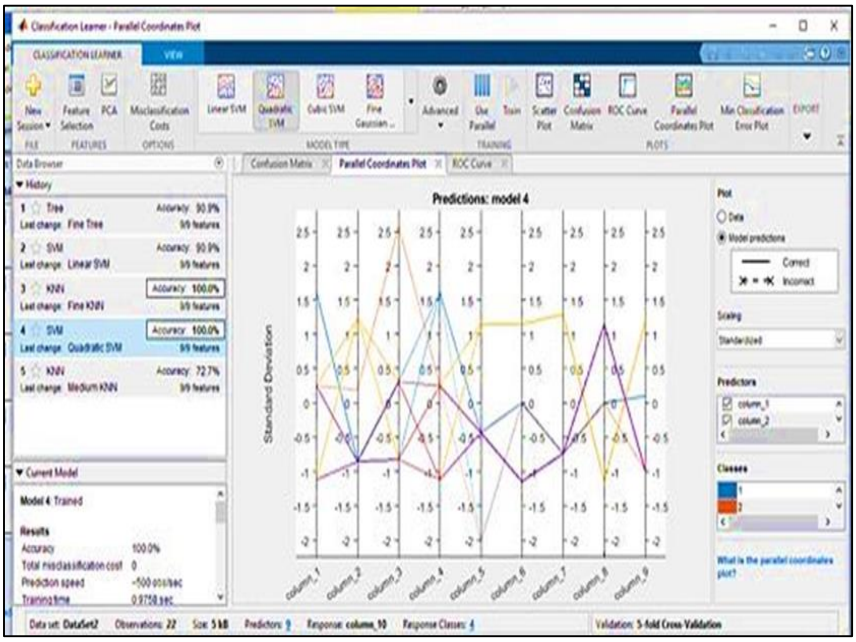
Figure 5: Methodology flow chart of the recommended offloading cloud computing scheme.

From Figure 5, the method of the recommended model will begin and initiated by setting up the datasets and read the utilizing the Read the Dataset choice utility. Then, the Classifier Student will be utilized that will give the essential AI programming devices. From that point onward, the AI Methods will be applied utilizing this classifier student utility with the end goal that the stacked datasets will be prepared to track down the reasonable outcomes. Moreover, the Recognize Spillage choice will really look at the places of spillages in the prepared datasets lastly the exactness of the spillage discovery will be acquired from the grouping and preparing aftereffects of the AI calculations activity. Finally, the program will really take a look at the general advances and closures the handling. Thus, the results of the suggested model will be the ability of the cloud computing network of determining to the correct and suitable network kind according to the offloading states provided by the task given in the dataset information. Also the obtained accuracy of the employed machine learning techniques will be considered as program outcomes.

As a result, the suggested model's output will be the cloud computing network's capacity to select the appropriate network kind based on the task-specific offloading states in the dataset information. Likewise the got precision of the utilized AI strategies will be considered as a program results.

4. Results & Discussion

By implementation of the suggested "distributed computing offloading" model according to the design specifications and needs illustrated previously in Section 2, the results of the classifier learner have been recorded for each kind of the examined machine learning technique (i.e. SVM, FT, and KNN). The best machine learning algorithm to be examined according to the entered datasets was the SVM machine learning (ML) algorithm with results of this training has shown in Figure 6.



History

1 Tree — Accuracy: 90.9%
Last change: Fine Tree — 9/9 features

2 SVM — Accuracy: 90.9%
Last change: Linear SVM — 9/9 features

3 KNN — Accuracy: 100.0%
Last change: Fine KNN — 9/9 features

4 SVM — Accuracy: 100.0%
Last change: Quadratic SVM — 9/9 features

5 KNN — Accuracy: 72.7%
Last change: Medium KNN — 9/9 features

Current Model

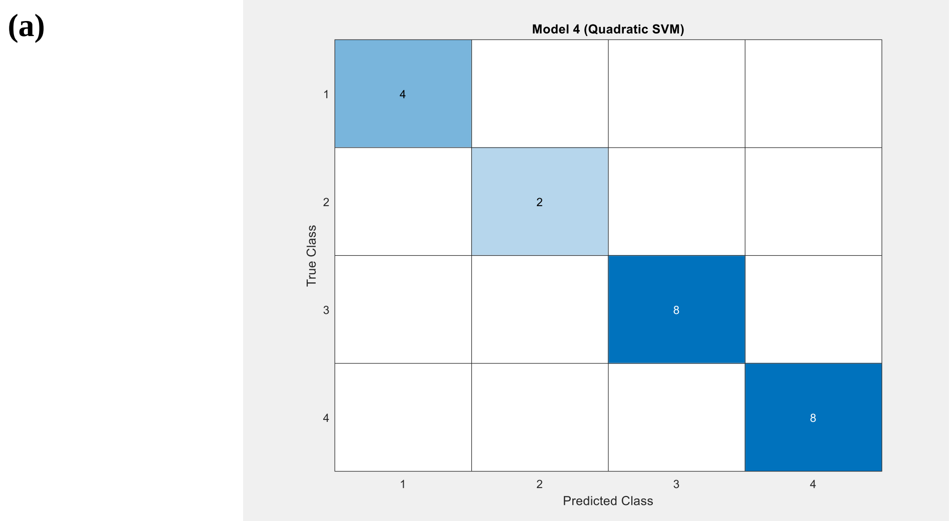
Model 4: Trained

Results
Accuracy 100.0%
Total misclassification cost 0
Prediction speed ~500 obs/sec
Training time 0.9758 sec

Data set: DataSet2 Observations: 22 Size: 5 kB Predictors: 9 Response: column_10 Response Classes: 4 Validation: 5-fold Cross Validation

Figure 6: Results of the SVM-ML training.

From Figure 6, one might observe that the accuracy of the fine tree training reaches to 100%. Now, the measuring function of the confusion matrix is achieved as shown in Figure 7.



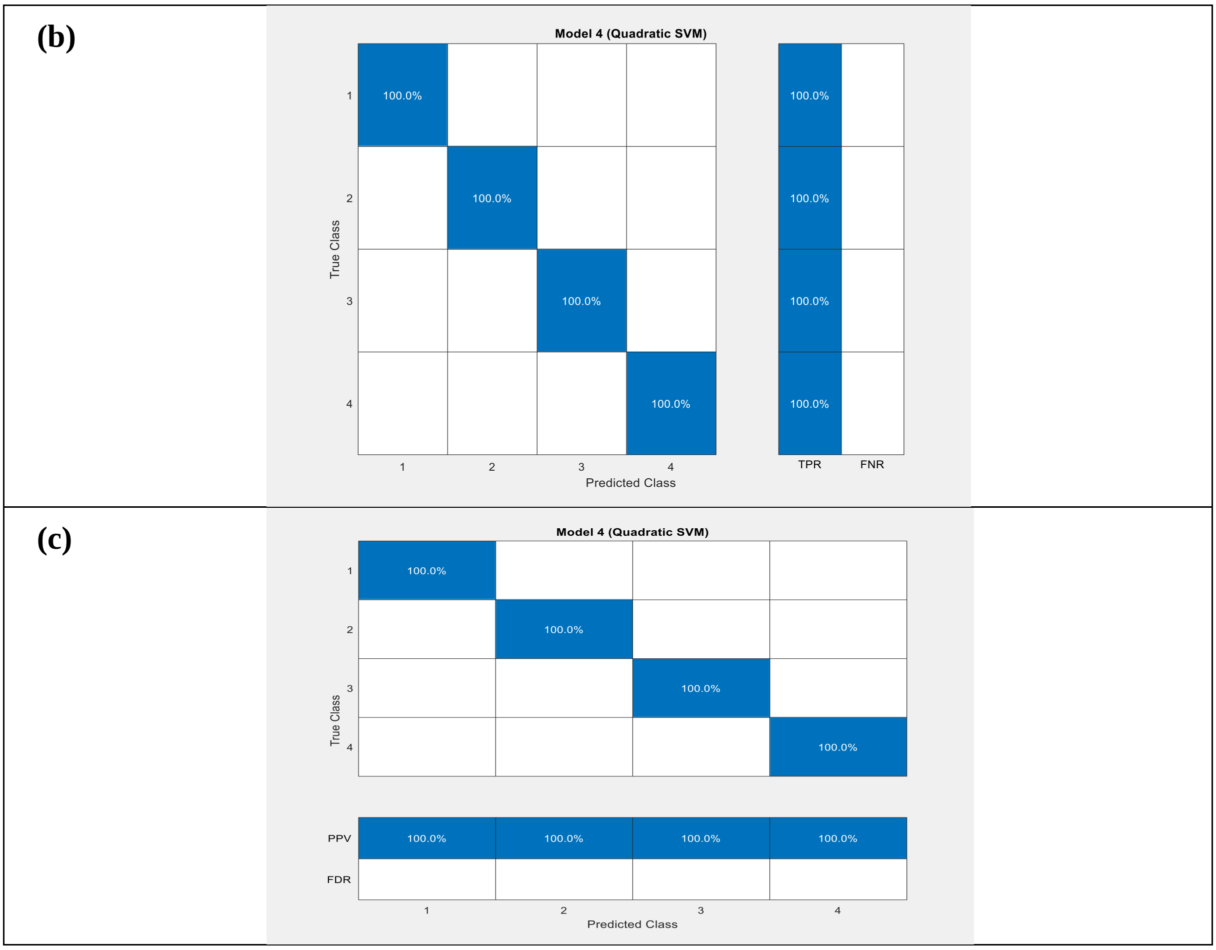


Figure 7: SVM confusion matrix measuring function, (a) Observations sum, (b) True positive rates (TPR) and false negative rates (FNR), and (c) Positive predictive values (PPV) and False discovery rates (FDR).

By observing Figure 7, one might recognize the confusion matrix readings measurements that provide observations of how much the SVM machine learning algorithm training has perform a sufficient data classification. Since from Figure 7, (a) the confusion matrix indicates that all the 8 observations have been matched among the true and predicted classes especially for the 4th and 3rd classes, with 2 observations matching for the 2nd classes and 4 observations matching for the 1st classes. Also the TPR was 100% with FNR of only 0% between the true and predicted learned data samples for all the four classes as displayed in Figure 7, (b). Furthermore, the Positive predictive values (PPV) were 100% with False discovery rates (FDR) of only 0% for all the four classes as shown in Figure 7, (c). Such confusion matrix readings are perfect as indicate a excellent classification for the SVM-ML algorithm. Also the receiver observer curve (ROC) measure has been computed for SVM ML algorithm as shown in Figure 8.

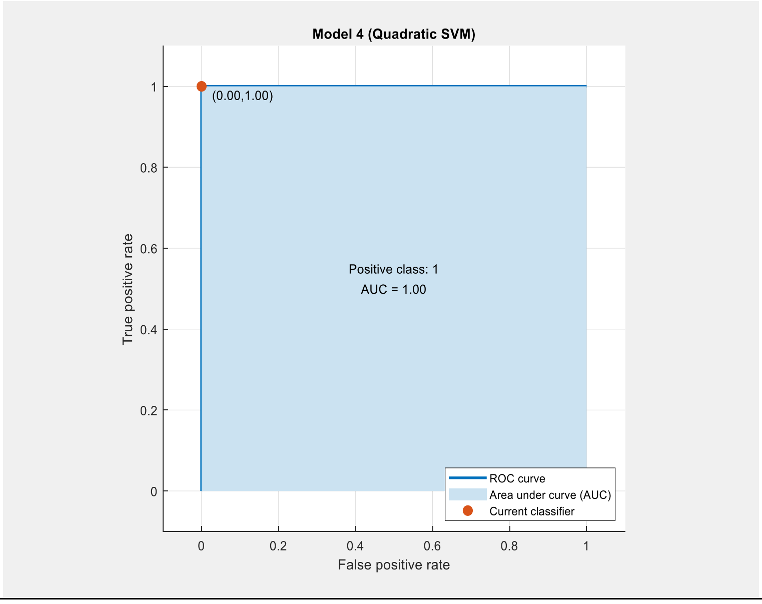


Figure 8: The receiver observer curve (ROC) metric achieved for SVM ML algorithm.

By concerning the results in Figure 8, one could measure how many the True positive rates (TPR) and False negative rates (FNR) are matched for the trained data samples. In this fine tree ML algorithm, the ROC reads only 1 area under the curve (AUC) which is a perfect indication measurement. The third function measurement is the parallel coordinates plot as demonstrated in Figure 9 for SVM ML algorithm learning.

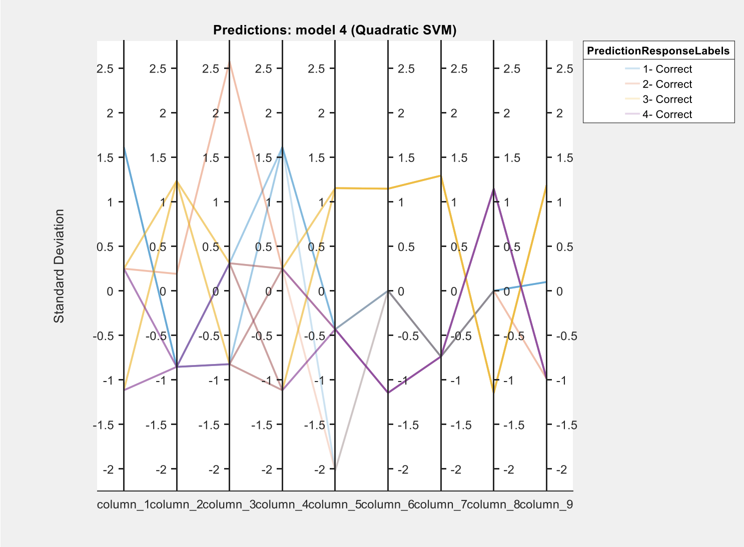


Figure 9: Results of the parallel coordinates plot metric function for SVM ML algorithm.

From the readings shown in Figure 9, one might compute the standard deviation for all the tested dataset samples classes and how it matched to that for the predicted samples. In this study, the suggested model of the SVM ML algorithm, the parallel coordinates plot measure provides excellent matching. Next, the outcomes of the employed m. file MatLab2020b program script code written for training the SVM ML algorithm are achieved. The results of the cloud computing offloading detection using SVM (FT) ML algorithm are introduced in Figure 10.

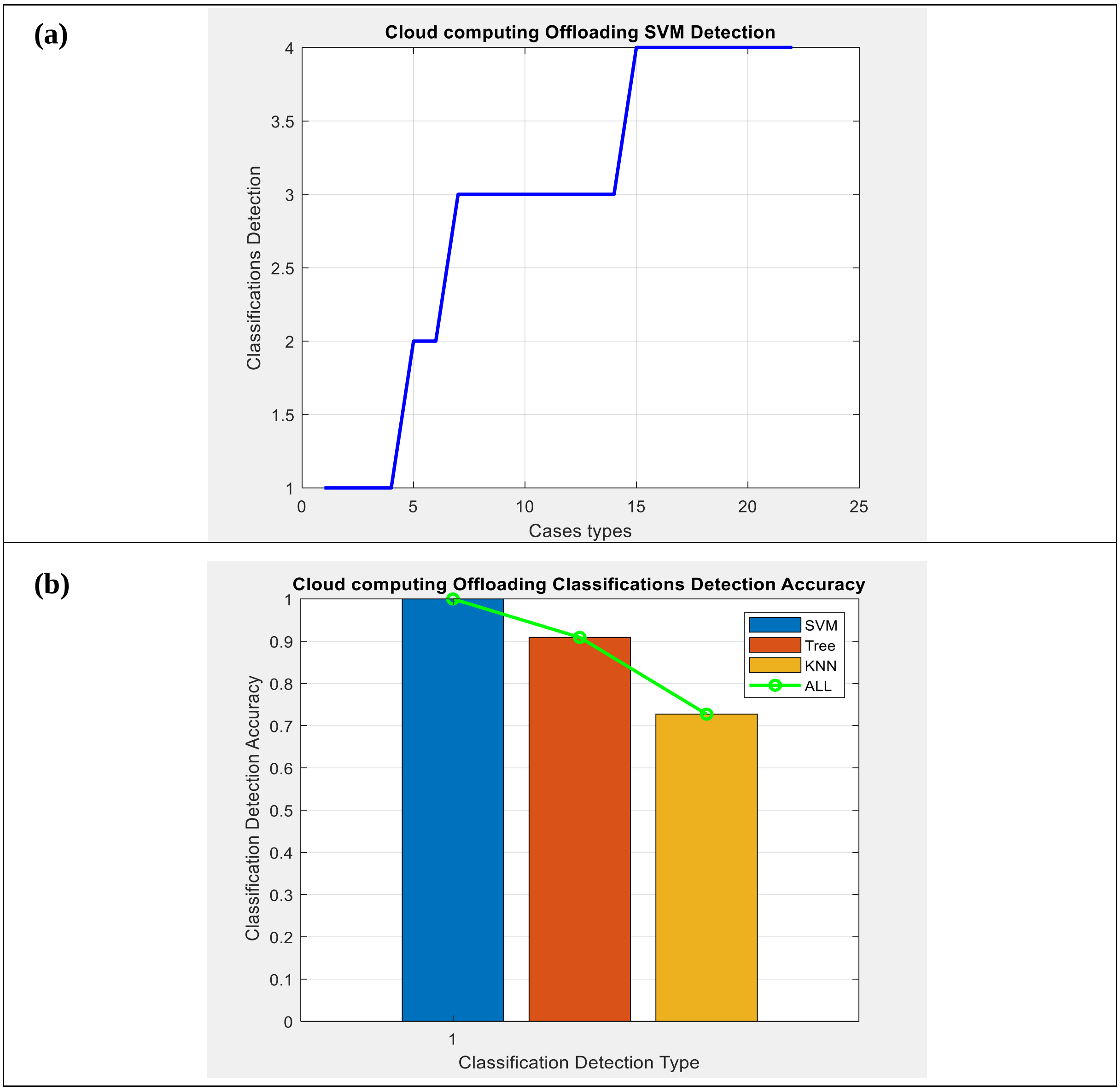
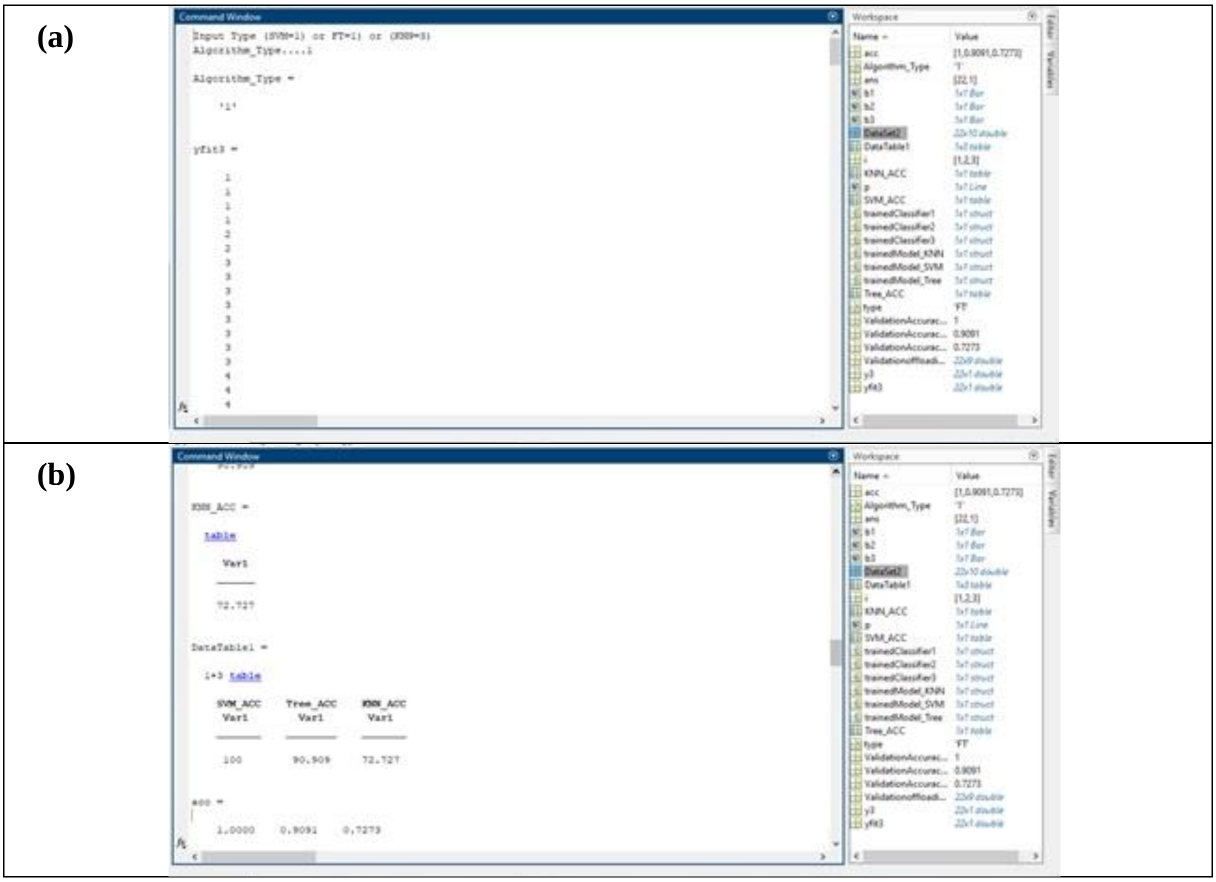


Figure 10: Results of the cloud computing offloading detection accuracy using SVM ML algorithm.

By analyzing the results obtained in Figure 10.(a), one might observe that the classification detection curvefor the SVM ML allgorithm has been improved with a perfect offloading detection progress against the examined classes kinds. It has been found that very excellent detection accuracy of 99-100% has been obtained using SVM ML algorithm as illustrated along the results displayed in Figure 10. The screen shoot of the program implementation for SVM ML algorithm has been shown in Figure 11.



```
Input Type (SVM=1) or FT=1) or (KNN=3)
Algorithm_Type....1

Algorithm_Type =

    '1'


yfit3 =

     1
     1
     1
     1
     2
     2
     3
     3
     3
     3
     3
     3
     3
     3
     4
     4
     4
```

Name ▲	Value
acc	[1,0.9091,0.7273]
Algorithm_Type	'1'
ans	[22,1]
b1	1x1 Bar
b2	1x1 Bar
b3	1x1 Bar
DataSet2	22x10 double
DataTable1	1x3 table
i	[1,2,3]
KNN_ACC	1x1 table
p	1x1 Line
SVM_ACC	1x1 table
trainedClassifier1	1x1 struct
trainedClassifier2	1x1 struct
trainedClassifier3	1x1 struct
trainedModel_KNN	1x1 struct
trainedModel_SVM	1x1 struct
trainedModel_Tree	1x1 struct
Tree_ACC	1x1 table
type	'FT'
ValidationAccurac...	1
ValidationAccurac...	0.9091
ValidationAccurac...	0.7273
Validationoffloadi...	22x9 double
y3	22x1 double
yfit3	22x1 double

```
KNN_ACC =

  table

     Var1
    ______

    72.727


DataTable1 =

  1×3 table

    SVM_ACC    Tree_ACC    KNN_ACC
     Var1        Var1        Var1
    _______    ________    _______

      100       90.909      72.727


acc =

    1.0000    0.9091    0.7273
```

Name ▲	Value
acc	[1,0.9091,0.7273]
Algorithm_Type	'1'
ans	[22,1]
b1	1x1 Bar
b2	1x1 Bar
b3	1x1 Bar
DataSet2	22x10 double
DataTable1	1x3 table
i	[1,2,3]
KNN_ACC	1x1 table
p	1x1 Line
SVM_ACC	1x1 table
trainedClassifier1	1x1 struct
trainedClassifier2	1x1 struct
trainedClassifier3	1x1 struct
trainedModel_KNN	1x1 struct
trainedModel_SVM	1x1 struct
trainedModel_Tree	1x1 struct
Tree_ACC	1x1 table
type	'FT'
ValidationAccurac...	1
ValidationAccurac...	0.9091
ValidationAccurac...	0.7273
Validationoffloadi...	22x9 double
y3	22x1 double
yfit3	22x1 double

Figure 11: Results of the program simulation for SVM ML algorithm.

5. Conclusions

Reproducing edge computing capacities close submachines inside the network limit is one illustration of the idea of cloud computing. A particular report will be introduced in this thesis on the degree to which the task offloading issue can be settled along edge as well as cloud integration. Preparing artificial intelligence with control theory optimization techniques, which can be utilized to accomplish the various objectives, needs, and dynamic states of the beginning and end execution technique, gets specific attention. Central issue penchants. Utilizing strong machine learning algorithms, we inspected the recommended model in light of the got results and the cloud computing offloading recognition implementation utilizing various states of various network plans like WiFi, D2D, MEC, and MCC models. The data of the states these organizations have been given using coordinated datasets which have been imported to set up the used man-made intelligence calculations. In light of the implementation results, it was resolved that the SVM ML algorithm conveys the very best offloading identification results at a rate of 99%, while the FT ML technique came in runner up with a rate of almost 95%, and the KNN ML algorithm finished dead last with a rate of just 75%..

6. References

[1] Z. Wang, Z. Zhao, G. Min, X. Huang, Q. Ni, and R. Wang, “User mobility aware task assignment for mobile edge computing,” Future Generation Computer Systems, vol. 85, pp. 1–8, 2018.

[2] Z. Li and Q. Zhu, “Genetic algorithm-based optimization of offloading and resource allocation in mobile-edge computing,” Information, vol. 11, no. 2, p. 83, 2020.

[3] AQ Raheema, HA Tarish, Analyze and design of secure user authentication protocol for wireless sensor networks, AIP Conference Proceedings 2839 (1), 2023

[4] H. Zhang, X. Liu, X. Bian, Y. Cheng, and S. Xiang, “A resource allocation scheme for real-time energy-aware offloading in vehicular networks with mec,” Wireless Communications and Mobile Computing, vol. 2022, Article ID 8138079, 17 pages, 2022.

[5] L. Dong, M. N. Satpute, J. Shan, B. Liu, Y. Yu, and T. Yan, “Computation offloading for mobile-edge computing with multi-user,” in Proceedings of the IEEE 39th international conference on distributed computing systems (ICDCS), pp. 841–850, IEEE, Dallas, TX, USA, July 2019.

[6] S. Cheng, Z. Chen, J. Li, and H. Gao, “Task assignment algorithms in data shared mobile edge computing systems,” in Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 997–1006, IEEE, Dallas, TX, USA, July 2019.

[7] C. Yang, Y. Liu, X. Chen, W. Zhong, and S. Xie, “Efficient mobility-aware task offloading for vehicular edge computing networks,” IEEE Access, vol. 7, Article ID 26652, 2019.

[8] HA Tarish, Enhancing 5G communication in business networks with an innovative secured narrowband IoT framework HA Tarish Journal of Intelligent Systems 33 (1), 20230278, 2024.

[9] L. Yang, H. Zhang, M. Li, J. Guo, and H. Ji, “Mobile edge computing empowered energy efficient task offloading in 5g,” IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6398–6409, 2018.

[10] H. Peng, W.-S. Wen, M.-L. Tseng, and L.-L. Li, “Joint optimization method for task scheduling time and energy consumption in mobile cloud computing environment,” Applied Soft Computing, vol. 80, pp. 534–545, 2019.

[11] P.-Q. Huang, Y. Wang, K. Wang, and Z.-Z. Liu, “A bilevel optimization approach for joint offloading decision and resource allocation in cooperative mobile edge computing,” IEEE Transactions on Cybernetics, vol. 50, 2019.

[12] J. Bi, H. Yuan, S. Duanmu, M. C. Zhou, and A. Abusorrah, “Energy-optimized partial computation offloading in mobile Information Systems 15 edge computing with genetic simulated-annealing-based particle swarm optimization,” IEEE Internet of 2ings Journal, vol. 8, 2020.

[13] A. Gupta and R. K. Jha, “A survey of 5g network: Architecture and emerging technologies,” IEEE access, vol. 3, pp. 1206–1232, 2015.

[14] M. Series, “Imt vision–framework and overall objectives of the future development of imt for 2020 and beyond,” Recommendation ITU, pp. 2083–0, 2015.

[15] Beraldi, Roberto & Massri, Khalil & Mtibaa, Abderrahmen & Alnuweiri, Hussein. (2013). Delay-Energy Tradeoff in Mobile Cloud Computing: An Experimental Approach.

[16] S. Deng, L. Huang, J. Taheri and A. Y. Zomaya, "Computation Offloading for Service Workflow in Mobile Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 12, pp. 3317-3329, 1, Dec. 2015, doi: 10.1109/TPDS.2014.2381640.

[17] Shiraz, M., Gani, A., Shamim, A. et al. Energy Efficient Computational Offloading Framework for Mobile Cloud Computing. J Grid Computing 13, 1–18 (2015).

[18] B. Zhou, A. V. Dastjerdi, R. N. Calheiros, S. N. Srirama and R. Buyya, "A Context Sensitive Offloading Scheme for Mobile Cloud Computing Service," 2015 IEEE 8th International Conference on Cloud Computing, 2015, pp. 869-876, doi:10.1109/CLOUD.2015.119.

[19] X. Chen, L. Jiao, W. Li and X. Fu, "Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing," in IEEE/ACM Transactions on Networking, vol. 24, no. 5, pp. 2795-2808, October 2016, doi: 10.1109/TNET.2015.2487344.

[20] X. Chen, "Decentralized Computation Offloading Game for Mobile Cloud Computing," in IEEE Transactions on Parallel and istributed Systems, vol. 26, no. 4, pp. 974-983, 1 April 2015, doi: 10.1109/TPDS.2014.2316834.

[21] S. Guo, B. Xiao, Y. Yang and Y. Yang, "Energy-efficient dynamic offloading and resource scheduling in mobile cloud computing," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, 2016, pp. 1-9, doi: 10.1109/INFOCOM.2016.7524497.

[22] B. Wang, C. Wang, W. Huang, Y. Song and X. Qin, "A Survey and Taxonomy on Task Offloading for Edge-Cloud Computing," in IEEE Access, vol. 8, pp. 186080-186101, 2020, doi: 10.1109/ACCESS.2020.3029649.

[23] Shakarami, A., Ghobaei-Arani, M., Masdari, M. et al. A Survey on the Computation Offloading Approaches in Mobile Edge/Cloud Computing Environment: A Stochastic-based Perspective. J Grid Computing 18, 639–671 (2020). https://doi.org/10.1007/s10723-020-09530-2

[24] Barker, A., & Swany, M. (2020). Energy Aware Routing with Computational Offloading for Wireless Sensor Networks. arXiv. https://doi.org/10.48550/arXiv.2011.14795

[25] jaydip kumar. (2019). Cloud Computing Security Issues and Its Challenges: A Comprehensive Research. International Journal of Recent Technology and Engineering (IJRTE). https://doi.org/10030681S419/19

[26] Huang, Sheng-Zhi & Lin, Kun-Yu & Hu, Chih-Lin. (2022). Intelligent task migration with deep Qlearning in multi-access edge computing. IET Communications. 16. 10.1049/cmu2.12309.

[27] Shuchen Zhou, Waqas Jadoon, Junaid Shuja, "Machine Learning-Based Offloading Strategy for Lightweight User Mobile Edge Computing Tasks", Complexity, vol. 2021, Article ID 6455617, 11 pages, 2021. https://doi.org/10.1155/2021/6455617

[28] S. Aljanabi and A. Chalechale, "Improving IoT Services Using a Hybrid Fog-Cloud Offloading," in IEEE Access, vol. 9, pp. 13775-13788, 2021, doi: 10.1109/ACCESS.2021.3052458.

[29] Y. Ai, M. Peng, and K. Zhang, “Edge computing technologies for internet of things: a primer,” Digital Communications and Networks, vol. 4, no. 2, pp. 77–86, 2018.

[30] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, “Edge computing: A survey,” Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.

[31] L. Mendiboure, M.-A. Chalouf, and F. Krief, “Edge computing based applications in vehicular environments: Comparative study and main issues,” Journal of Computer Science and Technology, vol. 34, no. 4, pp. 869–886, 2019.

[32] M. Maray, A. Jhumka, A. Chester, and M. Younis, “Scheduling dependent tasks in edge networks,” in Proceedings of the IEEE 38th International Performance Computing and Communications Conference (IPCCC), pp. 1–4, IEEE, London, UK, October 2019.

[33] HA Tarish, SS-FD: Internet of medical things based patient health monitoring system, Periodicals of Engineering and Natural Sciences 9 (3), 641-651, 2021.

[34] D. Mazza, D. Tarchi and G. E. Corazza, "A Unified Urban Mobile Cloud Computing Offloading Mechanism for Smart Cities," in IEEE Communications Magazine, vol. 55, no. 3, pp. 30-37, March 2017, doi: 10.1109/MCOM.2017.1600247CM.

[35] J. Zheng, Y. Cai, Y. Wu and X. Shen, "Dynamic Computation Offloading for Mobile Cloud Computing: A Stochastic Game-Theoretic Approach," in IEEE Transactions on Mobile Computing, vol. 18, no. 4, pp. 771-786, 1 April 2019, doi: 10.1109/TMC.2018.2847337.

[36] L. Yang, C. Zhong, Q. Yang, W. Zou, and A. Fathalla, “Task offloading for directed acyclic graph applications based on edge computing in industrial internet,” Information Sciences, vol. 540, pp. 51–68, 2020.

[37] L. Chen, J. Wu, J. Zhang, H.-N. Dai, X. Long, and M. Yao, “Dependency-aware computation offloading for mobile edge computing with edge-cloud cooperation,” IEEE Transactions on Cloud Computing, 2020.

Fabrication of hybrid (PEDOT: PSS/n-Si) Solar Cells Application

Rafal Saleh Sachit [1]

Abstract

Heterogeneous hybrid solar cells (HHSCs) have been the subject of much investigation and development interest to a simplistic system structural and technological methods that are low-cost. HHSCs, which utilize a high concentration of Poly(3,4-ethylenedioxythiophene): poly(styrene sulfonate) (PEDOT) is a transparent conductive polymer, are fabricated by drop casting directly onto n-type crystalline silicon. Microscopic chemical etching is employed to induce surface roughness, a technique commonly used in traditional processes. The parameters of the contact between PEDOT: PSS and hermetic n-Si were examined. The properties related to structure, optics, and morphology, along with the electrical characteristics of PEDOT, were thoroughly investigated. The effectiveness of conversion is ascribed to the excellent match among the PEDOT film and the underlying silicon substrate. The integration of silver enhances efficiency, presenting a viable pathway to achieving Solar cells that are both highly efficient and low-cost. At a temperature of 300 K, it was obtaining the open circuit voltage (VOC), short circuit current (ISC), and supply element (F.F.) with values of 29.5 mV, 1.8 mA, and 33.29, respectively. The PEDOT: PSS photovoltaic cell efficiency was 0.92 percent.

Keywords: *HHSCs, N-Si, Poly(3,4-Ethylenedioxythiophene) with Poly (Styrene Sulfonate), Solar Cells.*

http://dx.doi.org/10.47832//RimarCongress03-5

[1] Al-Iraqia University, Baghdad, Iraq rafal.s.sajit@aliraqia.edu.iq

1. Introduction

Energy is the greatest challenge facing humanity in this century [1]. Energy sources are broadly classified into two categories: nonrenewable and renewable sources. Nonrenewable sources, such as fossil fuels (Coal, petroleum, and natural gas have historically served as the principal energy sources for human society [2]. However, excessive exploitation has led to the rapid depletion of fossil fuels, and their combustion has caused significant and ongoing environmental damage [3]. In contrast, alternative or renewable energy sources such as biomass, geothermal, hydropower, solar, and wind, offer sustainable options regarding the meeting energy needs [4]. Among these, Solar energy is the most plentiful and promising renewable resource accessible, though only a small fraction of the accessible solar radiation is currently utilized. Notably, the total proven deposits of fossil fuels amount to approximately 1.4% of the solar energy that arrives at the Earth's exterior annually [5].

Fossil fuels themselves are essentially concentrated solar energy, stored as biomass over millions of years [6]. On a global scale, solar photovoltaic energy is the fastest-growing energy source and is poised to become the primary energy source soon [7]. Crystalline silicone solar cells occupy around 90% of the worldwide photovoltaic industry for both economic and efficient performance[8].Researchers are favorites for poly (style sulfonate) is made from crystalline silicon and polymer (3,4ethyleneedioxythiophen) (PEDOT: PSS)[9]. The characteristics of non-dopant, low-temperature, vacuum-free, and solution manufacturing methods discover PEDOT: PSS/n-Si solar cells provide a range about expenses advantages [10].The efficiency gap is gradually decreasing between HHSCs and traditional silicone cells. With Minority carriers with significant mobility and a long history life, crystalline silicone is a photon absorber that is active collection to transport electrons in the form of photo-generated carriers HHSC. The high transmission (85% for a thickness of 100 nm and high conductivity of 1000 S/cm for Clevia's PH1000) from the other extreme, are the PEDOT: PSS layer[11].

Consequently, HHSCs can reach greater PCEs. However, the Personal Consumption Expenditures (PCE) of HHSCs the engagement PEDOT: PSS/N-Silicon is very limited to lower junction quality. For Surface development for PEDOT: PSS/n-Silicon solar cells are critical since It enhances carrier transmission and separation while reducing interface recovery speed [12] .

However, contact qualities of PEDOT: PSS have rarely been considered with a textured substrate, which improves Effectiveness of the JSC and PEDOT: Hybrid solar cells incorporating PSS/n-Si from the interaction design standpoint[13]. The normal alkaline solution textured the Si surface. method is conducted on our work[14]. Solar panels composed of PEDOT: PSS/n-Si were manufactured by drop casting in this paper. Applying electrodes to cells enables a viable, affordable, high-efficiency metallization method.

2. Experimental Setup

2.1. PEDOT: PSS Materials:

The investigation obtained a 250g aqueous solution of PEDOT from Sigma. This product, which is of photovoltaic (PV) grade, contains a 1.3 wt.% dispersion of Poly(3,4-ethylenedioxythiophene) in H_2O, with a PEDOT-to-PSS ratio of 1:1.6, making it suitable for use as an active solar cells consist of many layers.

2.2. N-Si :

Wafers n-type [100] with a thick of 215 µm and Substrates with dimensions ranging from 1 to 3 centimeters were utilized. To eliminate the compromised layer, the specimens underwent standard cleaning procedures (SC1 and SC2), followed by polishing at 75 °C in high-concentration solutions for 2–3 minutes by alcohol.

3. Manufacturing of HHSCs in Silicon

The PEDOT solution was placed onto Transparent silicon that has been warmed and is capable of conducting electricity with n-type characteristics via Investment casting at 50°C, followed by calcination for 10 minutes. The heated substrates were then allowed to cool to room temperature. Aluminum flakes (0.1 cm^2) were subsequently applied to the PEDOT layer. The samples were obtained from the PSS (n-Si/PEDOT) process. Figure 01 illustrates this setup:

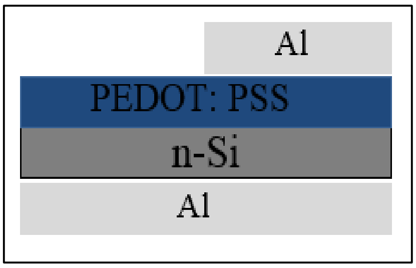


Figure 1: A photovoltaic display chart representing the Al/Si/PEDOT/Al structure, deposited onto n-type silicon

4. Result and discuss

The physicochemical and structural properties of the Si/PEDOT specimens were described or identified using (XRD). Morphological, topography and roughness were analyzed through AFM, and FE-SEM. Optical characteristics, including the optical band gap, were quantified utilizing a UV-Vis spectrophotometer. Additionally, the electrical properties of the samples, such as carrier concentration and type, were assessed using the Hall effect.

4.1. X-Ray Diffraction Analysis:

Figure 02 illustrates The X-ray diffraction (XRD) patterns of the Si/PEDOT crystalline structure compound. The XRD patterns displayed in this figure correspond with previously reported values for Si and PEDOT, as referenced in [15]. The magnitude of the peaks in the X-ray diffraction (XRD)sequences are indicative of the existence of a nanostructure. The X-ray diffraction patterns of n-Si encompass two primary peaks at angles (27.5, 28.5). The hkl (100) and 2θ (27.5, 28.5 Deg.). X- ray diffraction patterns of crystalline compound (PEDOT: PSS) This outcome aligns closely with that reported in the sources,[16]. All diffraction peaks are indexed to a monoclinic Structure that aligns well with the conventional peaks (JCPDS No. 04-015-5877). The x-ray pictures clearly indicate the broadening of the nanoparticles' diffraction peaks.

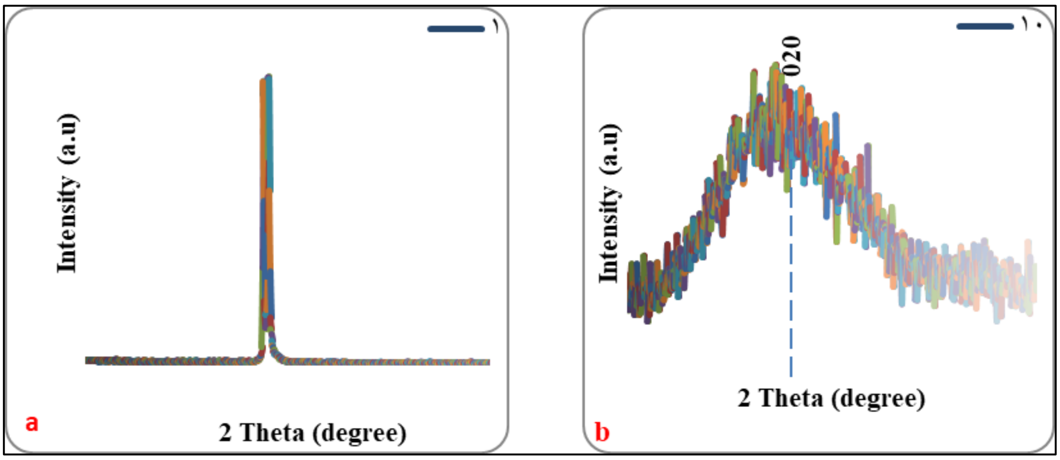


Figure 2: The patterns of XRD (a) n-Si, (b) PEDOT: PSS

4.2. AFM Analysis :

Atomic Force Microscopy (AFM) constitutes a powerful tool accustomed to analyzing the configuration and tactile quality of diverse surfaces. This technique enables accurate control and characterization of a sample's morphology features, offering superior capabilities compared to alternative microscopic techniques. AFM enables Three-dimensional surface scanning and provides detailed visual analysis, including measurements of root mean square roughness, mean particle height, and periodicity intensity spectra in particle arrangement.[17].

Figure 03 displays Three-dimensional atomic force microscopy pictures and the granular film distribution (n-Si and PEDO). These images, obtained from atomic force microscopy, provide information on root mean square (RMS) roughness and mean surface roughness. Table 1 presents the RMS roughness values of the thin films. The RMS roughness, also referred to as the roughness index, quantifies surface irregularity by measuring surface height variance expressed as a standard deviation from the average height. Higher RMS values indicate greater surface roughness, which is proportional to increased optical loss and reduced surface light emission. Therefore, improving surface finish can help minimize optical losses agree with [18]. This component is utilized to symbolize the characteristics of the surface random uneven dispersion.

Table 1: shows the mean diameter, root mean square, and roughness density of the roughness density Si and PEDOT: PSS.

	Avg. Diameter(nm)	Root Mean Sq. (nm)	Ave. Roughness (nm)
Si	31.31	19.6	17
PEDOT: PSS	61.14	7.63	6.61

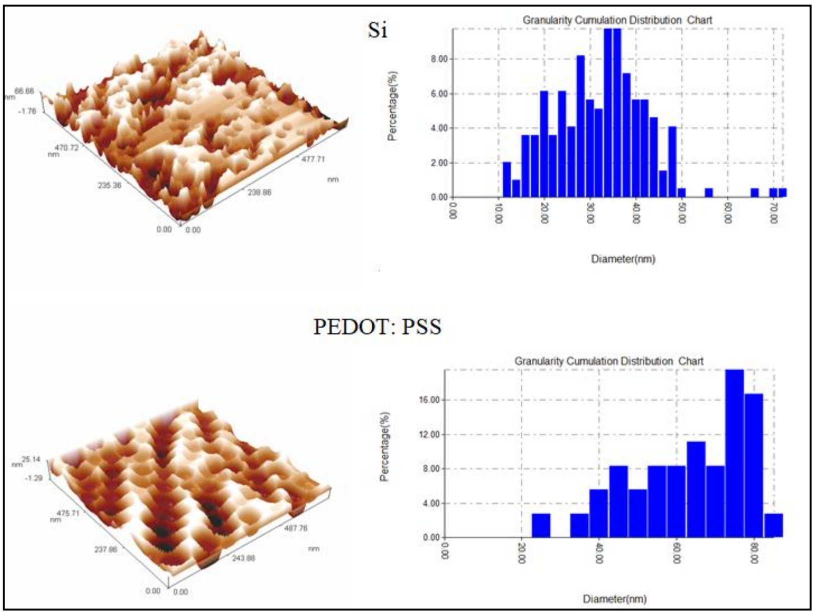


Figure 3: Displays a 3D image with a Chart depicting the dispersion of granular accumulations(a) Si and (b) PEDOT: PSS for AFM analysis.

4.3. FE-SEM Measurement:

As-prepared FSEM images of thin films PEDOT: PSS at two distinct magnifications. Figure 04 and d illustrated that the (PEDOT: PSS) form is sheets [18].

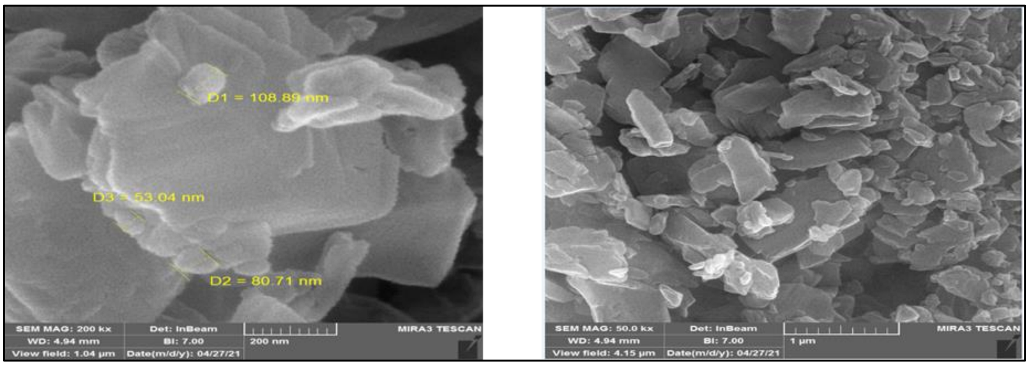


Figure 4: Elevated measurements for (a) scale nano and (b) scale micro for FE-SEM analysis.

4.4. Optical Properties:

Figure 05 presents the absorption spectrum of thin film, measured using a UV-Vis UVD-3500 double beam spectrophotometer (300–1100 nanometers. The absorption margins of the specimens can be analyzed by identifying either on top of the head or the apex in the spectra and extrapolating the linear segment of the curve to estimate the energy band gap. Energy disparity is determined by means of the equation derived from the absorption peak. (1) [19].

$$\alpha h\nu = B \times \left(h\nu - E_g\right)^n \ldots\ldots\ldots\ldots\ldots(1)$$

The energy band gap of (PEDOT: PSS) The estimation is conducted by graphing the square of $(\alpha h\upsilon)^2$ against $(h\upsilon)$. The extrapolation of the straight line to $(\alpha h\upsilon)^2 = 0$ yields the value of the energy gap, namely the band gap. (PEDOT: PSS) Nano crystalline was direct. The Eg of (PEDOT: PSS) is (5.05eV).

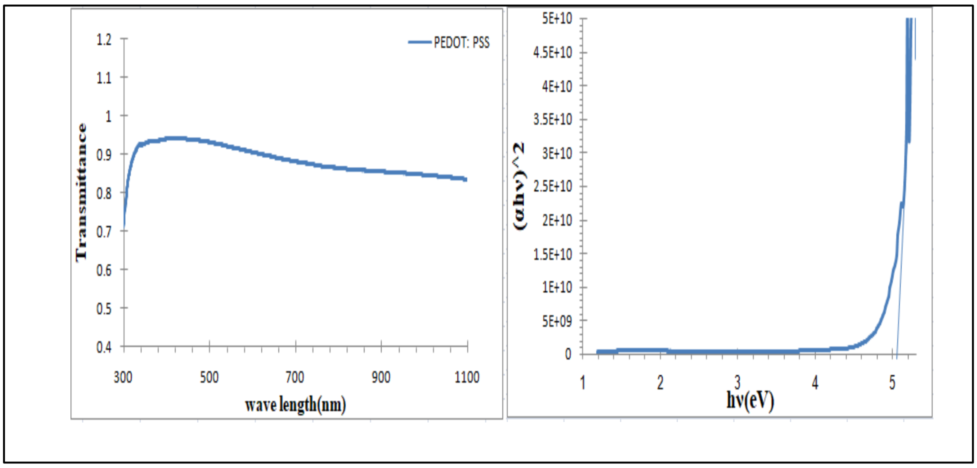


Figure 5: UV-VIS analysis (a) Transmission and (b) Energy band gap

4.5. ElectricityCharacterization:

The Hall measures taken on were performed on the deposited sample to calculate its (nH), (μH), (σ), and (ρ), which serve as indicators of charge carriers for thin film. This data is presented in Table 02.

Table 2: displays the values for electrical properties

Materials	(ρ) [Ω cm]	(σ) (Ω cm)$^{-1}$	(RH) [cm^3/C]	(n$_H$) [/cm^{-3}]	(μ) [cm^2/V$_s$]	Type
PEDOT: PSS	4.61E-03	2.17E+02	4.20E-04	1.49E+22	9.12E-02	p-Type

4.6. I-V Under Illumination:

Figure 06 displays the photocurrent generated when a (150) W/ m^2 irradiates the device. The figures also illustrate the inverted Current-voltage characteristics of the gadget observed in both dark and illuminated conditions. The diagrams clearly demonstrate that the current value is greater when the lighting is at a specific voltage compared to when it is in darkness. This implies that the production of light induces the development of electron-hole pairs, which in turn leads to the generation of a photocurrent carried by the carriers. This behavior yields valuable insights into the pairs of electrons and holes created in the circuit by light photons.

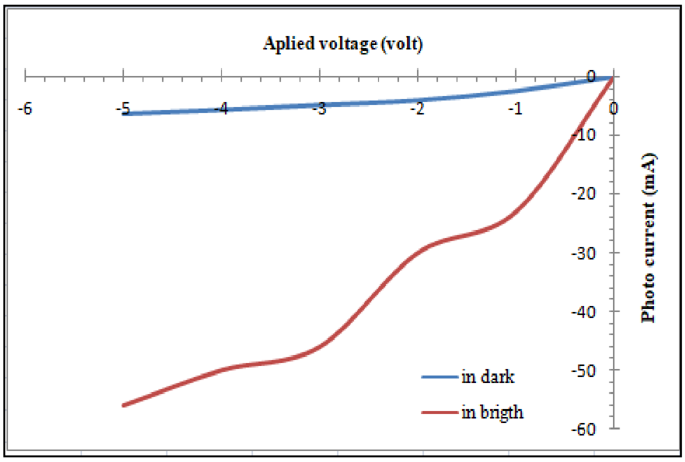


Figure 6: Dark and bright the solar cell's I-V curve.

4.7. The I-V Curve for thin film in solar cell:

The PCE features of the cell, namely the n-Psi/PEDOT: PSS qualities, as well as the measured values include the V$_{oc,}$ I$_{sc}$, F.F, and efficiency. all crucial metrics to be considered, as depicted in Figure 8. Research consistently demonstrates that the (n-Psi/PEDOT: PSS) configuration is very efficient for solar PEDOT: PSS cells.

Photovoltaic energy, often known as solar energy, is harnessed using Equations formulated from a solar cell. [20] (2) and (3):

$$PCE = \frac{V_{oc} \,.I_{sc}\,.F.F/A_{sc}}{P_{in}\; mw/cm^2} \ldots\ldots\ldots (2)$$

$$F.F = \frac{I_m V_m}{V_{oc}\, I_{sc}} = \frac{P_m}{V_{oc}\, I_{sc}} \ldots\ldots\ldots..(3)$$

At a temperature of 300 K, it is achievable to acquire the open circuit voltage (VOC), short circuit current (ISC), and supply factor (F.F.) with values of 29.5 mV, 1.8 mA, and 33.29, respectively. The PEDOT: PSS solar cell efficiency was 0.92 percent. Agree with Rafal Saleh [1].

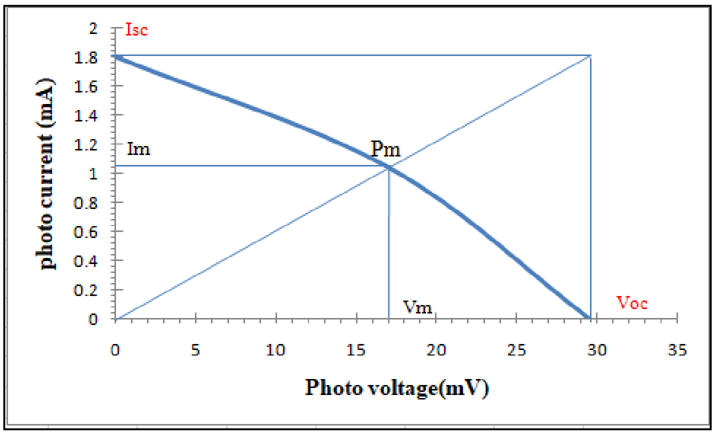


Figure 7: PEDOT: PSS solar cell I-V curve

5. Conclusion

We have successfully demonstrated the creation of a Si/PEDOT: PSS function with electron-blocking properties using a spin coating technique at room temperature. Reverse recovery experiments involve inserting minority carriers into the forward bias condition to measure the stored charge. By introducing the minority carrier hole originating from the anode, it thus facilitates a means of measuring the current in the silicon/PEDOT device. The results indicate the Si/PEDOT: PSS interface effectively inhibits the flow of electrons. Consequently, the dark current observed in n-Si hetero junction devices is mostly due to the injection of minority carrier holes from the anode to silica, rather than the movement of electrons.

Reference:

[1] Rafal ,S. (2021). Solar cells based on inkjet-printed layer polymer, J. Phys. Conf. Ser., vol. 2114, no. 1, p. 012026, Dec., doi: 10.1088/1742-6596/2114/1/012026.

[2] Abdalameer, N. K., Fahad, O. A., & Khalaph, K. A. (2022). Effect of Pulsed Laser Frequency on CdTe Deposited as Solar Cells Device. International Journal of Nanoscience, 21(01), 2150062.https://doi.org/10.1142/S0219581X21500629.

[3] Fan, J. Jia, B. and Gu, M. (2014). Perovskite-based low-cost and high-efficiency hybrid halide solar cells, Photonics Res., vol. 2, no. 5, p. 111, doi: 10.1364/PRJ.2.000111.

[4] Khalaph, K. Qasim, A. Abdalameer, N. Otaiwi, S. Jafar, A. & Numan, N. (2024). Pb-Free Two-Dimensional Perovskite, Nanoparticulate, in the Solar Cells. International Journal of Nanoscience, 23(01), 2350056.

[5] Article, R. Loganathan, K. Logavaseekaran, R. Nithiya, and Jayabharathi, V. (2016).Green Synthesis of Nanoparticles Their, vol. 5, no. 5, pp. 454–478, doi: 10.20959/wjpps20165-6686.

[6] Khalaph, K. Jafar, A. & Abdal Ameer, N. (2022). Pb-Free Metal Halide Double Perovskite, Cs2 InAgCl6, in the Solar Cells Application. International Journal of Nanoscience, 21(01), 2250001.

[7] Taguchi , M. (2014). 24.7% Record efficiency HIT solar cell on thin silicon wafer, IEEE J. Photovoltaics, vol. 4, no. 1, pp. 96–99, doi: 10.1109/JPHOTOV.2013.2282737.

[8] Wei , W . (2013). Above-11%-efficiency organic-inorganic hybrid solar cells with omnidirectional harvesting characteristics by employing hierarchical photon-trapping structures.Nano Lett., vol. 13, no. 8, pp. 3658–3663, doi: 10.1021/nl401540h.

[9] Wen , H. (2017). Improving the organic/Si heterojunction hybrid solar cell property by optimizing PEDOT:PSS film and with amorphous silicon as back surface field, Appl. Phys. A Mater. Sci. Process., vol. 123, no. 1, pp. 1–9, doi: 10.1007/s00339-016-0612-8.

[10] Ph, C. “Significant Different Conductivities of the Two Grades of Poly(3,4-ethylenedioxythiophene):Poly(styrenesulfonate), Clevios P and Clevios PH1000, Arising from Different Molecular Weights,” 2012.

[11] Yang , Z. (2017).Tuning of the contact properties for high- efficiency Si/PEDOT:PSS heterojunction solar cells, ACS Energy Lett., vol. 2, no. 3, pp. 556–562, doi: 10.1021/acsenergylett.7b00015.

[12] Battaglia, C. Cuevas, A. and De Wolf, S. (2016). High-efficiency crystalline silicon solar cells: Status and perspectives, Energy Environ. Sci., vol. 9, no. 5, pp. 1552–1576, doi: 10.1039/c5ee03380b.

[13] Wang, R. Shang, Y. Kanjanaboos, P. Zhou, W. Ning, Z. and Sargent, E. H. (2016). Colloidal quantum dot ligand engineering for high performance solar cells, Energy Environ. Sci., vol. 9, no. 4, pp. 1130–1143, 2016, doi: 10.1039/c5ee03887a.

[14] Gao, C. Li, J. Liu, J. Zhang, J. and Sun, H. (2009). Influence of MWCNTs doping on the structure and properties of PEDOT:PSS films, Int. J. Photoenergy, vol., doi: 10.1155/2009/650509.

[15] Wang , X. (2018). Enhancement of thermoelectric performance of PEDOT:PSS films by post-treatment with a superacid, RSC Adv., vol. 8, no. 33, pp. 18334–18340, doi: 10.1039/c8ra02058b.

[16] Gao, C. Li, J. Zhang, J. and Sun, H. 2009. Influence of MWCNTs doping on the structure and properties of PEDOT:PSS films, Int. J. Photoenergy, vol. doi: 10.1155/2009/650509.

[17] Wang, W. (2017). Nonuniform Effect of Carrier Separation Efficiency and Light Absorption in Type-II Perovskite Nanowire Solar Cells, Nanoscale Res. Lett., vol. 12, no. 1, doi: 10.1186/s11671-017-1912-4.

[18] Jiang , X. (2018). High Performance of PEDOT:PSS/n-Si Solar Cells Based on Textured Surface with AgNWs Electrodes, Nanoscale Res. Lett., vol. 13, doi: 10.1186/s11671-018-2462-0.

[19] Abdulameer, N.(2020). Impact of Dielectric Barrier Discharge (DBD) Plasma on the Optical Properties of Thin Films, vol. 15, no. 8, pp. 1937–1942,.

[20] Suhail, M. Jafar, A. (2016).Fabrication and characterization of organolead halide

[21] peroviske solar, Elixir Renew. Energy 98 42709–42713.

Hydrological Characteristics of the Gharraf Rivers

Manal Abdulsatter Muhammed [1]

Ali Nadhim Manea [2]

Nuralhuda Aladdin Jasim [3]

Zainab Jaber Mohammed [4]

Abstract

Given that the study area is located within the dry regions of the country, the total reliance on surface water represented by the Gharraf River is primarily, in addition to the loss of rain to cover losses due to evaporation and the absence of seasonal rivers or tributaries that supply the river with water, so the area was ruled by a permanent water deficit, and for this reason water management in the Gharraf Basin must receive sufficient attention to secure water protests and other various requirements. The Gharraf River is one of the rivers that branch off from the Tigris River from the front of the Kut Dam and heads towards the southeastern administrative borders of Wasit Governorate, then enters Nasiriyah Governorate at dawn with a length of (230) km, of which (86) km are in Wasit Governorate. The hydrological study showed that the natural conditions affecting the Gharraf River, such as high temperatures, increased evaporation, filtration and sediment values, caused its water discharges to decrease during the period (1985-2020) from 192 m3/s to 146 m3/s. The river was also calibrated with field levels using the (HEC-RAS) program, so the average Manninck coefficient was (0.026), in addition to knowing the effect of return water (RATING CURVES). There was a significant effect when closing and opening the gates of the neighborhood regulator. It was noted that the levels affected by the gate openings were more than 175 m3/s. Most of the streams branching off from the Gharraf River, which are located on the left side of the river, needed a discharge of (137) m3/s, and the right bank of the river needed (113) m3/s along its length.

Keywords: *Gharraf River, Management, Regions, Hydrological, and Characteristics.*

http://dx.doi.org/10.47832/DuhokCongress-6

[1] College of Engineering, Wasit University, Al Kut, Iraq mabdulsattar@uowasit.edu.iq

[2] 2Ministry of Water Resources, Wasit,Iraq aliarrar93@gmail.com

[3] College of Engineering, Wasit University, Al Kut, Iraq njasim@uowasit.edu.iq

[4] college of Engineering, Wasit University, Wasit, Iraq zainab.jaber@uowasit.edu.iq

1. Introduction

The research area is situated in arid regions, lacking dependence on the surface water provided by the Gharraf River. The evaporation rate in the studied area is quite high, rendering rainfall ineffective in replenishing the Gharraf River, as losses occur throughout the entire year. Consequently, water management in the Gharraf River must get adequate attention to address various water requirements. The initial scientific advisory research for the study area was conducted by the American engineering firm. A preliminary study of the East and West Al Gharraf project was conducted, resulting in a report that encompassed all investigations, regional development stages, cost estimates, results, recommendations, designs, and preliminary plans. During the year 1958 The French Cotha Consulting Company (1961, Cotha) conducted an analysis of the Al-Gharraf project, completing all field investigations and submitting its final report in 1961, which was among the foremost studies in the region. The Euphrates Center for Studies and Design of Irrigation Projects conducted an analysis of the East Al-Gharraf project and submitted its final report in 1993. Hydraulic modeling of the Gharraf River between the cities of Kut and Hay. Determine the Manning coefficient value of 0.025 in a steady condition and elucidate the impact of discharges in the upstream Gharraf River on the rating water curve. The hydrological study seeks to elucidate the fluctuations in the Gharraf River's water levels and the volume of water resources necessary to meet diverse water demands.

2. Steady Area

Branches from the Tigris River near the Kut Bridge upwards, specifically at the Gharraf regulator. It persists on its southwest trajectory between the Tigris and Euphrates rivers, extending from the cities of Kut to Nasiriyah. The whole length is 230 km from upstream to downstream in the marshes of Nasiriyah, which includes 86 km in Wasit. Its currents traverse Al-Muwaffia, Al-Hay the Fajer, Qalah-Sukkar, and Al-Rifai. The environmental factors influencing the Gharraf River are analogous to those impacting the Tigris River, characterized by elevated temperatures and heightened evaporation rates throughout the majority of the year, along with groundwater infiltration, resulting in diminished water availability, particularly from April to October. The disparity in discharge prompted the establishment of four regulators to elevate water levels for agricultural and various water needs in the research area.

3. Discharge Characteristics for the period 1985 - 2020

The annual water flow of the rivers in Iraq has significantly diminished during the past two decades, primarily due to the construction of massive water impoundment projects, some of which are still underway in Turkey, Syria, and Iran (Al-Ansari and Knutsson, 2011). Furthermore, arid climatic years in Iraq. The flow of the Gharraf has decreased significantly by approximately 29% during the discharge period from 1990 to 2020. The mean The annual discharge of the Gharraf at Wasit from 1990 to 2003 averaged 195 m³/s, which decreased to 146 m³/s from 2003 to 2020, as illustrated in Fig. 1. This reduction represents a decline of over 25% from the mean daily discharge prior to 2003 and is significantly lower than the flood discharges of 220, 309, and 302 m³/s recorded in 1974, 1988, and 2004, respectively. The annual average discharge was 6.05 billion m³ for the period from 1990 to 2003, while the estimated discharge for 2003 to 2020 was 4.54 billion m³.

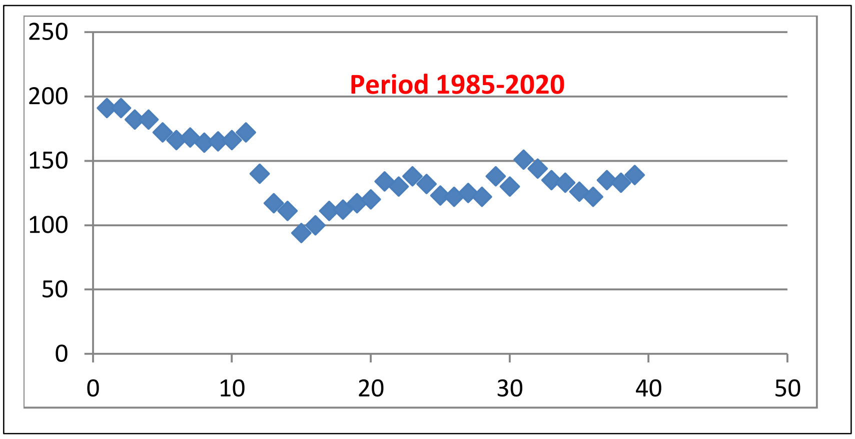


Figure 1: Annual mean discharge of Gharraf River downstream for Gharraf Regulator

4. Factors Affecting Flow

4.1. geological structure :

Topographic manifestations, such as the side-looking configuration of radar highlighting relief, are possible manifestations of geological features that frequently have characteristic forms and are located near the Earth's surface. For sensitive topographical features that benefit from shadowing, shallow incidence angles are perfect. Because shallow incidence angles might cause an excessive amount of shadowing in high relief situations, intermediate incidence angles may be more suitable. So, it's important to think about how geological structures are oriented in relation to the direction of sight.

As erosion causes folds, domes, and basins to change shape, it reveals their attitudes. Scarp and dip slopes can be better understood and classified, as well as their approximate direction, through the analysis of drainage networks and distinctive erosion patterns. This section will go over the basic requirements for finding the dip direction of slanted rock units.

4.2. Control structures & surface :

Terrain influences discharge by dictating the velocity of water flow. Increased flow velocity on steep surfaces results in reduced seepage and a heightened degree of erosion, whereas flat surfaces enhance filtering (seepage) and decrease discharge owing to evaporation. The overall slope gradient of the river is 0.000048 in HEC-RAS software. To elevate water levels, four regulators have been constructed on the river during and since the latter half of the twentieth century between the cities of Hay and Sattrah, in addition to the Gharraf regulator that manages the outflow. Regulator No. 1 is situated in Al-Hay city, 59 km south of the Al-Gharraf regulator. Regulator No. 2 is established 30 km from Regulator No. 1, while Regulator No. 3 is located north of Sukkar Castle, 25 km south of Regulator No. 2. Regulator No. 4 is approximately 5 km south of Al-Rifai city, 140 km from the Al-Gharraf regulator. The maximum discharge permitted through regulators No. 1 to No. 4 is 450 m³/sec, 350 m³/sec, 300 m³/sec, and 250 m³/sec, respectively.

4.3. Gradient:

The flatness of the gradient led to the very slow gradient of the river reach Therefore, the river decreases velocity for the greater part of its energy, and sediments are deposited on its sides**.** A large part of suspended load is deposited on the bed and its valley widens, so the Gharraf River is considered to be in the late aging stage. Either side slope of the river is simple, ranging from (1-3) m to a width for (40-70) km.

5. Annual discharge Characteristics

The examination of the average annual discharge is crucial in hydrological research as it indicates the pattern of rainy, moderate, and dry years. To ascertain the volume of water required for storage from rainy years to dry years, together with the methodology for managing river water in alignment with the needs of each research region. Furthermore, it is essential to understand the extent of fluctuation in water volume resulting from the quantities injected and drained between Wasit and Nasiriyah, as well as their influence on hydrological features.

Characteristics of the yearly discharge of the Gharraf River are analyzed through the variation in the average annual discharge from 1990 to 2020 at the downstream Gharraf regulator and regulator No. 2, which marks the boundary between Wasit and Dhi Qar governorates. Table 1 presents the average discharge and annual income.

Table 1: Average annual discharge of the Garraf Basin area

Location	Period	Chemist area (KM^2)	Average discharge	Average Year (miller/m3)	Ave. H (mm/year)
D/S For Gharraf Reg.	1990-2003	1123	195	6.05	5365
	2003-2020		146	4.54	4127
D/S For NO 2	1990-2003	2152	120	3.81	1556
	2003-2020		92	2.86	1245
After Reclamation Projects in the Future (in wasit only)					
East Gharraf	2020 ~	545	102	1.5	-
West Gharraf	2020 ~	542	113	2.0	-

The data in Table (2) indicates that the average discharge of the Gharraf River at the station downstream of the Gharraf regulator for the period from 1990 to 2003 is 192 m³/sec. In contrast, the average discharge decreased to 120 m³/sec at the station downstream of Regulator No. 2 for the period from 2003 to 2020, with respective averages of 146 m³/sec and 90 m³/sec.

The variance in discharge between the stations arises from multiple factors, including the management and regulation of water releases from regulator No. (1) and regulator No. (2) to ensure water availability for agricultural and other applications.

- variables of seepage and evaporation in the research region.
- An inverse relationship exists between area and average water height, resulting in significant losses of land unsuitable for cultivation owing to salinization.
- Obsolete and underdeveloped irrigation systems and lack of canal maintenance.

The height of the Gharraf River downstream is 4746 mm per year, however it decreased to 2800 mm per year at downstream Regulator No. 2. Due to the decline in water revenue on one hand and the extensive territory of the region on the other hand. Tourist irrigation losses were calculated at 50%, with an average increase in evaporation of 1300.

Utilize the mean discharge coefficient from the equation to ascertain wet, medium, and dry years. $\mathbf{K = \frac{Q}{Q^{-}}}$

Where

K = discharge coefficient

Q = discharge average for once year

Q^{-} =discharge average for study period

IfK > 1 the wet year

K < 1 the dry year

K $= 1$ the medium year

Table (2) presents the coefficient model results for the average discharge of the Gharraf River for each study reach.

A disparity was evident among the wet, medium, and dry seasons. The period from 2000 to 2002 for the Gharraf River was marked by aridity, with a discharge rate declining to 90.5 m³/s. In contrast, the period from 2003 to 2007 was characterized by increased precipitation, resulting in an average discharge of approximately 184 m³/s. The period from 2012 to 2015 exhibited moderate conditions, with an average discharge of 134 m³/s.

Table 2: Duration of time (wet, temperate, dry) of the Gharraf Basin

station	period	No. year	Type of year	Average discharge	K
Down Stream Gharraf River	1990-1993	3	Medium	158	=1
	1994-1999	4	Wet	202	<1
	1999-2003	5	Dry	110	>1
	2003-2007	5	Wet	184	<1
	2008-2011	4	Dry	110	>1
	2012-2013	2	Medium	136	=1
	2015-2020	6	Medium	148	=1

Advantages (K): It serves as a dependable criterion for assessing storage capacity in riverine projects. The storage capacity is contingent upon the discharge throughout a specific duration, as well as the variable discharge over different years. What is the significance of the temporal sequence of wet and dry periods that indicate positive or negative discharge deviation.

The hydrographs illustrate the variation in the annual average discharges at the D/S Gharraf Regulator station from 1990 to 2020, with 12 years exceeding the average, 10 years falling below it, and 8 years approximating the general average. This indicates that approximately 40% of the years were wet, 33% were dry, and 27% were near the average. The table (3) presents the maximum and minimum discharge for the D/S Gharraf Regulator.

Table 3: shows the highest and lowest discharge for D/S Gharraf Regulator

Period	Ave.	min		max		station
		discharge	year	discharge	year	
1985-2003	192	85	2001	300	1988	D / S Of Gharraf Reg.
2003-2020	146	94	2009	200	2005	

6. Control Regulator

The table down below explained the details built on Gharraf river in other words regulators.

Table 4: Regulators built on the Gharraf River

Name Reg.	Constriction	Dimension/For Once	No . Gate	Water Level Operation	Kilometers about Kut	Operation Run	Material
Gharraf Reg.	**1939**	**8*6**	**7- vertical**	**17.98**	**2 km**	**Manual + Mechanical**	**Concrete**
Al-Hay Reg. (No1)	**1960**	**5.6*9**	**5 - curvature**	**16.00**	**58 km**	**Manual + Mechanical**	**Concrete**
No 2. Reg.	**1960**	**5.5*9**	**4 - curvature**	**17.70**	**87 km**	**Manual + Mechanical**	**Concrete**
No 3. Reg.	**1962**	**5.5*9**	**4 – Radial**	**14.00**	**112 km**	**Manual + Mechanical**	**Concrete**
No 4. Reg.	**1962**	**5.5*9**	**4 – Radial**	**12.00**	**140 km**	**Manual + Mechanical**	**Concrete**
Al-Bddah Reg.	**1939**	**7*5**	**6 - Double**	**10.00**	**170 km**	**Manual + Mechanical**	**Concrete**
Al-Shattra Reg.	**--**	**7*2.5**	**3 -- Radial**	**10.00**	**170 km**	**Manual**	**Concrete**
Al- kisser Reg.	**--**	**5*2**	**2 – Radial**	**-**	**198 km**	**Manual**	**Bricks**
AL- Ibrahimy Reg.	**--**	**5*2**	**2 – Radial**	**-**	**198 km**	**Manual**	**Bricks**

7. Morphology

a. River geometry & changes cross-section:

The variation among the majority of cross-sections is between 0.6 and 1.2 meters. The formation of the islands, bends, and twists of the Shatt al-Gharraf is attributable to numerous sources, including: The substantial sediments transported by the river, coupled with the gentle gradient of the Al-Gharraf River. The slope's decline results in the formation of river meanders, as it indicates a notable reduction in the river's gradient. The sedimentation intensity escalates due to the diminished velocity of the current, attributed to the decreasing slope of the water surface along the river's course. The river's gradient measured between its confluence with the Tigris River and Regulator No. (2) was (0.00004), while the gradient between the latter site and the heresy was (0.000058).Refer to Figure 2. This signifies the river's limited capacity to transport sediments obstructed by structures and impediments.

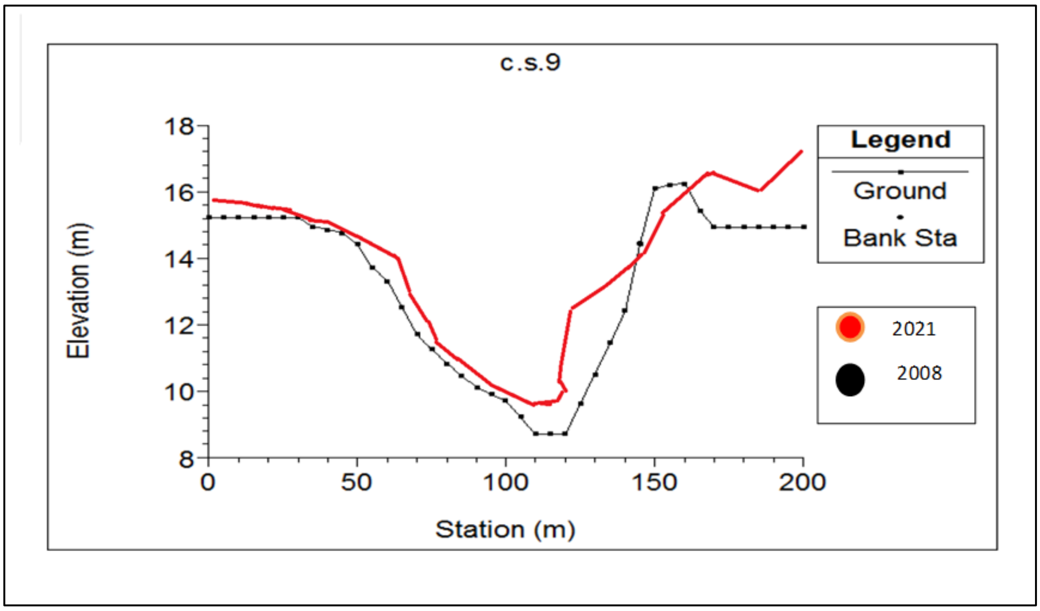


Figure 2: Changing in geometry shape of station 4+500 of downstream Gharraf Regulator

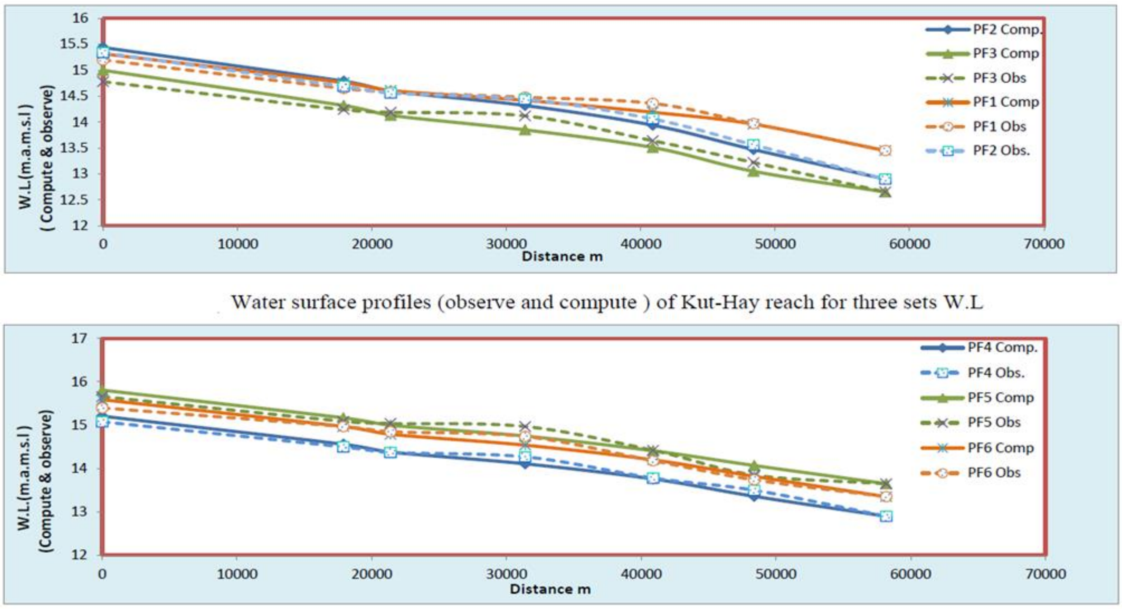
b. Boundary conditions:

The survey executed during the winter season of 2012-2014 by the Iraqi Ministry of Water Resources encompassed 86 km of the river, extending from the Al-Gharraf regulator to regulator No. 2, with assessments conducted at intervals of 250 meters (some cross sections were performed at shorter intervals, particularly at meanders), as illustrated in the figure. The results of this survey have been utilized in the current study to develop a one-dimensional constant flow model with the HEC-RAS software, incorporating supplementary data regarding the positions and dimensions of the bridges.

The average discharge of the river at Kut-Nasiriyah, computed over the past thirteen years, along with supplementary discharge data from prior studies (Al-Arrar 2018), has been utilized in the model to establish the downstream conditions, and a revised rating curve for the river segment between the Gharraf regulator and regulator No. 4 downstream boundary has been developed for each of the reach conditions.

c. Model calibration in (HEC-RAS):

The model was calibrated using observed water levels. Twenty-two cross sections were assessed along the Kut-Hay stretch. Figure 3.3. The sites of the surveyed cross sections. The Acoustic Doppler Current Profiler (ADCP) was employed to assess the underwater cross-section, while a total station was utilized to measure distances across the floodplain and banks. The cross sections were sequentially numbered from the downstream end and encompassed the whole research region. Calibration of the Manning's roughness coefficient for the river along the study reach by simulating flows and water depths using the HEC-RAS model. The value (n=0.025) for (125-150) m³/sec yields the minimal R.M.S.E. value. This example exhibits a significant discharge. The diminished water levels are attributable to the complete opening of the Hay Regulator gate at the downstream end of the reach, as illustrated in figure (3), with the observed difference being 0.2 m.



Water surface profiles (observe and compute) of Kut-Hay reach for three sets W.L

Water surface profiles (observe and compute) of Kut-Hay reach for three sets W.L

Figure 3: The water surface profiles (observe and compute) of Kut-Hay reach for three sets W. L.

By knowing the rate of Manning coefficient and other factors, the consumption discharge for both sides was estimated of the lateral inflow / outflow was included within the average inflow from the right sides is 113 m3 s−1. (for more than 50 branches) and left sides is 137 m3 s−1 (for more than 40 branches).

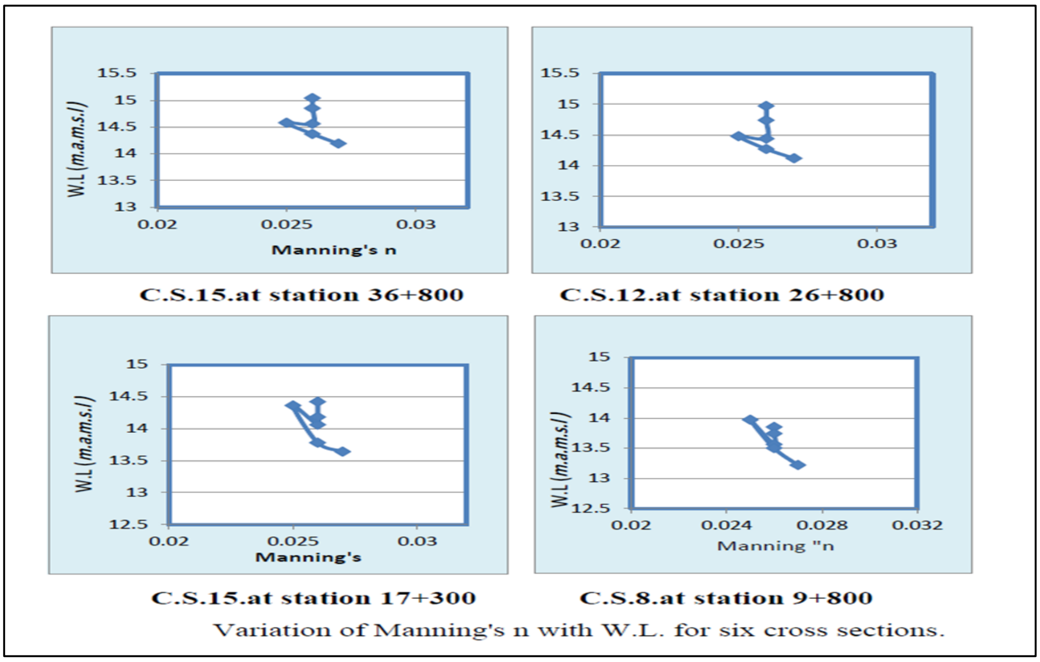
d. Results and discussion:

1- Capacity :

this condition, it’s important to estimate the current flood capacity of the river and to make modification to the cross sections to account for future expected extensive flood. This study was conducted to examine the discharge capacity of the reach of Gharraf River between Gharraf regulator and regulator No.2 for 86 km in length.

This reach had four main lateral outflow on right side about 35 m3/sec they ; dhaeh, mdeleel, hussaina and mrezeaja. Either the left three outflows, Ageel, sheeb northern and southern. The examination includes simulation the current capacity of the reach by using HEC-RAS model. Two hundred twenty five cross sections surveyed in 2010 were used in the simulation. Discharges varied between 100 and 500 m3/s at the downstream Gharraf to regulator No2.

The analysis shows the difference between observed and simulated can be having Manning’s n. 0.026. See Fig (4)



C.S.15.at station 36+800

C.S.12.at station 26+800

C.S.15.at station 17+300

C.S.8.at station 9+800

Variation of Manning's n with W.L. for six cross sections.

Figure 4: the variation of Manning’s n with W.L. for six cross sections.

The model was calibrated utilizing default discharges of 175, 250, 350, and 500 m³/s from the Gharraf River. The findings indicated that the present capacity of the Gharraf River comprises three tiers. The initial downstream Gharraf regulator has a capacity of 300 m³/sec over a distance of 5 km. The second regulator No. 1, equipped with lateral outflows (five branch sides), has a capacity of 250 m³/sec. The third regulator between No. 1 and No. 2, with lateral outflows (two branch sides), has a capacity of 175 m³/sec. The water levels maintained a height of 1 meter below the crest level on both sides. The Gharraf River is incapable of sustaining an operational discharge of 350 m³/s under any circumstances. The reach had a substantial quantity of sediment. Refer to Figure 5.

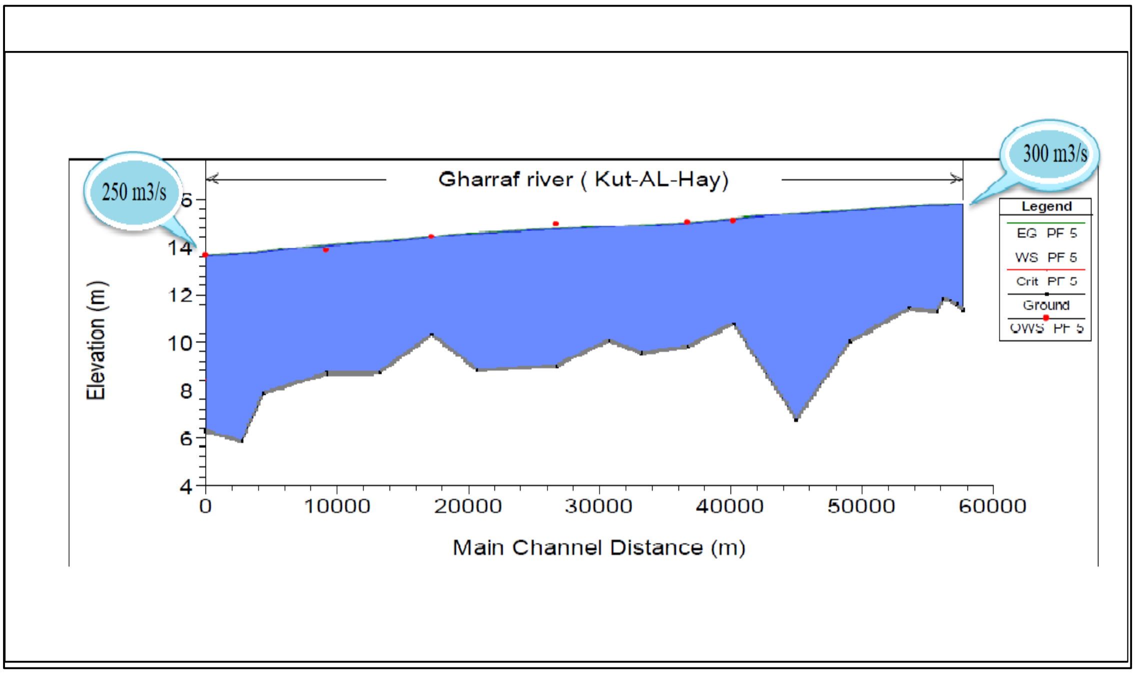


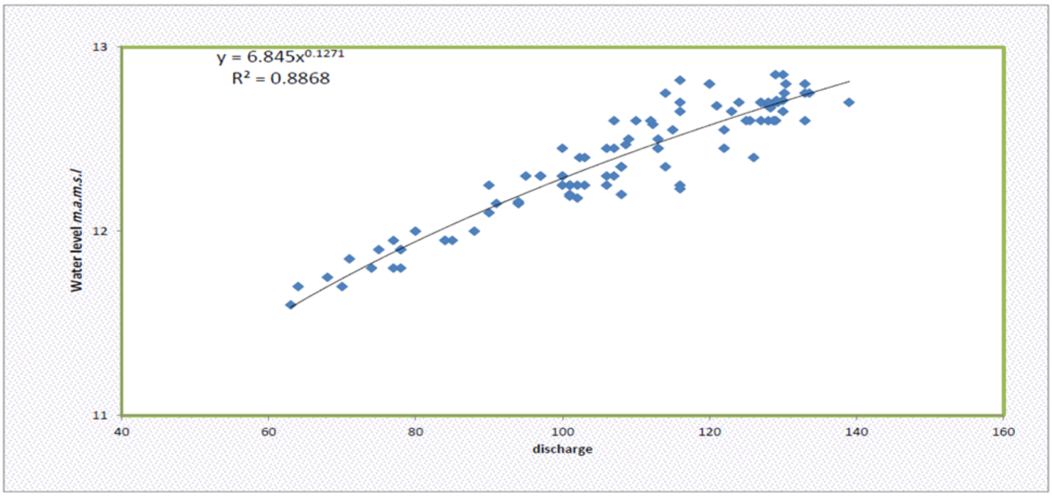
Figure 5: Capacity between Gharraf Reg. and Al-Hay Reg. (NO .1)

2- Rating curve:

The data inputted into the first model were utilized in the rating curve model following the incorporation of Hay Regulator data (inline structure) and additional cross sections to finalize the model.

Ten sets were utilized in the constant flow data. Nine discharges were recorded along the reach for each profile at designated cross sections, as seen in Fig. (6).

The upstream boundary condition is the discharge, whereas the downstream boundary condition is the rating curve at station 0+00 (C.S.1), situated downstream of the Hay Regulator. The rating curve for station 0+00 was derived from data January 2016 to January 2017, as illustrated in Fig. 6 provided by the Ministry of Water Resources (MoWR) for the period spanning .



Rating curve at station 0+00, (C.S.1) downstream Hay regulator

Figure 6: the relation between discharge and water level.

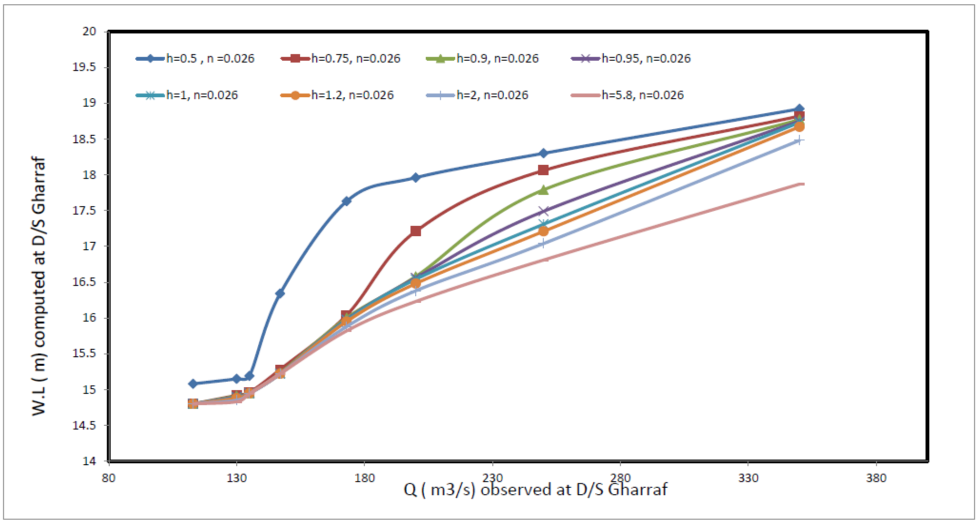
Manning's n coefficient (0.026) and gate openings of (0.5, 0.65 , 0.75, 0.90, 0.95, 1, 1.2, 2, 4,and 5.8(fully) *m*, were adopted to compute the rating curve for upstream reach to investigate the effect of Hay Regulator on upstream reach.

The results show that the effect of Hay regulator on upstream reach where the backwater curve was evident for different cases. The cases may be listed as shown in **table(4)**That mean the Gharraf regulator are affected by Hay regulator operation in all above cases, therefore the rating curve of Gharraf regulator is not valid due to this effect.

Table 5: rating curves in D/S for Gharraf Regulator.

Manning coefficient	gate openings for Hay Reg.	.Discharge in Gharraf Reg.
0.026	Less than (0.5) m	All available discharges
	(0.65-0.9) m	More than 175 m^3/s
	(0.9 – 4) m	More than 210 m^3/s
	(4 – 5.8) m	More than 350 m^3/s

The alteration of the Manning's n coefficient does not influence the rating curve at the upstream reach (gate openings Fully and 1.1), as illustrated in Fig. (7). The influence of Manning's resistance coefficient n on flow depth indicates that increasing n from 0.022 to 0.026 results in an approximate water depth rise of 30 cm, while further increasing n from 0.026 to 0.030 leads to an additional increase of approximately 40 cm in water depth.



Rating curve of upstream reach (C.S.22, downstream Gharraf regulator) for multi gate openings

Figure 7: The rating of upstream reach.

Rating curves were computed for upstream reach included the gate openings (0.5-0.9)*m*, with Manning's n of (0.026). The observed rating curve differs from the computed one and generally lies between the computed rating curves for the gate opening of 0.5*m* to 0.9*m* in Al Hay Regulator

8. Conclusions

- The rate of drainage at D/S Gharraf Regulator is (192 m^3/s) for the period (1985-2003) and it was (146 m^3/s) for the period (2003-2020).

- The difference between most cross-sections due the large sediments carried by the river, because the low slope for Al-Gharraf river.

- Global Manning's n coefficient was calculated steady state average values of all data is (0.026)

- The Kut-Hay reach and Al-Gharraf regulator are affected by Al-Hay regulator due Rating curves.

Reference:

[1] Al-Ghazi, H. S., “Hydrology and Investment of the Gharraf River”, M. Sc Thesis, submitted to Department of Physical Geography, College of Education, University of Basra, 2003**.**

[2] Muhammad, M. W., “The Hydrological Status of the Southern Part of the Lower Tigris and the River Transportation Project”, Dar Al-Kutub for Printing and Publishing, 1993,P107.

[3] Muhammad, M. W., “Saddam River and the Sand Dunes”, Dar Al-Kutub for Printing and Publishing, 1993, P17.

[4] Arrar, A. N., “Hydraulic Simulation of Gharraf River Between Kut and Hay Cities”, M. Sc. thesis submitted to the Department of Water Resources Engineering, College of Engineering, University of Baghdad,2018.

[5] Kharwfa, N., The “Transformations of Iraq's rivers and their impact on urbanization”, The Center for the Revival of Arab Scientific Heritage, Symposium on Irrigation among the Arabs, University Baghdad 1986, p 17.

[6] K.A. Rahi, T. Halihan, Salinity evolution of the Tigris River Reg Environ Change, 18 (7) (2018), pp. 2117-2127

[7] UN-ESCWA, B. United Nations economic and social commission for western Asia; Bundesanstalt für Geowissenschaften und Rohstoffe. Inventory of Shared Water Resources in Western Asia, Beirut; 2013.

[8] Partow H. The Mesopotamian Marshlands: Demise of an Ecosystem. Early Warning and Assessment Technical Report, 2001, UNEP/DEWA/TR. 01-3. Rev. 1. Division of Early Warning and Assessment.

[9] HEC. H.E.C., Discharge for selected gauges station in Iraq (1930- 1956). Bennie Deacon and Gourley (London) in association; 1958.

[10] HEC. H.E.C., Hydrological Survey of Iraq. Bennie, and Partnersin association Main Report, Ministry of Agriculture, Baghdad, Iraq; 1963.

[11] A. Kais, Discharges measurement at stations of Tigris and Euphrates Rivers D. G. Water resource management, Ministry of water resources (2008)

[12] Bruce JL, Greenwood MM, Jones SZ. Water-Resources Investigations in Wisconsin, 2004, Geological Survey Washington DC; 2004.

[13] Wurbs RA, James WP. Water resources engineering. Prentice-Hall; 2002.

[14] G. Braca, Stage-discharge relationships in open channels: Practices and problems Univ. degli Studi di Trento, Dipartimento di Ingegneria Civile e Ambientale (2008)

[15] H.A. Hussein, A.H. Alshami, Evaluation o the hydrological behavior in the greater zab river basin, Int J Civ Eng Technol, 9 (19) (2018), pp. 204-258

[16] H.A. Hussein, Dependable discharges of the upper and middle diyala basins, J Eng, 16 (2) (2010), pp. 4960-4969

[17] A.-S.-T. Al-Madhhachi, K.A. Rahi, W.K. Leabi, Hydrological impact of ilisu dam on mosul dam; the river tigris Geosciences, 10 (4) (2020), p. 120

[18] D.A. Solodovnikov, S.S. Shinkarenko, Present-Day Hydrological and Hydrogeological Regularities in the Formation of River Floodplains in the Middle Don Basin, Water Resour, 47 (6) (2020), pp. 977-986

[19] V.K. Keteklahijani, S. Alimohammadi, E. Fattahi, Predicting changes in monthly streamflow to Karaj dam reservoir, Iran, in climate change condition and assessing its uncertainty, Ain Shams Eng J, 10 (4) (2019), pp. 669-679.

[20] M. Zakwan, Z. Ahmad, Analysis of sediment and discharge ratings of Ganga River, India, Arab J Geosci, 14 (19) (2021), pp. 1-15

[21] A.S. Rahman, Z. Khan, A. Rahman, Application of independent component analysis in regional flood frequency analysis: Comparison between quantile regression and parameter regression techniques, J Hydrol, 581 (2020), Article 124372

[22] M. Zakwan, Spreadsheet-based modelling of hysteresis-affected curves, Appl Water Sci, 8 (4) (2018), pp. 1-5

[23] D. Faulkner, S. Warren, P. Spencer, P. Sharkey, Can we still predict the future from the past? Implementing non-stationary flood frequency analysis in the UK, J Flood Risk Manage, 13 (1) (2020), 10.1111/jfr3.12582

[24] G.R. de Souza, *et al.*, Regional flood frequency analysis and uncertainties: maximum streamflow estimates in ungauged basins in the region of Lavras, MG, Brazil, Catena, 197 (2021), Article 104970.

[25] H. Tiwari, S.P. Rai, N. Sharma, D. Kumar, Computational approaches for annual maximum river flow series, Ain Shams Eng J, 8 (1) (2017), pp. 51-58.

[26] M. Niazkar, M. Zakwan, Z.M. Yaseen.(2021). Assessment of artificial intelligence models for developing single-value and loop rating curves, Complexity, 2021 (2021), pp. 1-21.

[27] H. Yeung. An examination of BS3680 4C (ISO/DIS 4369) on the measurement of liquid flow in open channels—flumes Flow Meas Instrum, 18 (3-4) (2007), pp. 175-182.

Antibiofilm activity of Serratia marcescens purified gelatinase against Pseudomonas aeroginosa isolates

Nehad A. Taher [1]

Batool Abd Al Ameer Baqer [2]

Rusul A.A. Alshammary [3]

Abstract

Most bacteria can produce biofilms on avariety of surfaces in nature and it represents an important virulence factors such as the biofilm based infections by *Pseudomonas aeruginosa* can be life -threatening for people pationsand they can also lead to a long term infection. About 22 of *Serratia marcescens* clinical isolates were collected and characterized by morphological and biochemical tests even thogh PCR method .

All the 22 isolates were screened for gelatinase production by culturing them on gelatine agar medium and the results showed that the *S. m*. no. 16 was the highest gelatinase producer which gave a lysis area of (28)mm in diameter as a primary and qualitative detection of this enzyme, also, crude extraction and quantitative detection were carried out by preparing of cell-free culture (CFS) and detection of protein concentration of this crude extract to be equal to 12.144 by Bradford method. Purification of gelatinase was done by three steps: precipitation (80%) saturation of ammonium sulfate, followed by dialysis, ion exchange chromatography utilizing DEAE -Cellulose and gel filtration chromatography throughout Sephaeryl S-200 column. The results showed that *S. marcescens* 16 (S 16) gelatinase was obtained with specific activity of 3.75U\mg of protein with a fold of purification of about 49.23. Also, purified S16 gelatinase was characterized and the results showed that its molecular weight was 68 kDa by electrophoresis method (SDS-PAGE).

S16 gelatinase and gentamicin's minimum inhibitory concentrations (MIC) were calculated using broth microdilution. Purifie gelatinase was tested for antibacterial activity at 8-16-32-64 µg/ml in vitro using the agar well diffusion method against five isolates of *P. aeruginosa* that were multidrug resistant. Antibiofilm activity of purified gelatinase at sub-MIC was more effective than the antibiofilm activity of gentamicin ($P < 0.01$), and the gelatinase was high active than the gentamicin in a preventing the production of biofilm. Gentamicin and purified gelatinase both possess significant antibacterial activity against *P. aeruginosa* isolates as compared with control.

An aim of research is on the possible using gelatinase purified from *S. marcescens* as an alternative therapeutic antibacterial agent against multidrug resistant(MDR) *P. aeruginosa* isolates.

Key Words: *Serratia Marcescens, Pseudomonas Aeruginosa, Purified Gelatinase, and Antibiofilm Activity.*

http://dx.doi.org/10.47832/RimarCongress03-7

[1] College of Science, Mustansiriyah University, Baghdad, Iraq dnihad74@uomustansiriyah.edu.iq

[2] College of Science, Mustansiriyah University, Baghdad, Iraq batoolalsafar@uomustansiriyah.edu.iq

[3] College of Science, Mustansiriyah University, Baghdad, Iraq rusulabood.mc.s.zoo.2020@uomustansiriyah.edu.iq

Introduction

Serratia marcescens is an opportunistic, gram-negative, nosocomial pathogen that belongs to Enterobacteriaceae. Several environmental and numerous clinical strains of S. marcescens produce prodigiosin a red pigment. It was discovered by Bizio, an Italian pharmacist, in 1819, when The recognized it as a reason of the bloody dis-coloration of cornmeal mush (Khanna et al.,2019)]. S. marcescens was first thought to be undamaging (non-pathogenic). by reason of its capability to produce red pigmentation, it was first used in 1906 as a marker to trace bacterial activity or transmission. It was not until later in the 1950s that the US government researches with the S. marcescens and its damaging effects (Luthra et al., 2014). S. marcescens causes urinary and respiratory infections, endocarditis, osteomyelitis, septicemia, wound infections, eye infections, and meningitis (Buckle, 2015) . S. marcescens presents in two cell forms, which are short rods, and displays two kinds of motility by few flagella according on the type of growth surface encountered. In a broth medium, and illustrate classical swimming actions. During growth on a solid surface, they differentiate into elongated, multinucleate, copiously flagellated forms that swarm over the agar surface (O,Rear et al.,1992).

Serratia spp. Such as S. marcescens, S. liquefaciens, S. fonticola, S. rubidaea, S. plymuthica, S. marnorubra, S. odorifera, and S. proteamaculans, produce a variety of extracellular enzymes which increase its virulence including proteases, lipase, alpha-amylase, gelatinase, caseinase, chitinases, nuclease, etc. The secretion and activity of extracellular enzymes are a fundamental component of microbes' metabolic processes. These enzymes can perform several functions as breaking down the organic substrates into simpler molecules, having a role in industrial and pharmaceutical applications. They are used in detergent production, for instance, the use o protease, amylase, and lipase in removing stains at much lower temperatures. The usage of enzymes in detergent formulations also reduces the use and handling of solvents and toxi compounds.

Enzymes increase the virulence of bacteria, for example, Bacterial lipases play an essential role in the pathogenicity of gram(-ve) and gram(+ve) bacteria. They have been considered virulence factors due to their hydrolysis activity against host cell membrane phospholipids resulting in membrane rupture and release of intracellular nutrients. Furthermore, they can inhibit bacterial phagocytosis by alveolar macrophages that modulate the host immune response to bacterial infection and contribute to bacterial resistance I development (Ibrahim et al., 2021). The characteribation of infectantcrobial enzymes is important for understanding their role in the pathogenesis of infectious diseases and improving their application in biotechnology (Sharma 2005). Morcover, M.Os exist an excellent source of enzymes rather than plants or animals due to their advantages as (Ahmed et al., 2019).

It be able to grow in a shorter period. Natural abundance poor. Required limited zone for cell cultivation. Generate a specialized enzyme. The potential for genetic manipulation to produce new enzymes appropriate for numerous applications. This study focus on the ability of Serratia marcescens to produce many extracellular enzymes that can be important for many applications (Ohgiya et al., 1999), such as: Alpha-amylase: catalyzes hydrolysis (splitting a compound by adding a water molecule) a - 1, 4 glycosidic bindings of starch into smaller carbohydrate molecules such as glucose (Elyasi Far et al.,2020). Therefore, Amylase is a second type of enzyme used in a structure of enzymatic detergent. Also used in the food industry

Lipase: which catalyzes a hydrolysis of fats and oils to free fatty acids, glycerol, diglycerides, and monoglycerides. Lipase enzymes are used in diverse applications including the food industry (lipase utilizes to separate milk fat with gives desirable flavors to the cheese. Strong flavor cheeses) (Houde et al ., 2004), detergent industry, fats and oil industry, pulp, and paper industry, leather industry, textile industry, in organic synthesis, production of biodiesel cosmetics production (Garcia et al., 2017). It's also involved in fat-digesting supplements (Putri et al., 2021).

DNase: Deoxyribonuclease (DNase) enzymes are capable of degrading DNA by catalyzing the hydrolytic split of phosphor diester links in the DNA backbone (Varela –Rameriz et al., 2017). The extracellular DNase of Serratia could effectively disperse the biofilms of clinical pathogenic bacteria (Staphylococcus aureus, Klebsiella pneumonia, Escherichia coli, Enterococcus feacalis, Proteus Vulgaris, and Pseudomonas aeruginosa,) leads to a decrease in strength of biofilm matrix and as a result, make them high sensitive to the antibiotic treatment. Also, DNase is used in distinguishing S. marcescens from closely related members of the Enterobacteriaceae (Klebsiella-Enterobacter) since Klebsiella and Enterobacter do not produce DNase (Kranthi et al ., 2014).

Caseinase: which catalyzes the analyses of casein (milk protein) into small peptides and individual amino acids, Caseinase is used in the milk and dairy industry (Aehle ,2007) .

Gelatinase is specific protease that hydrolyze gelatin (which is a fibrous protein gets by thermal denaturation or partial hydrolysis of collagenous materials such as bovine skins and also demineralized bones) (Mad-Ali et al., 2017) to amino acids. This enzyme has been found in chemical, medical, and food processing (Ekpenyong et al., 2017).

Pseudomonas aeruginosa created siderophore, a rust agent, and iron vision systems are widely thought to be critical for bacterial development (Claudel et al., 2020). Due to iron-binding proteins such as transferrin in blood and lactoferrin in mucosal secretions, which are components of innate immunity and offer protection against pathogens, iron is not readily available in the host system under natural settings. P. aeruginosa uses siderophore units like pyoverdine and pyochelin to get beyond host defenses. These siderophores have unique structural and functional characteristics, and they can also chelate ferric ions (Mahdi et al., 2022).

Most bacteria can produce biofilms on a variety of surfaces in nature (Sharma et al., 2020). A biofilm is a complex aggregate of bacteria wrapped in a selfgenerated matrix of (EPS) extracellular polymeric substances (Da Silva et al., 2019), and it is one of the major strategies for species survival when environmental conditions change unexpectedly, such as temperature ature and nutrition availability or a existence of antimicrobial agents (Moser et al., 2021). Biofilm-based infections by P. aeruginosa can be life-threatening for people with cystic fibrosis, and they can also lead to a long-term infection (Kamali et al., 2020).

The main components of the P. aeruginosa biofilm matrix include proteins, polysaccharides, extracellular DNA (eDNA), and lipids. A 3 exo polysaccharides Psl , Pel, and alginate are crucial for surface adhesion, biofilm formation, and the stability of the biofilm morphology (Oluyombo et al., 2019). (Rewatkar and Wadher et al., 2013) noted that some environmental factors, such as nutrient and oxygen availability, appear to cause bacteria to develop biofilms (Mahdi et al., 2019). Gram positive and gram negative bacteria, including E.

faecilis, Bacillus spp., S. aureus, and yeasts like candida spp., as well as K. pneumonia, P. mirabilis, and Salmonella enteritidis, can all produce biofilms.

There are five major phases of a biofilm: Through their flagella and pili, planktonic bacteria attach to the surface of the biomaterial in the initial phase.

In the second phase, cells form microcolonies and secrete polymeric extracellular materials. As a result of the surface's and the matrix's cells' close interaction, the binding is irreversible. At this phase, exopolysaccharides, eDNA, rhamnolipids, type-IV pili, siderophores, and flagella all participate to the formation and attachment of a biofilm matrix (Muhammad et al., 2020). Third phase involves coordinating social activities within the group by organizing gene control in a variety of bacterial populations via quorum sensing (Maura et al., 2016). The biofilm creates a three-dimensional architecture in fourth phase, shieldingit from the host's defenses and drugs. Fifth phase sees the biofilm attain a critical mass and spread out to establish itself in different places (Moormeier , Bayles et al., 2017).

The production of biofilms, which serve as a fundamental component of pathogen physiology, an adhesive foundation, a defense barrier that prevents the detachment of embedded cells, and a source of diverse diseases, is the main factor in nosocomial infections (Zhang et al., 2020). Nosocomial pathogens frequently develop novel drug resistance, which is a general issue with nosocomial infections. Patients with nosocomial infections, particularly those in the intensive care unit (ICU), frequently isolate multidrug-resistant (MDR) strains of P. aeruginosa. It can be challenging to treat P. aeruginosa infections because the bacteria can develop drug resistance. This resistance develops because bacteria have the capacity to create biofilms, which are made up of bacterial colonies encased in an.

Materials and Methods

Isolation and Identification of Bacterial isolates

A total of 22 S. marscence were collected from urine clinical samples, also, only 5 isolates of highly antibiotic resistant P. aeruginosa were collected from different clinical sources. Both of them were identified as in Bergey,s manual of systematic bacteriology ,second edition to guide the biochemical and morphological test s used during this study (Forbes et al., 2007).Even though PCR method.

The Qualtitive Detection of Gelatinase production

S. marcescens isolates were cultured in LB broth underneath aerobic conditions at 37°C for 48hours, then centrfuged at 3000 rpm at 4°C and 100ml of colony free supernatant (cfs)were transferred to twells on gelatine agar media and incubated at 37°C for 48 hours then the diameter of lysis area were measured in millimeter's and represent a single for gelatinase production by tested isolates

Quantitive Detention of Gelatinase production

A quantitive experiment was carried out using the technique outlined by (Mad-Ali et al., 2017) to asses the enzyme activity and protein concentration of all strain.

production of S16 Gelatinase

The optimized fermentation mediumwas composed of (g/1L) gelatin 30g, tryptone 10g, sodium chloride 10g and agar 15g (Mad-Ali et al., 2017). The 50mL of this medium in Erlen-Meyer flasks 250ml were inoculated with 5mL Inoculums (6.2 x10 CFU/mL). These flasks were incubated at 30°C for 60 hr. on the orbital shaker. After that at 10000 g for 12min. a microbial suspension was centrifuged ,and a clear supernatant was assayed for gelatinase activity.

Purification and determination of the molecular weight of S16 Gelatinase

At 80% saturation of ammonium sulphate $(NH_4)_2SO_4$, the culture supernatant was subjected, and after over night preservation at 4°C, a precipitated enzyme solution was separated by centri fugation (10000 g, 15min.), next was dis- solved in phosphate buffer (0.25 mol/L, pH 7.5). After that a gelatinase enzyme was desalinated at (0.5mL/min.) with phosphate buffer (0.25 mol/L, pH 7.5) by a Sephadex G- 25 column (0.9 x 30cm). The enzyme was concentrated by ultrafiltration membrane (Millipore, USA) using centri- fuge (6000 g, 25 mint.). lastly, a partially purified enzyme was passed through a di-ethyl-amino-ethyl (DEAE) cellulose column (3 x 20cm) and active enzyme was eluted by Tris - HCI pH 8.5 with a gradient of NaCl (0.1- 0.6 mol/L) at the flow rate of 2mL/min.. The fractions with enzyme activity were collected, concentrated by lyophili- zation and used for further experiments.

Gelatinase from the DEAE cellulose column was loaded on to sodium dodecyl sulfate polyacrylamide - gel 12% electrophoresis (SDS-PAGE) following the method of Laemmli (1970). A molecular weight (M.W.) of gelatinase was determined by comparing its mobility with the medium moved by range marker proteins (14.3-97.2 kDa). Protein concentration was measured by the Lowry method.

According to (Lewus and Montville et al., 1991), the antibacterial activity of purified Gelatinase generated by S16 marescens against five isolates of P. aeruginosa at the concentration (8, 16, 32, 64) µg/mL was detected using the agar well diffusion technique (Mahdi et al., 2017).

Determination of MIC and sub-MIC for gentamicin and purified Gelatinase

Different quantities of gentamicin and purified Gelatinase (1-1024 µg/ml) were dissolved in MHB (Muller - Hinton broth) in a 96 well polystyrene microtiter plate using the microdilution technique described by(Hasson et al., 2021) by using Resazurin stain. With the exception of the positive control wells. Each well, received bacterial suspension (10 µl) compare to 0.5 McFarland standard, Resazurin 0.015% was added to all wells (30 µL per well) and incubated for an additional 2-4 hr. to observe any color change after 24hr. at 37°C. After the incubation period was through, were columns with no color change (the blue resazurin color stayed the same) given a score over the MIC value.

Antibiofilm effect of purified Gelatinase on P. aeruginosa biofilm formation in vitro

The biofilm development assay followed the same procedure as follow:- The 180 µl of B.H.I. broth containing 2 percent sucrose, 20 µl of bacterial suspension were employed as an overnight culture used to inoculate a 96-well flat-bottomed microtiter plate with Each isolation was performed in triplicate, with the control wells containing 200 µl of Brain heart infusion broth with 2percent sucrose used to inoculate. The plates were allowed to air dry for 15 minutes before the adherent bacteria were fixed for 15 minutes in each well with 200 µl of 99 percent ethanol. After being decanted, the plates were given time to completely dry. - The wells were treated with 1% crystal violate for 15 minutes. The adherent cells' dye was dissolved in 200 µl of ethanol.-ELI-SA readers were used to measuring the absorbance of each well at 630 nm.

However, BHIB has sub-MIC levels of gentamicin and Gelatinase separately. For 24 hours, the plates were incubated at 37°C. Following that, each well was cleaned, stained, and read at 630 nm. Additionally, positive controls were carried out by adding 200 µl of fresh bacterial culture (compatible to the 0.5 McFarland standard) devoid of gentamicin and Gelatinase. According to (Hasson et al., 2021), every assay has been performed.

Results and Discussion

Microorganisms

The 22 isolates were characterized morphologically and biochemically and the results showed that all the 22 tested isolates were related to Serratia marscens as in table .1 (Forbes et al., 2007). The identification was verified by using molecular detection especially for S. marscence isolates as in figure .1.

The results of the qualtitive detection of gelatinase production was demonstrated as in figure .2 that revealed the S16 marscens showed the maximum gelatinase productivity of (28 mm in diameter of lysis area on gelatinase agar medium) as in table .2 and figure .2.

Table 1: Biochemical tests of S. marscens isolates

Biochemical Test	Results
Oxidase	-
Catalase	+
Gram stain	-
Indol	-
Voges Proskaur	+
Motility	+
Urease	+
Citrate	+
Pigmented	+

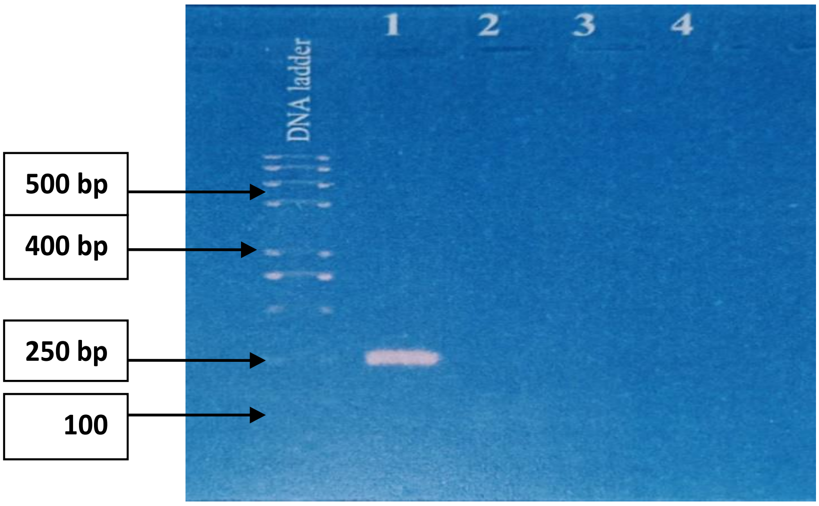


Figure 1: Agarose gel – electro-phoresis of PCR products for S16 isolate (line 1 of 250 bp in size) 1.5 % gel agarose was used to detect the gene at 100 voltage for 45 min .DNA was run alongside the sample to detect the sample size.

Table 2: Screening for Gelatinase production among S. marscens isolates

Isolate Number	Diameter in mm of lysis area
1	18
2	20
3	23
4	22

5	18
6	18
7	21
8	23
9	19
10	19
11	21
12	21
13	20
14	18
15	18
16	28
17	21
18	24
19	23
20	23
21	22
22	19

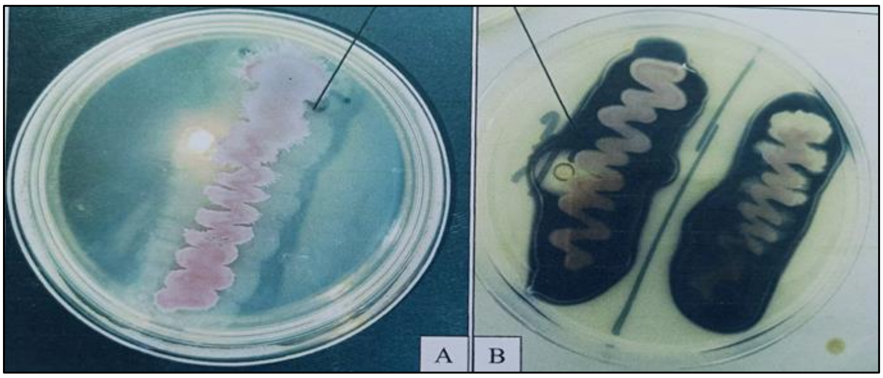


Figure 2: Qualtitive Detection of Gelatinase production by S. marscens isolates .

A: Before the addition of an indicator. B: After the addition of an indicator .

Purification of S16 m Gelatinase

Purification of an enzyme was executed during the following steps: ammonium sulphate $(NH_4)_2SO_4$ precipitation, a Sephaeryl S-200 column, and DEAE cellulose column chromatography. Each purification steps are summarized in Table 3., which show 40.43-fold purification with a recovery of 2.12 % and specific activity of 3.23 U/mg protein.

Figure 3. The SDS-PAGE experiments illustrated that a gelatinase enzyme reaches electrophoresis type of purity with a molecular mass of approximately 68.0 kDa calculated by using Syngene G: BOX (USA).

Table 3: Purification of S16 Gelatinase

Fraction	Volume	Total activity (U\ ml)	Total protein (mg\ml)	Specific activity (U\mg)	Purification fold	Yield (%)
Crude extract	100	6500	4.32	1.50	1.00	100
		5.40	2.33	3.74	2.47	68.60
DEAE – Cellulose	8	4.26	1.19	3.41	2.33	45.23
Sephaeryl S-200	6	3.20	0.86	3.23	2.12	40.43

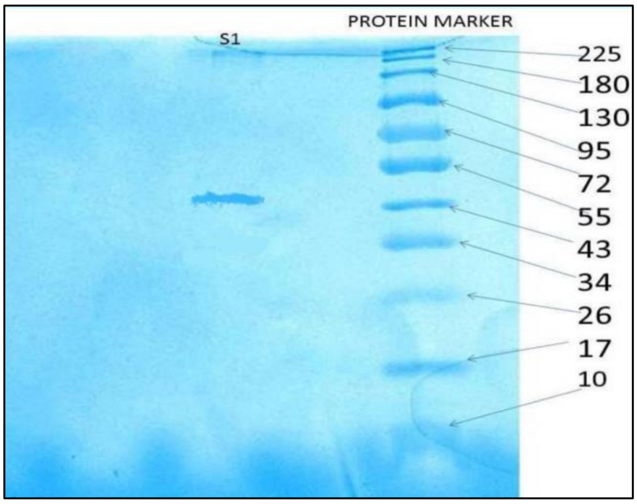


Figure 3: Detection of S16 Gelatinase (S1) molecular weight by SDS-PAGE method .

Antibacterial activity of purified S16 Gelatinase against P. aeruginosa in vitro

This part was done by well diffusion method and the results showed that the S16 Gelatinase has considerable antibacterial activity aganst 5 MDRwith strong biofilm P. aeruginosa isolates .compared to control (P 0.01) , and that this activity was stronger at a concentration of 64 g \ml against all isolates than it was at a concentration of 8 m \ml (table .4) .

As showen the greatest antibactrial activity of this enzyme against P. aeruginosa NO.3was achieved 28.12 mm at a concentration of 64 m \ml . Other study showed that the Glutaminase recorded maximum antibacterial activity against P. areuginosa isolate (18.4 mm) at a concentration of (64 g\ml) (Hasson et al ., 2021).

Table 4: Antibacterial activity of purified Gelatinase on P. aeruginosa Isolates.

S16 Gelatinase concentration µg\ml						
Bacterial Isolates	**64 µg \ml**	**32 µg\ml**	**16 µg\ml**	**8 µg\ml**	**D.W.**	**P-value**
1	*15.5±0.4c*	13.12±0.6*	11.16±0.6*	9.44±0.6*	0±0	0.01SIG
2	*17.5±0.6c*	15.16±1.08*	13.15±0.4*	11.33±0.8*	0±0	0.01SIG
3	*28.12±0.6c*	20.5±0.6*	16.00±0.2*	11.4±0.8*	0±0	0.01SIG
4	*18.33±1.4c*	16.16±0.6*	12.4±0.8*	7.6±0.8*	0±0	0.01SIG
5	*24.5±1.9c*	18.33±0.7*	16.14±1.02*	10.16±6*	0±0	0.01 SIG

C: Propability compared to other concentration p 0.01.*: Propability compared to control p 0.01 .

The antibiofilm activity of S16 Gelatinase and Gentamicin sub-MIC by ELISA technique

The antibiofilm activity of S16 Gelatinase and gentamicin sub-MIC in microtiter plate. S16 Gelatinase and Gentamicin were tested at sub-MIC concentrations for their inhibitory effects on P. aeruginosa biofilm production. The results of treating the bacterial isolates with sub-MIC levels of Gentamicin and S16 Gelatinase reveal the bacterial isolates were sensitive to these antibiotics, and the production of biofilms is also reduced. In comparison to gentamicin ((0.544 ±0.06, 0.67 ± 0.06, 0.780 ± 0.09, 0.687 ± 0.01 and 0.502 ± 0.05) and purified S16 gelatinase (0.731 ± 0.08, 0.454± 0.05, 0.967 ± 0.03, 0.435 ± 0.08 and 0.645 ± 0.05 respectively)the OD of the biofilm of five P. aeruginosa isolates before treatment is significantly higher (P<0.01) than the control(before treatment), but purified S16 Gelatinase inhibits the biofilm more effectively Table(5).

Table 5: Antibiofilm activity of S16 Gelatinase and Gentamicin sub –MIC

Bacteria OD	Before Treatment	After Treatment		P-value
		S16 Gelatinase	Gentamicin	
		Mean SD		
Ps 6	1.233 ± 0.066	0.731 ± 0.08	0.544 ± 0.06	< 0.01**
Ps 16	0.987 ± 0.043	0.454 ± 0.05	0.67 ± 0.06	< 0.01**
Ps 20	1.861 ± 0.08	0.967 ± 0.03	0.780 ± 0.09	< 0.01**
Ps 28	1.112 ± 0.13	0.435 ± 0.08	0.687 ± 0.01	< 0.01**
Ps 32	1.762 ± 0.09	0.645 ± 0.05	0.502 ± 0.05	< 0.01**

LSD: Least Significance Difference ,ANOVA Test was usedto compare between data ,P: Probability : Significance at 0.01.

S16 Gelatinase activity as an antibiofilm agent was higher than the activity of the gentamicin in vitro, MIC values of S16 Gelatinase and gentamicin used to treat biofilms of former isolates. There was a significant difference in optical density before and after S16 Gelatinase treatment (P <0.01). The significant antibiofilm activity of purified S16 Gelatinase was observed against the tested isolates of P. aeruginosa (Hasson et al., 2021)

Mahdi et al., 2021 reported using sub-MIC concentrations of gentamicin and amikacin to reduce the growth of biofilms on plastic sheets. Sub-inhibitory aminoglycoside concentrations cause P. aeruginosa Secretary System VI to form biofilms (Jones et al., 2017).

Despite certain studies showing that, depending on the antibiotic class and the bacterial strain, antibiotics could significantly increase biofilm development, in general, biofilm generation was suppressed by antibiotics (Zhang et al., 2020). This variation may be regarded as normal due to the types of studied isolates and their origins, as well as the genetic makeup of the isolates and the laboratory condition that preceded the detection of the sub-MIC.

Conclusions

S. marcescens is an opportunistic pathogen of concern, harbouring a variety of virulence factores and enzymes .

S16 Gelatinase was purified with single protein band of 68 kDa that has antibacterial activity against MDR P. aeruginosa (5) selected isolates .

Purified S16 Gelatinase was more effective as an antibiofilm agent comparing with Gentamicin in vitro .

Refrences:

[1] Ahmed, S.A., Saleh, S., Abdel-Hameed, S., and Fayad, A.M., (2019). Catalytic, kinetic,c, and thermodynamic properties of free and immobilized caseinase on mica glass-ceramics. Heliyon, 5(5), e01674.

[2] Black, W. A., Hodgson, R., and McKechnie, A., (1971): Evaluation of three methods using deoxyribonuclease production as a screening test for Serratia marcescens. Journal of Clinical Pathology, 24, 313-316.

[3] Buckle, J., (2015). Infection Clinical Aromatherapy, 130-167.

[4] Ekpenyong, M., Asitok, A., Odey, A., and Antai, S., (2017). Production and activity kinetics of gelatinase by Serratia sp.SLO3. Nigerian Journal of Biopesticides, 1 (1): 70-82.

[5] Elder, B. L., Trujillo, I. N. E. S., and Blazevic, D.J., (1977). Rapid deoxyribonuclease test with methyl green. Journal Of Clinical Microbiology, 6(3), 312-313.

[6] Elyasi Far, B., Ahmadi, Y., Yari Khosroshahi, A., and Dilmaghani, A., (2020). Microbial Alpha-Amylase Production: Progress, Challenges, and Perspectives. Advanced pharmaceutical bulletin, 10(3), 350-358.

[7] Garcia-Silvera, E. E., Martinez-Morales, F., Bertrand, B., Morales-Guzman, D., Rosas- Galván, N. S., León-Rodriguez, R., and Trejo-Hernández, M.R., (2017). Production and application of a thermostable lipase from Serratia marcescens in detergent formulation and biodiesel production. Biotechnology and Applied Biochemistry, 65(2), 156-172.

[8] Gürkök, S., (2019). Microbial enzymes in detergents: a review. Int J Sci Eng Res, 10(9), 75-81.

[9] Haenni, M., Bour, M., Châtre, P., Madec, J. Y., Plésiat, P., and Jeannot, K., (2017). Resistance of animal strains of Pseudomonas aeruginosa to carbapenems. Frontiers in Microbiology, 8, 1847.

[10] Hasan, K. A., Hussein, A. S., and Mohammed, T. K., (2021). Detection of Lasb and Pich Genes in Pseudomonas Aeruginosa Isolated From Urinary Tract Infections by PCR Technique. Annals of the Romanian Society for Cell Biology, 25(6), 123-134.

[11] Hashim, I. and Pharma, S., (2013). Microbiological culture media in pharmaceutical industry. Foster city, USA: OMICS Group eBooks. Hasson, B., Mahdi, L., &Essa, R. (2021). Evidence of AntioxidantActivity of Novel L-Glutaminase Purified from L. Gasserí BRLHM. Journal of Applied Sciences and Nanotechnology. 1(4), 44-51.

[12] Hill, D., Sugrue, I., Tobin, C., Hill, C., Stanton, C., and Ross, R.P., (2018). The Lactobacillus casei group: history and health related applications. Frontiers in microbiology.

[13] Houde, A., Kademi, A., and Leblanc, D., (2004). Lipases and Their Industrial Applications: An Overview. Applied Biochemistry and Biotechnology, 118(1-3), 155-170.

[14] Ibrahim, U. H., Devnarain, N., Omolo, C. A., Mocktar, C., and Govender, T., (2021). Biomimetic pH/lipase dual responsive vitamin-based solid lipid nanoparticles for on- demand delivery of vancomycin. International Journal of Pharmaceutics, 607, 120960.

[15] Khanna, A., Khanna, M., and Aggarwal, A., (2013). Serratia marcescens- a rareopportunistic nosocomial pathogen and measures to limit its spread in hospitalized patients. Journal of clinical and diagnostic research: JCDR, 7(2), 243-246.

[16] Kranthi, U.S., Yamarthi, A.,and Jonnalgadda, S., (2014). Biofilm dispersal activity of DNase produced by Serratia sp. YAJS. Int. J. Curr.Microbiol. App.Sci, 3(6) 839-849.

[17] Krieg, N.R. Sneath, P.H. Staley, J.T. and Willians, S.T. (1994). Hotterbeekx, A. Kumar-Singh, S. Goossens, H. and Malhotra-Kumar. S., (2017). in vivo and in vitro Interactions between Pseudomonas aeruginosa and Staphylococcus spp. J. Front. Cell. Infect. Microbiol. 2(4),345-350.

[18] Laemmli UK., (1970). Cleavage of structural proteins during the assembly of the head of bacteriophage T4. Nature. 1970;227:680-685.

[19] Lovell, D. J., and Bibel, D. J., (1977). Tween 80 medium for differentiating nonpigmented Serratia from other Enterobacteriaceae. Journal of clinical microbiology, 5(2), 245-247. 25.LUZ, B. D., Sarrouh, B., Bicas, J. L., and Lofrano, R. C., (2021). Lipase production by microorganisms isolated from the Serra de Ouro Branco State Park. Anais da Academia Brasileira de Ciências, 93.

[20] Lowry, OH., Rosebrough, NJ., and Farr, AL., (1951). Protein measure- ment with the Folin phenol reagent. J Biol Chem. 1951;193(1):265-275

[21] Luthra, U., Singh, N. K., Bhosle, V., Gupte, V., and Patil, R. R., (2014). Media Optimization for Serratiopeptidase by Statistical Approach followed by Isolation and Product Purification. International Journal of scientific research and management(IJSRM), 2(11) 1608-1614.

[22] M Orabi, H., El-Fakharany, E. M., Abdelkhalek, E. S., and Sidkey, N. M., (2021). L-asparaginase and L-glutaminase: sources, production, and applications in medicine and industry. Journal of Microbiology. Biotechnology and Food Sciences, 2021, 179-190.

[23] Mad-Ali, S., Benjakul, S., Prodpran, T., and Maqsood, S., (2017). Characteristics and gelling properties of gelatin from goatskin as affected by drying methods. Journal of food science and technology, 54(6), 1646-1654.

[24] Maharem, T. M., Emam, M. A., and Said, Y. A., (2020). Purification and characterization of L-glutaminase enzyme from camel liver: Enzymatic anticancer property. International journal of biological macromolecules, 150, 1213-1222.

[25] Mahdi, L. H., Jabbar, H. S., and Auda, I. G., (2019). Antibacterial immunomodulatory and antibiofilm triple effect of Salivaricin LHM against Pseudomonas aeruginosa urinary tract infection model. International Journal of Biological Macromolecules, 134, 1132-1144.

[26] Mahdi, L., Al Mathkhury, H. J. F., Sana'a, A. K., Rasool, K. H., Zwain, L., Mahdi, L.H. Ali, R. L. Kadhim, H.Y. Ibtesam, G. A. and Rajwa, H. E., (2021). Eatsblishing novel roles of bifidocin LHA, antibacterial, antibiofilm and immunomodulator against Psedomonas aeruginosa corneal infection model. Internati. J. Biologi.

[27] Mahdi, L.H. Ghufran, N. A. and Ibtesam, G. A.(2020). Evidence of anti-K pneumoniae biofilm activity of Novel Entrococcus faecalis enterocin GLHM. Microbi. Pathogene. 104366.

[28] Ohgiya, S., Hoshino, T., Okuyama, H., Tanaka, S., and Ishizaki, K., (1999). Biotechnological Applications of Cold-Adapted Organisms, 17-34.

[29] Olsen, H.S.O., and Falholt, P., (1998). The Role of Enzymes in Modern Detergency. Journal of Surfactants and Detergents 1, 555-567.

[30] O'Rear, J., Alberti, L., and Harshey, R. M., (1992). Mutations that impair swarming motility in Serratia marcescens 274 include but are not limited to those affecting chemotaxis or flagellar function. Journal of bacteriology, 174(19), 6125-6137.

[31] Putri, M. H., Handayani, K., Setiawan, W.A., Damayanti, B., Ratih, C. L.,and Arifiyanto, A., (2021). Screening of Extracellular Enzymes on Serratia marcescens strain MBC1. Jurnal Riset Biologi dan Aplikasinya, 5(1): 23-29. 15. Achle, W., (2007). Enzymes in Industry, 99-262.

[32] Sharma, A., and Tiwari, R., (2005). Extracellular enzyme production by environmental strains of Serratia spp. isolated from river Narmada. Indian journal of biochemistry and biophysics, 42(3), 178-181.

[33] Sigmon, J., (2008). The starch hydrolysis test. American Society for Microbiology (ASM).

[34] Taherikalani, M., Maleki, A.. Karimi, S and Sadeghifard, N. (2014). The correlation between the presence of quorum sensing, toxin-antitoxin system genes and MIC values with ability of biofilm formation in clinical isolates of Pseudomonas aeruginosa. Iranian journal of microbiology, 6(3), 133.

[35] Varela-Ramirez, A., Abendroth, J., Mejia, A. A., Phan, L. Q., Lorimer, D. D., Edwards, T. E., and Aguilera, R. J. (2017). Structure of acid deoxyribonuclease. Nucleic acids research, 45(10), 6217-6227.

[36] Zakaria, A. S., Edward, E. A., and Mohamed, N. M. (2019). Evaluation of ciclopirox as a virulence-modifying agent against multidrug resistant pseudomonas aeruginosa clinical isolates from Egypt. Microbiology and Biotechnology Letters, 47(4), 651-661.

[37] Zawistowska-Rojek, A., and Tyski, S. (2018). Are probiotic really safe for humans?. Polish journal of microbiology, 67(3), 251-258.

[38] Zeshan, B., Karobari, M. I., Afzal, N., Siddiq, A., Basha, S., Basheer, S. N., and Noorani, T. Y. (2022). The Usage of Antibiotics by COVID-19 Patients with Comorbidities: The Risk of Increased Antimicrobial Resistance. Antibiotics, 11(1), 35.-

[39] Zhang, L., Liang, E., Cheng, Y., Mahmood, T., Ge. F., Zhou, K., and Tan, Y. (2020). Is combined medication with natural medicine a promising therapy for bacterial biofilm infection?. Biomedicine and Pharmacotherapy, 128, 110184.

PURE SCIENCES, APPLLED SC

مؤتمر ريمار الدولي الثالث للعلوم الصرفة والتطبيقية

III.International Rimar Congress of Pure, Applied Sciences

ISBN 978-625956420-3