



Faculty of Information and Communication Technology



**ECG ENCRYPTION ENHANCEMENT WITH MULTI-LAYERS OF
AES AND DNA COMPUTING**

Jamal Kh-Madhloom

Doctor of Philosophy

2023

**ECG ENCRYPTION ENHANCEMENT WITH MULTI-LAYERS OF AES AND
DNA COMPUTING**

JAMAL KH-MADHLOOM

**A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy**



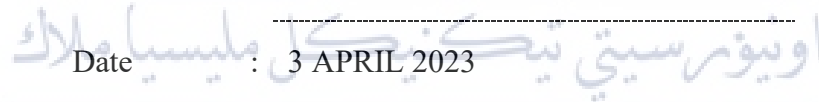


UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION


I declare that this thesis entitled “ECG Encryption Enhancement With Multi-Layers Of AES and DNA Computing“ is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

 Signature : 
Name : JAMAL KH-MADHLOOM
Date : 3 APRIL 2023 

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Doctor of Philosophy.

Signature : 

Supervisor Name : PROFESSOR DR. MOHD.
KHANAPI ABD. GHANI

Date : 3 APRIL 2023

اونيورسيٲى ٲيكنيكل مليسيا ملاك
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DEDICATION

I am dedicating this thesis to my beloved family, especially my parents, my mother, and wife, who have supported me throughout my life. They are always persistent in providing me the assistance and encouragement to push forward. This thesis is a humble and sincere acknowledgment of their graciousness given to me during my journey.



ABSTRACT

The Internet of Things (IoT), which is defined as a network of interconnected computing devices, mechanical and digital machines, and objects with unique identifiers (UIDs), which are able to transmit data across a network without requiring human-to-human or human-to-computer interactions, is currently a hot topic in the scientific community. This is due to the fact that IoT is defined as a network of interconnected computing devices, mechanical and digital machines, and objects with UIDs. IoT study fields currently involve security and privacy due to the fact that the installation of Cryptographic Internet Communications "ICs" for protected IC applications like Fog Computing and Cloud Computing devices is extremely crucial in any developing technology. Devices that use the internet of things for DNA sequence testing also require a high level of expertise in the application of public-key cryptography. Using brute force techniques, it is possible, in theory, to decipher any key if one has sufficient processing capacity. In order to more effectively incorporate both present technology and developing technology, models of DNA cryptography need to be developed. MATLAB 2017b, a reliable simulation method, was utilised throughout the construction and validation of the algorithm. The performance of the recommended approach makes it possible to thwart an attack using brute force considerably more fast than is possible with the encryption technologies that are currently in use. Evaluations of algorithms reveal that the proposed algorithm has achieved a level of security and complexity that is 48 times superior to that of other methods that have been tried and tested. The solution that has been suggested is one that is both secure and effective when it is put to use in conjunction with the ECG and Covid-19 image encoding algorithms. A reference electrocardiogram (ECG) signal as well as the Covid-19 image dataset were utilised in the validation and analysis of the recommended method. The pairing-based encryption known as "DNA sequence Enhanced Advanced Encryption Standard (EAES)" can be used to protect medical ECG signals that are stored in the cloud for healthcare purposes using the nebula network architecture. The proposed method indicates the feasibility of constructing such a dependable DNA sequence system in such a manner that it can be applied and integrated with either the biological environment or on DNA computers. This possibility is demonstrated by the fact that this system can be built. The proposed model is able to protect the DNA sequence stored in the Fog Computing cloud from plain text attacks by generating (I) the main key, which is the key to the EAES encryption algorithm, (II) the rule 1 key, which represents the DNA base number of possible key probabilities, and (III) the rule 2 key, which represents the number of binding probabilities for the DNA helical structure. These three keys are referred to collectively as the EAES encryption key. The construction of this key prioritises the highest possible level of safety.

PENINGKATAN ENKRIPSI ECG DENGAN PELBAGAI LAPISAN AES DAN PENGKOMPUTERAN DNA

ABSTRAK

Internet of Things (IoT), yang ditakrifkan sebagai rangkaian peranti pengkomputeran yang saling berkaitan, mesin mekanikal dan digital, dan objek dengan pengecam unik (UID), yang mampu menghantar data merentasi rangkaian tanpa memerlukan manusia ke manusia atau interaksi manusia-ke-komputer, kini menjadi topik hangat dalam komuniti saintifik. Ini disebabkan oleh fakta bahawa IoT ditakrifkan sebagai rangkaian peranti pengkomputeran yang saling berkaitan, mesin mekanikal dan digital serta objek dengan UID. Bidang kajian IoT pada masa ini melibatkan keselamatan dan privasi kerana pemasangan "IC" Komunikasi Internet Kriptografi untuk aplikasi IC yang dilindungi seperti Pengkomputeran Awan dan peranti Pengkomputeran Awan adalah amat penting dalam mana-mana teknologi yang sedang membangun. Peranti yang menggunakan internet perkara untuk ujian jujukan DNA juga memerlukan tahap kepakaran yang tinggi dalam aplikasi kriptografi kunci awam. Menggunakan teknik 'brute', adalah mungkin, secara teori, untuk menguraikan sebarang kunci jika seseorang mempunyai kapasiti pemprosesan yang mencukupi. Untuk menggabungkan kedua-dua teknologi semasa dan teknologi yang sedang dibangunkan dengan lebih berkesan, model kriptografi DNA perlu dibangunkan. MATLAB 2017b, kaedah simulasi yang boleh dipercayai, telah digunakan sepanjang pembinaan dan pengesahan algoritma. Prestasi pendekatan yang disyorkan memungkinkan untuk menggagalkan serangan menggunakan 'brute' dengan jauh lebih pantas daripada yang mungkin dengan teknologi penyulitan yang sedang digunakan. Penilaian algoritma mendedahkan bahawa algoritma yang dicadangkan telah mencapai tahap keselamatan dan kerumitan yang 48 kali lebih tinggi daripada kaedah lain yang telah dicuba dan diuji. Penyelesaian yang telah dicadangkan adalah penyelesaian yang selamat dan berkesan apabila ia digunakan bersama dengan algoritma pengekodan imej ECG dan Covid-19. Isyarat elektrokardiogram (ECG) rujukan serta set data imej Covid-19 telah digunakan dalam pengesahan dan analisis kaedah yang disyorkan. Penyulitan berasaskan pasangan yang dikenali sebagai "DNA jujukan Enhanced Advanced Encryption Standard (EAES)" boleh digunakan untuk melindungi isyarat ECG perubatan yang disimpan dalam awan untuk tujuan penjagaan kesihatan menggunakan seni bina rangkaian nebula. Kaedah yang dicadangkan menunjukkan kemungkinan untuk membina sistem jujukan DNA yang boleh dipercayai sedemikian rupa sehingga ia boleh digunakan dan disepadukan dengan sama ada persekitaran biologi atau pada komputer DNA. Kemungkinan ini ditunjukkan oleh fakta bahawa sistem ini boleh dibina. Model yang dicadangkan mampu melindungi jujukan DNA yang disimpan dalam awan Pengkomputeran Awan daripada serangan teks biasa dengan menjana (I) kunci utama, yang merupakan kunci kepada algoritma penyulitan EAES, (II) kunci peraturan 1, yang mewakili nombor asas DNA kemungkinan kebarangkalian kunci, dan (III) kekunci peraturan 2, yang mewakili bilangan kebarangkalian mengikat untuk struktur heliks DNA. Ketiga-tiga kunci ini dirujuk secara kolektif sebagai kunci penyulitan EAES. Pembinaan kunci ini mengutamakan tahap keselamatan setinggi mungkin.

ACKNOWLEDGEMENTS

سَمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ * الَّذِي عَلَّمَ بِالْقَلَمِ * أَقْرَأْ وَرَبُّكَ الْأَكْرَمُ * خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ * أَقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ

صدق الله العظيم

(1-5) سورة العلق

First and foremost, praise is to Allah for giving me this opportunity, the strength, and the patience to complete my thesis finally, after all the challenges and difficulties.

My utmost appreciation goes to my main supervisor, Professor Dr. Mohd. Khanapi Abd. Ghani, from Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM) for all his support, advice and inspiration.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

TABLE OF CONTENTS

| | PAGE |
|--|-------------|
| DECLARATION | |
| APPROVAL | |
| DEDICATION | |
| ABSTRACT | i |
| ABSTRAK | ii |
| ACKNOWLEDGEMENTS | iii |
| TABLE OF CONTENTS | iv |
| LIST OF TABLES | vii |
| LIST OF FIGURES | x |
| LIST OF ABBREVIATIONS | xii |
| LIST OF PUBLICATIONS | xiii |
| | |
| CHAPTER | |
| 1. INTRODUCTION | 1 |
| 1.1 A review of cryptography | 1 |
| 1.2 Cryptography and information security | 2 |
| 1.3 Research background | 5 |
| 1.4 Research gap derivation | 7 |
| 1.5 Problem statement | 8 |
| 1.6 Research questions | 10 |
| 1.7 Research objective | 11 |
| 1.8 Scope of research | 11 |
| 1.9 Contribution of research | 12 |
| 1.10 Thesis outline | 13 |
| | |
| 2. LITERATURE REVIEW | 15 |
| 2.1 Introduction | 15 |
| 2.1.1 Telemedicine systems using IoT-based healthcare devices | 18 |
| 2.1.2 Telemedicine systems using IoT-based healthcare applications | 21 |
| 2.1.3 Security and privacy challenges for IoT and fog computing | 37 |
| 2.2 Cryptography background | 39 |
| 2.2.1 Advanced Encryption Standard (AES) | 40 |
| 2.3 Classification of cryptographic procedures | 48 |
| 2.3.1 Symmetric key algorithm | 48 |
| 2.3.2 Asymmetric key algorithm | 48 |
| 2.4 Existing cryptographic algorithms | 50 |
| 2.4.1 Data Encryption Standard (DES) | 50 |
| 2.4.2 Triple Data Encryption Standard (T-DES) | 51 |
| 2.4.3 Educational Data Encryption Standard (E-DES) | 52 |
| 2.4.4 BLOWFISH | 53 |
| 2.4.5 Rivest Cypher 2 (RC2) | 54 |
| 2.4.6 Rivest Cypher 4 (RC4) | 55 |
| 2.4.7 Rivest Cypher 6 (RC6) | 55 |

| | | |
|-----------|--|-----------|
| 2.4.8 | Rivest, Shamir and Adleman (RSA) | 56 |
| 2.4.9 | Elliptic Curve Cryptography (ECC) | 58 |
| 2.4.10 | Diffie-Hellman (DH) | 59 |
| 2.4.11 | ElGamal Encryption System (EES) | 60 |
| 2.4.12 | Digital Signature Algorithm (DSA) | 60 |
| 2.5 | Deoxyribonucleic Acid (DNA) | 62 |
| 2.5.1 | DNA structure and central dogma | 62 |
| 2.5.2 | DNA computing | 64 |
| 2.5.3 | Comparison of DNA and conventional electronic computers | 68 |
| 2.6 | Related works in telemedicine systems focusing on data security | 68 |
| 2.7 | Features of IoT devices for telemedicine | 69 |
| 2.8 | Earlier research and methods for DNA computing and data encryption | 72 |
| 2.9 | Summary | 75 |
| 3. | RESEARCH METHODOLOGY | 77 |
| 3.1 | Introduction | 77 |
| 3.2 | Research paradigm (Research framework) | 78 |
| 3.2.1 | Literature phase | 79 |
| 3.2.2 | Research Design (Design phase) | 79 |
| 3.3 | Development phase | 80 |
| 3.3.1 | Programming phase | 81 |
| 3.3.2 | Evaluation phase | 82 |
| 3.4 | Validation methods of the proposed model | 84 |
| 3.4.1 | Quantitative evaluation | 84 |
| 3.4.1.1 | Correlation coefficients | 84 |
| 3.4.1.2 | Histogram analysis | 85 |
| 3.4.1.3 | MSE | 85 |
| 3.4.1.4 | Correlation analysis | 85 |
| 3.4.1.5 | Entropy analysis and differential analysis metrics | 86 |
| 3.4.1.6 | Structural Content (SC), Normalised Absolute Error (NAE), Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) analysis | 88 |
| 3.4.1.7 | Benchmarking | 89 |
| 3.4.1.8 | Dataset | 90 |
| 3.5 | Summary | 93 |
| 4. | PROPOSED ENCRYPTION ENHANCEMENT WITH MULTI-LAYERS OF AES AND DNA COMPUTING (EEML-AES-DNA-M) | 94 |
| 4.1 | Introduction | 94 |
| 4.1.1 | EEML-AES-DNA-M algorithm design considerations | 95 |
| 4.1.2 | Proposed algorithm design metrics | 97 |
| 4.2 | Algorithm model | 98 |
| 4.3 | Algorithm model steps | 104 |
| 4.3.1 | ECG binarisation “Pre-Processing” | 104 |
| 4.3.2 | Image binarisation “Pre-Processing” | 104 |
| 4.3.3 | Converting to DNA | 105 |
| 4.3.4 | SubBytes layer | 106 |
| 4.3.5 | ShiftRow operation | 108 |

| | | |
|-----------|--|------------|
| 4.3.6 | Mix Columns operation | 109 |
| 4.3.7 | AddRoundKey operation | 110 |
| 4.3.8 | DNA swapping | 112 |
| 4.3.9 | Proposed algorithm pseudo code | 113 |
| 4.4 | Summary | 113 |
| 5. | RESULTS AND ANALYSIS | 115 |
| 5.1 | Introduction | 115 |
| 5.2 | Test conditions | 115 |
| 5.2.1 | ECG signal Quality Assessment Metrics (ECGQAMs) | 116 |
| 5.3 | Performance evaluation metrics | 117 |
| 5.3.1 | Execution time encryption | 117 |
| 5.3.2 | Security performance metrics | 117 |
| 5.3.2.1 | Keyspace | 117 |
| 5.4 | Experimental and security analysis | 118 |
| 5.4.1 | Encryption and decryption time analysis | 119 |
| 5.4.2 | ECG signal encryption security analysis | 119 |
| 5.4.2.1 | Keyspace analysis | 121 |
| 5.4.2.2 | Histogram analysis | 122 |
| 5.4.2.3 | Correlation analysis | 127 |
| 5.4.2.4 | Correlation analysis of original and encrypted ECG signal | 140 |
| 5.4.2.5 | Information entropy analysis | 142 |
| 5.4.2.6 | Mean Square Error (MSE) | 143 |
| 5.4.3 | Covid-19 encryption security analysis | 145 |
| 5.4.3.1 | Analysis of encryption and decryption times | 145 |
| 5.4.3.2 | Histogram analysis | 145 |
| 5.4.3.3 | Correlation analysis | 147 |
| 5.4.3.4 | Entropy analysis and differential analysis metrics | 151 |
| 5.4.3.5 | Structural Content (SC), Normalized Absolute Error (NAE), Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) analysis | 151 |
| 5.5 | Summary | 154 |
| 6. | CONCLUSION AND RECOMMENDATIONS | 155 |
| | REFERENCES | 158 |

LIST OF TABLES

| TABLE | TITLE | PAGE |
|-------|--|------|
| 2.1 | Advantages and disadvantages of AES (Sabry et al., 2015) | 44 |
| 2.2 | AES enhancement attempts | 46 |
| 2.3 | Symmetric and asymmetric cryptography comparison (Ma Jin, 2018) | 49 |
| 2.4 | Advantages and disadvantages of DES | 50 |
| 2.5 | Capabilities of T-DES | 51 |
| 2.6 | Advantages and disadvantages of RC4 | 55 |
| 2.7 | Encryption and decryption procedures for RSA | 57 |
| 2.8 | Advantages and disadvantages of RSA | 57 |
| 2.9 | Advantages and disadvantages of ECC | 58 |
| 2.10 | Advantages and disadvantages of DH | 59 |
| 2.11 | Advantages and disadvantages of EES | 60 |
| 2.12 | Advantages and disadvantages of DSA | 61 |
| 2.13 | Comparison between DNA-based and conventional computers (Cardelli, 2013) | 68 |
| 2.14 | Comparison of features available in IoT devices in telemedicine | 70 |
| 2.15 | AES enhancing attempts using DNA Encryption | 73 |
| 3.1 | The operational structure for literature phase | 79 |
| 3.2 | Operational design phase structure | 80 |
| 3.3 | The structural operational research design for development phase | 80 |

| | | |
|------|--|-----|
| 3.4 | The structural operational research design for implementation phase | 81 |
| 3.5 | Performance evaluation process | 82 |
| 3.6 | Simulation machine specifications | 84 |
| 3.7 | Original X-ray image samples | 92 |
| 4.1 | DNA rule 1 | 105 |
| 4.2 | S-Box table (Abood and Guirguis, 2018) | 107 |
| 4.3 | Inverse S-Box table (Abood and Guirguis, 2018) | 108 |
| 5.1 | ECG signal quality metrics | 116 |
| 5.2 | The execution times of encryption and decryption with various rounds “Signal length=1000” | 120 |
| 5.3 | Decryption breaking time results | 121 |
| 5.4 | ECG signal histograms used in the simulations, both the original and encrypted signals | 122 |
| 5.5 | Correlations of the original and encrypted ECG signals on the horizontal, vertical, and diagonal axes | 128 |
| 5.6 | The correlation of original and encrypted ECG signals “Signal length=1000” | 141 |
| 5.7 | Information entropy measurements of the original and encrypted ECG signals “Signal length=1000” | 142 |
| 5.8 | MSE of “Signal length=1000” | 144 |
| 5.9 | Encryption and decryption time with different rounds “299*299 X-Ray” | 145 |
| 5.10 | Histograms (original and encrypted Covid 19 image dataset) | 146 |
| 5.11 | Correlations of original and encrypted X-ray images | 148 |
| 5.12 | The correlation between original image and cypher-image | 150 |

| | | |
|------|---|-----|
| 5.14 | MSE of “Signal length=1000” | 151 |
| 5.15 | Original, encrypted and decrypted X-ray image samples | 152 |



LIST OF FIGURES

| FIGURE | TITLE | PAGE |
|--------|--|------|
| 1.1 | Research gap derivation | 8 |
| 2.1 | Cogsense modules | 19 |
| 2.2 | Internet of Things implementation in healthcare | 22 |
| 2.3 | Process of Cryptograph (Wang et al., 2018) | 40 |
| 2.4 | Flowchart of AES algorithm (Albahar et al., 2018) | 41 |
| 2.5 | Symmetric key cryptography (Jain and Bhatnagar, 2014) | 48 |
| 2.6 | Asymmetric key cryptography (Jain and Bhatnagar, 2014) | 49 |
| 2.7 | Flowchart of DES algorithm (Ahmad et al., 2015) | 51 |
| 2.8 | A flowchart of T-DES algorithm (Jain and Bhatnagar, 2014) | 52 |
| 2.9 | Flowchart of E- Encryption Standard (Jain and Bhatnagar, 2014) | 53 |
| 2.10 | Flowchart of BLOWFISH encryption and decryption algorithm (Tang et al., 2018) | 54 |
| 2.11 | Flowchart of RC2 algorithm (Tang et al., 2018) | 54 |
| 2.12 | Flowchart of RC4 algorithm (Tang et al., 2018) | 55 |
| 2.13 | Flowchart of RC6 Algorithm (Chaturvedi and Gupta, 2016) | 56 |
| 2.14 | Flowchart of RSA Algorithm (Al-Wattar et al., 2015) | 58 |
| 2.15 | Digital signature Algorithm RSA (Venkataraman and Sadasivam, 2019) | 61 |
| 2.16 | DNA Structure (Shakhovska et al., 2020) | 64 |
| 2.17 | DNA conversion process | 68 |

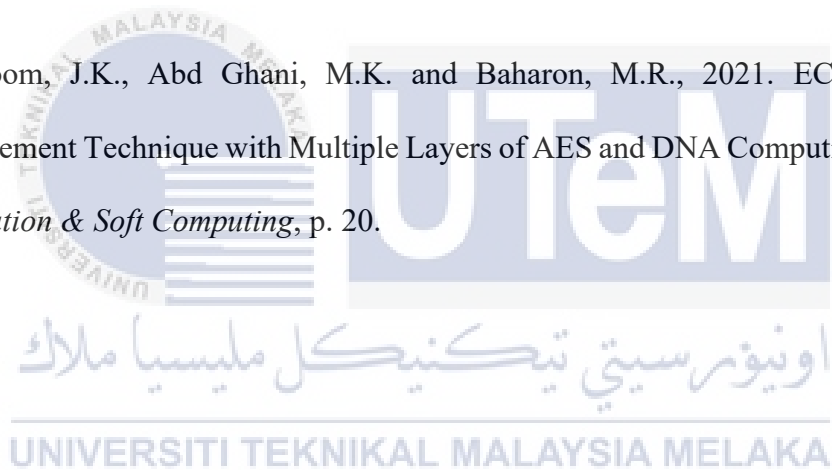
| | | |
|------|---|-----|
| 3.1 | Research methodology phases | 78 |
| 3.2 | Evaluation steps flowchart | 83 |
| 3.4 | MIT-BIH arrhythmia dataset samples | 91 |
| 4.1 | Flowchart of the Encryption process on ECG signal | 100 |
| 4.2 | Flowchart of the Decryption process on ECG signal | 101 |
| 4.3 | Flowchart of the Encryption on Covid-19 image | 102 |
| 4.4 | Flowchart of the Decryption on Covid-19 image | 103 |
| 4.5 | Flowchart of the ECG pre-processing | 104 |
| 4.6 | Flowchart of the greyscale image pre-processing | 105 |
| 4.7 | Sample of DNA helix conversion (Abood and Guirguis, 2018) | 106 |
| 4.8 | SubBytes operation representation (El Hennawy et al., 2014) | 106 |
| 4.9 | Transformations using SubBytes and the inverse of SubBytes (El Hennawy et al., 2014) | 107 |
| 4.10 | ShiftRows structure (El Hennawy et al., 2014) | 109 |
| 4.11 | ShiftRows schema (El Hennawy et al., 2014) | 109 |
| 4.12 | Mix columns operations (El Hennawy et al., 2014) | 110 |
| 4.13 | Process to generate key round (El Hennawy et al., 2014) | 111 |
| 4.14 | AddRoundKey operation (El Hennawy et al., 2014) | 111 |
| 4.15 | DNA swapping (Ping et al., 2019) | 112 |

LIST OF ABBREVIATIONS

| | | |
|----------------|---|--------------------------------------|
| AES | - | Advanced Encryption Standard |
| DES | - | Data Encryption Standard |
| DES | - | Digital Signature Algorithm |
| DH | - | Diffie-Hellman |
| DNA | - | Deoxyribonucleic Acid |
| ECC | - | Elliptic Curve Cryptography |
| E-DES | - | Educational Data Encryption Standard |
| E-DES | - | Educational Data Encryption Standard |
| EES | - | ElGamal Encryption System |
| IoT | - | Internet of Things |
| LFSR | - | Linear Feedback Shift Register |
| LSB | - | Least Significant Bit |
| RSA | - | Rivest, Shamir and Adleman (RSA) |
| T-DEA or 3-DES | - | Data Encryption Standard |
| WSN | - | Wireless Sensors Network |

LIST OF PUBLICATIONS

1. Madhloom, J.K., Abd Ghani, M.K. and Baharon, M.R., 2021. Enhancement to the patient's health care image encryption system, using several layers of DNA computing and AES (MLAESDNA). *Periodicals of Engineering and Natural Sciences*, Vol.9, pp. 928-947.
2. Madhloom, J.K., Abd Ghani, M.K. and Baharon, M.R., 2021. ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing. *Intelligent Automation & Soft Computing*, p. 20.



CHAPTER 1

INTRODUCTION

1.1 A review of cryptography

Cryptography is a science that guarantees the securities of messages and communications of information. Cryptanalysis, the other sub-discipline, tries to compromise or circumvent cryptographic stability. Cryptography and cryptoanalysis are based on mathematics. Cryptography is commonly synonymous with encryption, translation of data and knowledge into a kind not authorised by an individual to access the information. Historically, cryptography was used to encrypt coded messages used in military and diplomatic correspondence. Based on this traditional definition, cryptography can be viewed as a science of encryption and message decryption, where the primary concern was to protect a message if it was leaked to someone other than the intended receiver (Nagaraj et al., 2015).

With the rise of the knowledge economy, where the exchange of classified information by untrusted media has become a prevalent activity, the use of cryptography has become a standard practice for both companies and individuals. The data continuum has surpassed the range of information sharing and entertainment in technical, research and medical ISM domains (Nagaraj et al., 2015).

Recent cryptography applications have seen cryptography rather than encryption and decryption. Although encryption and decryption methods are used to secure sensitive information where secrecy is required, encryption enforces other facets of information

protection. This includes message authentication, sender and recipient, message integrity, and message transmission non-repudiation (Ogiela and Ogiela, 2018). The word cryptography used today encompasses techniques and applications used to encrypt both stored and distributed knowledge.

1.2 Cryptography and information security

The ultimate aim of cryptography in general information and communication systems is to accomplish the following four core information security aims, including preserving and transmitting information and data. These priorities apply to general communication processes. Some communication schemes have more distinct targets depending on this system's architecture, protocols, transmitting media and end-user devices (Dogra and Kohli, 2016).

Confidentiality: also referred to as "Privacy" or "Secrecy," confidentiality means that data and knowledge can only be obtained by people who can see and use this information. Encryption is used to shield unauthorised communication disclosure by making it unintelligible to unauthorised individuals. Registered information users could decrypt and access the message information. If the encryption and decryption keys were kept private, unauthorised individuals intercepting this message could not interpret and comprehend the message (Hamamreh et al., 2018).

Integrity: preserving knowledge and data integrity means that it is modified by approved systems only. Unauthorised modifications include adding, removing, and replacing data components. Cryptography can prevent and track unauthorised modifications

(Hamamreh et al., 2018). This is usually achieved by adding a cryptographic signature to protected records.

Authentication: The practice of identifying and verifying the identities of data access or contact process parties is known as authentication. Authentication provides access and validity of data transfers by providing a method to validate the identity of accepted parties or individuals. Authentication may be applied to data sharing entities, accessed or shared in a transaction, or to all entities and data. Typically verified validity elements are data sender and source, point of origin, date and period of origin, and real data (Gordon et al., 2019).

Non-repudiation: non-repudiation forbids a data exchange party from declining to engage in the contract, and both communications parties could not deny that the contact node did not transmit a response while non-repudiation is introduced into the cryptographic process (Gordon et al., 2019).

Meanwhile, Fog Computing's architecture introduces new protection and privacy problems that conventional security and privacy algorithms cannot address. SES algorithms were developed and applied in various Fog Computing scenarios and network architectures. Therefore, Fog Computing technology situations cannot follow their security and privacy solutions. These technologies considered the availability, confidentiality, integrity and privacy of the network architecture they are deployed in, whereas recent Telemedicine developments have extended their deployments and applications. This introduced new protection and privacy problems that shaped our study context.

A quick analysis of different cryptography algorithms was made in section 2.4, the outcome of this comparison explicitly shows that each algorithm has its limitation and power depending on domain scenario demands. There are various output metrics for each

application. These include encryption time, decryption time, memory use, avalanche effect, entropy and number of bits required for optimum encoding (Wahid et al., 2018). Telemedicine's application demands over Fog Computing vary from the comparable scenario in all ways, so that the comparative algorithms cannot be explicitly implemented in Fog Computing Telemedicine implementations without recognising their distinct cryptography metrics.

Implementing authentication algorithms like RSA and AES encryption algorithms is not adequately safe for applications like cloud computing and fog computing in telemedicine and healthcare applications. It was shown that attackers could successfully get encrypted data (Bhardwaj et al., 2016) and find a way to get the original decrypted data copy.

Based on the above results related to the implementation of AES and other encryption algorithms, this study aims to design a new encryption model that can resolve security issues and challenges while using Fog computing in the IoT network environment (Pereira et al., 2017), where large amounts of data are produced from a broad range of heterogeneous end-user devices using different operating platforms.

The suggested algorithm would be introduced with all encryption features based on DNA bit signals rather than combining column measures for an intricate DNA encryption method that is ideal in a biological environment. The algorithm can produce more complicated and longer encryption keys with other encryption metrics such as encryption time, decryption time, memory use, avalanche effect, entropy and number of bits needed for optimal encoding.

1.3 Research background

The Internet of Things (IoT) has improved data collection and delivery while increasing its availability to users of cloud computing and storage services. The IoT environment consists of interconnected physical instruments for data storage and distribution. The Internet of Things (IoT) theory supported the connection between computer programs and the real world. IoT offers numerous prospects in a variety of industries (Rahmani et al., 2018), including healthcare and telemedicine facilities, one of the industries gaining from numerous computer applications based on the IoT. It provides patients with high-quality clinical treatment and improved illness management. Business researchers looked for a solution to create IoT healthcare software that is safer and more effective in order to enhance healthcare services and provide remote care for patients with chronic conditions (Rahmani et al., 2018). These applications use a variety of sensory instruments to collect and control patient data as ECG signals and the Covid-19 dataset. Sensor arrays, cloud-based platforms, programming techniques, and wireless communication sensors are examples of common Internet of Things components (WSN). Sensors are used to capture body data such as ECG signals and the Covid-19 dataset. WSN provides contact facilities (Medvediev et al., 2018). Algorithms process the data gathered to perform the necessary analysis. Additionally, cloud vendors provide data-gathering computing facilities to provide user access (Chacko and Hayajneh, 2018), whether health professionals or patients. Secure and safe in order to increase patient wellbeing, IoT healthcare apps must take into consideration the security and confidentiality threats they bring to patient life as well as other consequences, like invasions of privacy and economic hazards. This chapter addresses IoT healthcare apps' privacy and security concerns by reviewing device architecture elements.

Nodes in Wireless Sensor Networks (WSN) are identified by unique ID numbers. These distinct identifying codes are utilized by sensor nodes to establish connection while assisting nodes in gathering and exchanging smart grid ECG data and Covid-19 information (Elhoseny et al., 2018). As a consequence, the services are distributed using various network equipment. This, however, posed IoT healthcare systems' privacy and security issues (Elhoseny et al., 2018). These problems can be divided into three main categories: problems with data collection, problems with data sharing, and problems with data administration (Manogaran et al., 2018). IoT networks frequently include a cloud computing system that offers a reasonably priced, adaptable, and effective setting. IoT healthcare apps face yet another serious security issue in this regard. Therefore, cloud-related cyber security concerns are crucial. The cloud architecture may, however, have some benefits, such as scale economies that are advantageous to customers (Salahuddin et al., 2018).

Various telemedicine services respond to patients in medical centres and home patients by remote medical procedures. Patient data is stored in a data centre or network running in a fog-based cloud. Cloud also provides connections to different healthcare providers, including transmitting ECG signals to help patients. These facilities are gradually shifting patient care's traditional nature and making surgical practices more sensitive and effective (Abood, and Guirguis, 2018). Healthcare programmes and applications include remote control and warning systems. Data is the most important commodity of these applications since data collected from these procedures is considered critical. This is how it greatly impacts patients' well-being and overall wellness. The consequences of violating these data are always negative, having an effect on the stakeholders' and the system's overall security and privacy. Anonymity and accessibility should also be addressed. Sensitive information should be stored in addition to being guarded against unauthorized access and