Comparative Study in Enhancing AES Algorithm: Data Encryption

[1]Jamal kh-madhloom, Collage of Arts, University of Wasit, Iraq.
jamalkh@uowasit.edu.iq
[2]Prof. Dr.Khanapi Abd Ghan, Department … FTMK , Universiti Teknikal Malaysia Melaka
khanapi@utem.edu.my
[3]Dr. Mohd Rizuan Bin Baharon, Department … FTMK , Universiti Teknikal Malaysia Melaka
mohd.rizuan@utem.edu.my

Abstract: Advanced Encryption Standard (AES) algorithm is defined as the standard algorithm for the encryption of transmitted data packets specially over cloud computing. Therefore, this review was conducted with the aim of studying its enhancing trials based on different methodologies. eleven published review articles were reviewed, these articles have compared encryption standards with respect to certain transmission parameters. The results have clearly concluded that the transmission of data packets over the Internet is considered as a major threat, especially when we talk about the evolution of computation power and quantum computers near epoch, therefore, new solutions have been developed to maintain the issue of authentication and protect data by simultaneous encryption procedures. In addition, the comparative study concludes that enhancing AES algorithm is a promising field for data encryption. The study aims to provide academics with a better awareness of new encryption methods to enhance the performance of data encryption algorithms.

Keywords: AES, DNA, ECC, GEO and MAES.

1 Introduction

Cryptography or data encryption aims to strengthen the security, privacy or confidentiality of data by ciphering data using a variety of Symmetric or Asymmetric key cryptography algorithms such as: Advanced Encryption Standard (AES), Data Encryption Standard (T-DEA or 3-DES), Educational Data Encryption Standard (E-DES), Data Encryption Standard (DES), Triple, BLOWFISH, TWOFISH, SEAL, CAST, RC2, RC4, RC6, Adi Shamir and Leonard Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie Hellman (DH), ElGamal Encryption System (EES), and Digital Signature Algorithm (DSA) (Wang, 2018)(Patel, 2016). The counterpart of cryptography is the cryptanalysis, a term that refers to deciphering the cipher-text by analyzing cipher-text, the function of Cryptanalysis is to produce a strong cipher-text by applying techniques of cryptanalysis to the encrypted data to strengthen the cipher-text. Hackers utilize the capabilities of Cryptanalysis to break into the cipher-text for non-authenticated use of data. Developing a powerful cryptographic algorithm requires the development of both cryptography and cryptanalysis (Priyadharshini, 2013). Figure 2 illustrates the process of cryptography that contains both encryption and decryption processes. for obtaining original message Cryptanalysis breaks the cipher-text, while Cryptography is utilized to strengthen the cipher-text. Recently, many tools such as Frequency Analysis, Morse Code, Substitution are used for breaking the cipher-text like (Wang, 2018).

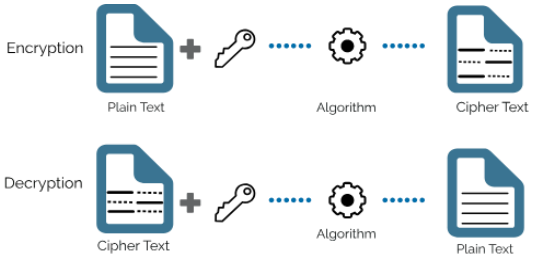

Figure 1: Process of Cryptography (Wang, 2018)

The National Institute of Standards and Technology (NIST) developed AES to replace DES (Singh, 2013). AES requires ten repetitions to encrypt and decrypt data packets, twelve for 192-bit encryption keys, and fourteen for 256-bit encryption keys to create the final encrypted document. Figure 2.4 shows the AES Flowchart. (Latifi) The following activities are required:

SubByte transformation: AES uses 128-bit data blocks; therefore, each database item is 16 bytes. The Rijndael S-box, which has an 8-bit resolution, is used to turn each data record entity into a distinct type of data (Wong et al., 2018).

First, the data in the remaining three rows of the state are shifted from one cycle to another using the ShiftRows transformation. The computer does a one-byte circular shift to the left in the following text. Rows 3 and 4 reverse two-byte and three-byte circular transformations to the right (Dixit et al., 2018). For example, a column-state matrix can be multiplied by a column-state matrix (Ibrahim and Dalklç, 2017). The column vector's values are multiplied by a polynomial matrix of constant values instead of integers. To construct the AddRoundKey transformation, the current state is XORed with the encryption key. As a result, this transformation is diametrically opposite. The transformation process involves several unique phases. Then comes SubBytes, ShiftRows through the round function, Mix Columns, and the AddRound Key transformation (Sabry et al., 2015). This approach is iterative depending on the key length. The decryption process is similar to the process of encryption. The AddRound Key actions, Inv-Mix Columns, Inv-ShiftRows, and Inv-SubBytes make the encryption and decryption key schedules equal (Panghal et al., 2016).

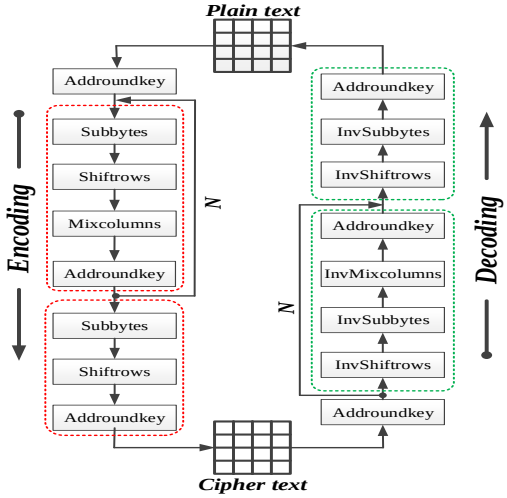

Figure 2: Flowchart of AES Algorithm [5].

In Singh (2013), the DNA computing and the round-reduced AES block cypher were combined, and in the current process, the dimensional images use n×m = 256 x 256 pixels. However, no implementation of smart network technologies has been applied. Moving Picture Experts Community (MPEG)-based AES video encryption algorithm is proposed to be updated in ShiftRows transformation. Any additional operation or hardware is not needed other than the original AES (Singh, 2013). In Kumar and Rana (2016), a high-definition encryption technique of image using AES algorithms is proposed. The well-known AES that brings a much stable block cypher algorithm was implemented, however, the drawback of this technique was the longer processing time, and the number of rounds is decreased by attacks on the encryption algorithm. The Cloud (Zhang and Ding, 2015) has also implemented hybrid RSA and AES-based encryption algorithms to protect user data. Three encryption keys—a public encryption key, a private encryption key, and a secret decryption key—are available when using the RSA and AES data encryption.

The Polybius square matrix is used in the current study's AES data security method to enhance the number of iterations and provide additional protection (Singh, 2013). Another work developed a key using chaotic maps where encryption is performed using AES (Albahar et al., 2018). To improve encryption speed, researchers have synchronised the key expansion unit where a round key is created in each clock cycle where the keys are stored and retrieved from the RAM key in the same clock cycle. In addition, (Deshmukh and Kolhe, 2014) researchers have introduced a digital image encryption technique based on an

AES encryption algorithm, concluding that their proposed technique is capable of dealing with the impact of encryption and decryption.

The 512-bit size of an improved AES algorithm is used to enable better levels of security and throughput supplied by applications (Xhafa et al., 2019). The key length is extended to 512-bit to improve the AES algorithm's strength, and the encryption efficiency can be improved by increasing the number of encryptions rounds for more secure communication. It has also been suggested to combine AES encryption with compression-based 64-encoder encryption approaches to create a trustworthy encryption system that performs data encryption, hence cutting down on encryption time and increasing output (Wadi and Zainal, 2014). First Base 64 encoder encodes the text and converts it to string values; it is also possible to convert the entire data stream to string values before encrypting the data using the AES algorithm; finally, the cypher-text is generated, the file size is further reduced after encoding and the processing time is decreased by encryption, which further reduces the processing time.

Similar to this, new techniques to address security challenges by combining AES and Steganography give users of the upgraded dual-key AES algorithm with Steganalysis confidence (Kumar and Rana, 2016). Later, MAC-level Message Authentication and Encryption is implemented based on the AES forward cypher-text feature using 128-bit key and block-chain cypher for power saving (Kumar and Rana, 2016). A mixture of cryptography and image steganography was proposed in another study. The proposed algorithm is derived from AES and Least Significant Bit (LSB) for cryptography and steganography to adjust data protection. According to the investigation, LSB is a trustworthy method for including critical information in the media carriers (Al-Wattar et al., 2015).

High efficiency (DBUS) for AES encrypting data generated by platforms and systems embedded in chips is implemented using DBUS, the technique pre-selects data sequences for AES encrypting and decrypting, thus minimising buffering and overhead rescheduling. The FPGA results show that the DBUS-based architecture minimises dynamic energy down to 66.93 percent and maximises performance up to 1.30 times higher than the Advanced eXtensible Interface (AXI)-based implementation (Shehab et al., 2014). A further authentication of the elliptical cryptography-based shared protocol for AES-based RFID detections is introduced (Shehab et al., 2014). In contrast to existing authentication protocols, the new protocol was able to encrypt the data pattern that holds the tag, and the functional form of the protocol was encoded and implemented using the RFID tag. A new updated method for the DNA system of the AES algorithm is proposed with the same objective, in which the encrypt and the keys are combined and communicated over a nutrient route (Shehab et al., 2014).

Table 1: Advantages and Disadvantages of AES (Sabry, et al., 2015)

Advantages:	Disadvantages:
1. Hardware and software implementation. 2. Highly reliable security protocols. 3. Uses higher length key sizes. 4. Used for several applications. 5. Commercial and open source solution. 6. Privacy is considered. 7. To break N bit keys, N^{128} attempts are required.	1. Its algebraic structure is simple. 2. Encryption procedure is common for all blocks. 3. Hardware implementation is complex. 4. Security and performance are primary concerns.

Using dynamic keys and S-box generation, the EAES improved AES algorithm for protected fiber-optic connection protects transmission of data by making AES more difficult and complex things and diffused in cipher-text. Simulated feedback from the proposed EAES method is assessed for throughput and conversion time (Hoang et al., 2016). Another scheme to minimise the usage of bandwidth in complex networks, such as PANs and SOHOs, is implemented using AES as an encryption algorithm. By reducing the potential alternatives for AES variants to 2, this method lowers the time for encryption while maintaining security (Ibrahim and Dalkılıç, 2017).

In Moschos et al. (2018), the first study introduced a detailed analysis of the architecture and a thorough examination of the hardware components used in different types of S-box devices. These devices will be classified into different categories based on their architectures and design, in addition to the Linear Feedback Shift Register (LFSR) based S-Box in the AES cypher, which is used in the implementation benchmarking study. Then, a specific S-box unit is selected from each group and used in complete AES encryption, which has been introduced through the FPGA platform. The AES hardware cypher is tested from a hardware size and speed output perspective with different S-box designs.

The improved AES encryption algorithm is combined with the JEX encoding-decoding technique for the image datagram, although smart grid applications have not been used with this kind of encryption (Moschos et al., 2018). Similarly, the study of DNA algorithms along with artificial intelligence to improve the process of key generation has introduced the idea of deep learning in DNA cryptography to hide cypher text using deep learning and DNA cryptography techniques. They also proposed a method for generating keys using natural selection (Kalsi et al., 2018). In general, Table 2.2 summarises the attempts to develop the AES encryption algorithm using DNA techniques.

Table 2: AES Enhancement attempts

Ref#	Issues	Existing Methods	Weakness	Proposed Technique	Advantages	Limitations
(Shehab, 2014)	• Block ciphers. • Poor encryption Effect	• An enhanced AES based algorithm with key generator is used to enhance performance. • Modifying the AES algorithm to be used for images ciphering especially the HD.	simulation results ensure that the modification AES performed faster considering security requirements satisfaction.	DNA computing and round-reduced AES block cipher integration.	• high security level.	Not applied to network smart applications.
[20]	• Cryptography. • Encryption. • Decryption.	• Data Encryption Standard (DES). • Triple DES(T-DES). • Advanced Encryption Standard (AES).	• DES, T-DES are breakable. • AES is a reliable. • AES requires 128-bit input. • AES requires variable length of key size.	• New approach of AES algorithm. • Both DNA cipher and key are merged and transmitted along a channel in protein form.	• Dynamic key generation. • Key values manipulation. • Improved security levels.	• Cipher and key overhead. • Protein bases are added to cipher and nth round key. • high computational cost.
[25]	• Cryptography algorithms	==	==	• Deep Learning encryption. • Key Generation using	• Hiding data in as DNA sequence and deep	• Computation basis is storage capacity required

	strength.			Genetic Algorithm with NW algorithm.	learning.	for DNA.
[26]	• Cryptography perception. • Bridge existing and new technology.	• RSA. • DES. • NTRU.	• long legacy of Traditional systems. • strong mathematical and theoretical basis.	• DNA bases- bit based design and implementation of AES. • DNA specifications consideration.	• It is possible to build a complex DNA basis system. • Suits biological environment • applicable for DNA machines.	• As strong and robust as the standard algorithm.
[27]	• Efficient parallel Computation operations	==	==	• DNA-based DNAES sequences with silent mutations	• Applicable to any type of data. • Applicable for biological environment. • DNA sequence hidden using cipher.	• Same security level as AES
[28]	• Key-dependent Mix Columns. • Quality of a cryptographic algorithm	==	• Cryptography is still behind proficient security approaches	• Altering the AES Mix Columns transformation. • DNA inspired methods from processes and structure.	• Analysis of security new MixColumns. • block cipher values tested using NIST Test Suite.	• Same key length of AES

[7]	• Video encryption algorithm	• DES. • IDEA. • AES.	• Unsecure and weak multimedia encryption schemes.	• Modified AES algorithm. • Reduced algorithm calculations. • Improving encryption performance.	• Adjustment of Shift Row Transformation. • No additional operations or hardware needed. • Stronger video data security against statistical threats.	• Same key length of AES
[29]	• IoT security and privacy.	• (ECC). • GEO encryption. • T-DES	• Privacy and security problems	• Hybrid confidentiality algorithm.	• Strong IoT data confidentiality.	• Same key length of AES
[30]	• secure communication	• AES	• attempts required to break AES are 232 instead of 2256. • Any user activity introduces a weakness.	• Introducing MAES for wired and wireless networks security.	• MAES protected the network from attacks more than AES.	• Same key length of AES
[31]	• Variable social requirements parameters. • Mobile devices need high-speed. • Fast response	• AES	• High speed designs. • latency of lookup tables is a drawback	• CFA-based optimization. • Area reducing for FPGA or VLSI designs in advanced communication services.	• Data is masked to avoid attacks.	• Increased Mask correction cost.

	applications					
[32]	• DNA cryptography.	• IDEA	• strong but not popular as DES and AES. • Patented and it does not have good track record.	• Integrating DNA Computing in IDEA	• Additional DNA cipher over the basic IDEA algorithm. • DNA sequence- like Cipher. • Hidden underlying IDEA algorithm. • Secure and efficient confidential data transmission.	• extended Key space. • Increased computational costs.

1.1 Comparison of Cryptographic Algorithms

The following table summarizes and compares the main features of the previous algorithms (key size, block size, round, structure).

Table 3: Comparison of Various of Cryptography Algorithms.

Ref.	Algo.	Key Size	Block Size	Round no.	Structure	Features
(Poulakis & Rolland, 2015)	DES	64 bits	64 bits	16	Feistel	Not Strong
(Joux, 2004)	DH	Variable	-	-	Public key	Good Security and Slow
(Abood & Guirguis, 2018)	E-DES	1024 bits	128 bits	16	Feistel	Good Security and Fast
(Abood & Guirguis, 2018)	RSA	1024 to 4096	128 bits	1	Public Key	Good Security and Slow
(Abood & Guirguis, 2018)	T-DES	112 or 168	64 bits	48	Feistel	Adequate Security and Fast
(Setiadi, et al., 2015)	ECC	Variable	variable	1	Public Key	Good Security and Fast
(Hardi, et al., 2018)	EEE	1024 bits	-	-	Public Key	Adequate Security and Fast
(Abood & Guirguis, 2018)	RC4	Variable	40-2048	256	Feistel	Fast
(Abood & Guirguis, 2018)	RC2	8,128,64 bits	64 bits	16	Feistel	Good Security and Fast
(Dixit, et al., 2018)	B. FISH	32,448 bits	64 bits	16	Feistel	Fast Cipher in SSL
(Abood & Guirguis, 2018)	DSA	Variable	-	-	Public Key	Good Security and Fast
(Abood & Guirguis, 2018)	RC6	128-256 bits	128 bits	20	Feistel	Good Security
(Abood & Guirguis, 2018)	AES	128,192,256-bits	128 bits	10,12,14	Substitution Permutation	Excellent Security. Best Encryption performance

2 Deoxyribonucleic Acid (DNA)

DNA is known to be the magic code of creation. The type is known as a double-stranded helix of nucleotides, which is responsible for deciding the genetic details of the cells that are then used to build proteins, which is considered to be the secret of our lives (Shimada et al., 2018).

Every human being contains around 100,000 different proteins. Their properties and their relations with each other decide the way we are. The knowledge that determines the key structure of each protein is encrypted in the DNA that encodes the genetic features used in the creation of all known living organisms. DNA is genetic material in humans and other species and can be considered a significant building block of our bodies (Zhang et al., 2019). The protein in its main structure is a linear sequence

of 20 distinct amino acids. DNA is a double-stranded sequence of 4 nucleotides and a portion of the DNA sequence encodes information that specifies the sequence of protein amino acids encoded by that particular gene (Enayatifar et al., 2019).

2.1 DNA Structure and Central Dogma

Genetic information is DNA, the enzyme that governs organism development and function. DNA is in the nucleus of body-forming cells. Moreover, DNA is initially one of the body's main building blocks (Shakhovska et al., 2020). It is an important inherited material present in all living creature cells, providing a blueprint for cell activity, growth, replication, and death. Figure 2.16 explains Waston and Crick's first added DNA structure (Su et al., 2017).

But it doesn't tell us anything about the molecule's sequence. According to Watson and Crick, genetic code variation may be accounted for by the molecule's variability. In addition, their model demonstrates how to make new DNA. They claimed that the molecule "unzips" and two new molecules were created by adding additional matching bases. Semiconservative replication got its name from the fact that each new molecule has both a "old" and a "new" strand of DNA in it. Because the two DNA strands are travelling in the polar opposite directions, they are called "antiparallel." An estimated one million long polymer strands containing these four nucleotides would produce billions of variants in a single double-helix DNA.

First, RNA codes for protein production. Adenine (adenosine) on the DNA couples with uracil (uracil) on the RNA, which is the "language" of nitrogen bases. As a point of reference, the mRNA chain is transcribed using the genome's one strand double helix as a template. After that, the RNA code is converted to protein code, which is a whole different script.

Ribosomes and mRNA and tRNA are among the RNA types found therein. The gene's mRNA and tRNA are both transcribed from the DNA, but the tRNA is specific to an amino acid group (Dong et al., 2009). Translating the message into the right protein or amino acid chain is done by these ribosomes, which function as translators. Each amino acid is made up of three RNA bases. Codons are three-nucleotide sequences in mRNA that organise amino acids into the proper sequence for protein production. In order to assemble proteins, the ribosome uses mRNA and tRNA (Shakhovska et al., 2020).

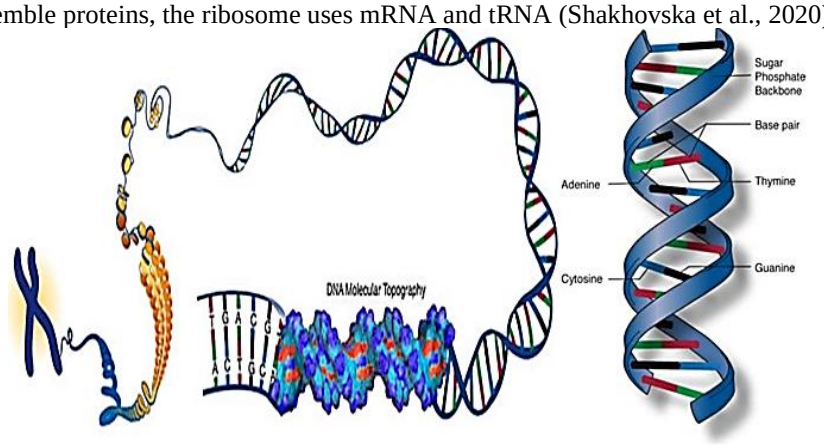

Figure 3: DNA Structure. (Sen, et al., 2018)

Each of the five sugar groups (deoxyribose and phosphate groups) in DNA has four nitrogen bases: adenine (A), cytosine (C), guanine (G) or thymine(T). The nucleotides that make up such polymers are called after the nitrogen base they are named after. The DNA structure reveals two twisted strands. There are linkages between the bases that connect these strands, as seen in the left picture (Shakhovska et al., 2020) and the DNA molecule that has been unravelled to create a 3-D structure (Shakhovska et al., 2020; Zhu et al., 2021).

2.2 DNA Computing

It is the concept of using biological neurons and molecules for complex computation rather than digital computing that has recently been explored by American scientist Leonard Adelman, who has made significant contributions to demonstrating how biological molecules can be applied and studied to solve complex mathematical computing problems.

The DNA computer is nothing more than a collection of DNA strands that are brought together to solve a specific computational problem; technology has made it possible to select the correct strands and manipulate the solution; this is how large and complex computational problems can be solved more quickly than with a conventional computer, which requires different processing and memory capacities; the use of DNA t has the potential to revolutionise the way we think about computing.

1. It can store far more information than traditional computers, which require 1,000,000,000 cubic nanometers of space to store storage media, such as videotapes, in order to function properly.

2. Because each action on the DNA test tube is carried out in parallel on all of the strands in the tube, DNA may perform parallel operations on trillions of strands at the same time.

Due to the linear operation of conventional computers, data can be manipulated one block at a time. For example, chemical reactions in biological environments occur in parallel, and each stage of these reactions affects a large number of strands within the DNA sequence. The use of the DNA computer for these calculations is very advantageous because it requires fewer ene than conventional computers. It is not just biologists who work in the subject of DNA computing; it also includes scientists from a wide range of other fields such as computer science, physics, chemistry, mathematics, and so on. The following are the most significant advantages of DNA computing: (Sabry et al., 2015).

1. The ability to handle millions of commands at the same time.
2. Come up with a large number of potential answers.
3. Using a vast variety of different search techniques.
4. Has the ability to manage extremely large memory sizes.
5. Bit encoding is accomplished by the use of specific memory regions.
6. The employment of a template strand and its storage complement increases the storage capacity by a factor of two.

The following are the most important DNA information for disadvantages (Sabry et el., 2015);

1. For basic and modest computations, a high number of memory locations are required to store all of the solutions that have been created.
2. Each correct response is created along with numerous erroneous ones, which in turn generate multiple incorrect pathways, allowing for the lowest possible error rates while maintaining the highest possible total throughput.

DNA Digital Coding Polymers' Chain Reaction PCR	The DNA strands are amplified using polymerize chain reaction.
DNA Based Bimolecular Cryptographic Design	This technique uses the method of one-time pad OTP and dynamic code book.
Symmetric Key Crypto System Using DNA	encryption and decryption are performed using a single DNA strand. encryption and decryption processes are performed using fabrication and hybridization respectively.
Asymmetric Key Crypto System Using DNA	This technique uses a Dual DNA strand key, one for encryption and another for decryption process.
Pseudo DNA Cryptography Method	this method uses mRNA to construct the cipher text based on the table of genetic code.
DNA Chip Based Technologies	The series of blots contained in genomic sequence of molecular array are used to bind nucleotide which electronically calculates data according to the binding probe in the blot.
Chaotic coding	It uses the features of chaotic systems like pseudo-randomness and deterministic and it depends on the initial condition.

Table 4:Comparison between Various DNA Cryptography Techniques.

2.3 DNA Cryptography

The theory of DNA cryptography is derived from biological fundamentals, the functions performed in DNA cryptography cannot be performed using conventional computers, this is because DNA chains have a very large scale of parallelism and that their processing capacity could exceed 1 billion instructions per second; another explanation is that DNA molecules can hold a very large amount of parallelism. Table 2.15 provides a comparison of the various DNA cryptography techniques (Tornea, 2013).

Data and knowledge are extremely valuable resource that has influenced this century, especially in the case of large companies. That is why the protection of information or data has become very critical to ensure optimum standards of security, privacy and confidentiality against threats and intruders, software has been developed to crack DES, AES and other modern security algorithms. While cryptographic techniques ensure the security of the systems, the attacker develops new methods for cracking or hacking the system. Therefore, to ensure that the information reaches the intended sender and recipient, it is important to resolve all the vulnerabilities of the security systems. A protection framework can have several weak points, such as the location where the cyphers are stored. DNA cryptography solves these problems and offers hope to create unbreakable algorithms. Data is stored either within the DNA (hide messages in DNA microdots) or using DNA sequences to generate encrypted text that can only be decrypted if the key or the correct sequence (of the DNA databases) is identified. DNA Cryptography is a rapidly emerging technology. Adelman demonstrated its usage in complicated issues like directed Hamilton path and NP-complete

problems (for example Travelling Salesman problem). Thus, users can create more complicated Crypto algorithms. It offers new hope for breaking impenetrable codes. DNA computing promises faster processing, less storage, and less power. Whereas standard storage media takes 1012 nm3/bit, DNA retains memory at 1 bit/nm3. While DNA computing is occurring, no electricity is required. One gram of DNA has 1021 DNA bases or 108 TB of data. Thus, can store all data in a few milligrams.

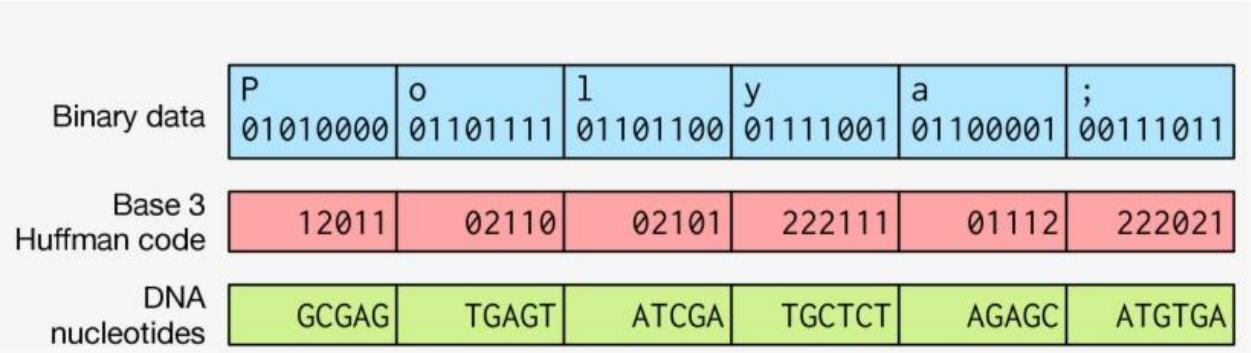

Figure 4: DNA conversion process

2.4 Binary coding scheme

Binary coding scheme is a scheme which converts the DNA sequence to produce its equivalent binary sequence code. In this scheme, 00, 11, 01, and 10 are used for the DNA bases A, T, C, and G respectively (Cardelli, 2013). For example, 0000110110100011 is equivalent to "AATCGGAT" sequence of DNA. Figure 4 represents the general process of conversion binary coding to DNA sequence.

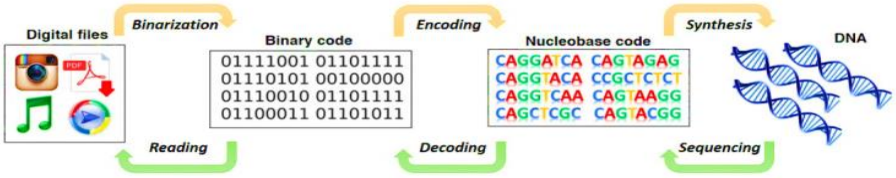

Figure 5: the process of binary coding to DNA conversion.

2.5 Comparison of DNA And Conventional Electronic Computers

There are enormous variations between DNA-based computers and traditional or conventional computers in terms of instruction execution and operating procedures,

Table 5: indicates a contrast between DNA-based computers and conventional electronic computers.

Table 5: Comparison between DNA-based and conventional computers (Cardelli, 2013)

DNA-based Computers	Microchip-based Computers
Slow at single operations	Performs faster when it performs single operations.
Performs billions of instructions simultaneously.	Can do substantially fewer operations simultaneously
Larger storage capacity	Less storage capacity
Require considerable preparations to set up.	Immediate set up

Table 5: Comparison between DNA-based and conventional computers (Cardelli, 2013)

3 Related Works in Telemedicine Systems Focusing on Data Security

Internet of Things (IoT) has recently been adopted as a backbone technology for many areas of technology, such as healthcare and telemedicine applications, the large adoption of this technology necessitated the development and empowerment of technology to become a reliable solution for these applications and others, this study was conducted to investigate security capabilities. In addition, telemedicine systems are typically based on stand-alone systems and thus need more study and development in the implementation of integrated systems and solutions (Chandrasiri et al., 2019).

3.1 Features of IoT devices for telemedicine

The software and the hardware are the two most important parts of any system. The algorithm and the platform that it runs on are both referred to as "software" in this comparison. The IoT devices indicated in these studies were the focus of this comparison, which analysed encryption methods based on their level of protection. The Internet of Things (IoT) connects smart equipment to applications that monitor the health of humans. Patients' lives are made a bit better by some technologies and wearables. This includes wearables such as fitness bands and stethoscopes as well as linked football helmets and hearing aids, among other things. Smart apparel and smart pharmaceutical bottles are also on the rise. The ability for physicians to guarantee patient compliance is one of the most valuable features of IoT in linked devices. Connected medical devices allow doctors to keep tabs on their patients' compliance with dose regimens while prescribing medications. On the basis of significant parameters, these instruments are compared in Table 6.

Reference	Algorithm	IoT Devices	Encryption enabled?	Communication mechanism	Mobile access allowed?	Protocols	Software	Platforms
Albalawi and Joshi, 2018	• CP- ABE. • AES.	• IOT sensor. • IOT adapter. • Contextual sensor.	Yes.	Radio frequency/bi communications	Yes	TCP/IP	IOT hub	• Big data platform
Alelyani and Ibrahim, 2018	• M.L algorithms. • D.L algorithms.	IOT sensors, HIS, self-quantification	No	-	Yes	-	-	-
Bharath and Rajalakshmi, 2018	• DDC algorithm • UVV algorithm	-	No	• WebRTC • peer-to-peer communication	Yes	• Session initiation protocol/jingle	-	-
Fook et al., 2018	• Variance based algorithm.	• IOT sensor • FBG sensors • Polysomnography devices • IoT thermometer • BCG sensor mat	No	-	Yes	• Internet protocol(IP)	• Service API	• Tomcat platform

Kuusik et al., 2018	• DV algorithm	• Motion sensor. • IoT sensors • Wireless sensors.	No	-	Yes	• Internet protocol (IP)	-	• PIP platform
Aldeer et al., 2018	• PillSense operation algorithm	• Motion sensors • Weight sensors • Magnetic switch sensor • Accelerometer	No	-	Yes	-	-	-
Hussein et al., 2018	• Pan-Tompkins • QRS algorithm	• IOT sensor	Yes	• Two-way wireless comm.	Yes	-	-	• Cloud computing • BSN data stream.
Elhoseny et al., 2018	• AES • RSA	• IP camera	Yes		Yes	• Communication protocol	MATLAB R2015a	-
Zagan et al., 2018	-	• Temperature sensor	No	Modbus Poll	Yes	• GSM/GPRS/3G • TCP IP	• Microcontroller software	• MCBSTM32 Kit • Keil platform • hSensor platform
Aloi et al., 2018	• Stress detection algorithm	• Body sensors Communication	No	• Multi-radio Client- server	-	• IoT device mgmt. protocol	• CoAP. • MQTT.	• Azure. • Raspberry Pi3.

		engine		comm. • BE-GTW interface mgmt.		• Application protocol	• LwM2M	• Edge platform
Saha et al., 2018	-	• Heartbeat sensor • Blood pressure sensor • Respiration sensor • Temperature sensor • Accelerometer sensor	No	-	Yes	-	• Putty software	• Raspberry Pi
Mohanty et al., 2018	• Compression algorithm. • (SAOT)	• BPG CMOS. • Digital signal. • CPU. • SDC. • JavaScript decoder. • BPG viewer.	Yes	-	Yes	-	-	-
Kotronis et al., 2018	-	• IOT medical sensors	No	• BLE. • ZigBee	-	• IPsec	-	• Healthcare • Network internet

Aloi et al., 2018	-	• Multi-radio comm. • Mall range comm. • ZigBee. • ZWAVE, • Wi-Fi. • Bluetooth. • ANT+. • Z-wave. • LTE/5G	Yes	• API. • CoAP, • MQTT, • LwM2M	Yes	• Public/ private cloud platforms. • Raspberry Pi3. • Zotac • CI540 NANO Pc Edge. • Azure cloud	-	• BodyEdge. • BE-GTW

Table 6: Comparison of Features Available in IoT Devices in Telemedicine.

4 Previous Studies and Techniques Related to Data Encryption and DNA Computing

The rapidly growing applications of telemedicine and healthcare recently imposed the need for securing the transmission of medical data and records when transmitted over the internet or any other transmission medium, this need motivated the researchers to focus on the enhancements and modifications of existing encryption algorithms as well as developing new algorithms for this purpose, as illustrated in section 5, the DNA has inspired the security encryption algorithm development due to the advanced and reliable method of encryption it is based on , thus, a number of attempts has been made to enhance the standard security and encryption algorithms inspired by the DNA method of encryption, the following table summarizes those attempts and outlines their pros and cons from perspective of the techniques they are using.

Table 7: AES enhancing attempts using DNA Encryption.

Ref#	Issues	Existing Methods	Weakness	Proposed Technique	Advantages	Limitations
Shehab, et al., 2014	• Block ciphers. • Poor encryption Effect	• Modifying the AES algorithm to be used for images ciphering especially the HD.	Simulation results ensure that the modification AES performed faster considering security requirements satisfaction.	DNA computing and round-reduced AES block cipher integration.	• high security level.	Not applied to network smart applications.
Krishna, et al., 2017	• Cryptography. • Encryption. • Decryption.	• Data Encryption Standard (DES). • Triple DES(T-DES). • Advanced Encryption Standard (AES).	• DES, T-DES are breakable. • AES is a reliable . • AES requires 128-bit input. • AES requires variable length of key size.	• New approach of AES algorithm. • Both DNA cipher and key are merged and transmitted along a channel in protein form.	• Dynamic key generation. • Key values manipulation. • Improved security levels.	• Cipher and key overhead. • Protein bases are added to cipher and nth round key. • high computational cost.
Kalsi, et al., 2018	• Cryptography algorithms strength.	==	==	• Deep Learning encryption. • Key Generation using Genetic Algorithm with NW algorithm.	• Hiding data in as DNA sequence and deep learning.	• Computation basis is storage capacity required for DNA .

Sabry, et al., 2015	• Cryptography perception. • Bridge existing and new technology.	• RSA. • DES. • NTRU.	• long legacy of Traditional systems. • strong mathematical and theoretical basis.	• DNA bases- bit based design and implementation of AES. • DNA specifications consideration.	• It is possible to build a complex DNA basis system. • Suits biological environment • applicable for DNA machines.	• As strong and robust as the standard algorithm.
Bahig & Nassr, 2019	• Efficient parallel Computation operations	==	==	• DNA-based DNAES sequences with silent mutations	• Applicable to any type of data. • Applicable for biological environment. • DNA sequence hidden using cipher .	• Same security level as AES
Al-Wattar, et al. 2015	• Key-dependent MixColumns. • Quality of a cryptographic algorithm	==	• Cryptography is still behind proficient security approaches	• Altering the AES MixColumns transformation. • DNA inspired methods from processes and structure.	• Analysis of security new MixColumns. • block cipher values tested using NIST Test Suite.	• Same key length of AES
Deshmukh & Kolhe, 2014	• Video encryption	• DES. • IDEA.	• Unsecure and weak multimedia encryption schemes.	• Modified AES algorithm. • Reduced algorithm	• Adjustment of ShiftRow	• Same key length of AES

	algorithm	• AES.		calculations. • Improving encryption performance.	Transformation. • No additional operations or hardware needed. • Stronger video data security against statistical threats.	
Chanal, & Kakkasageri, 2019	• IoT security and privacy.	• (ECC). • GEO encryption. • T-DES	• Privacy and security problems	• Hybrid confidentiality algorithm.	• Strong IoT data confidentiality.	• Same key length of AES

5 Conclusion

This paper examines analyses the Internet of Things (IoT) installations in the telemedicine domain in recent research studies. These articles show that data privacy is a primary cause for concern in the field of telemedicine. Having the ability to quickly capture, secure, analyse, and transfer data has emerged as the most essential component contributing to this problem. This is because it makes it simpler for the medical industry to perform more efficiently. On the other hand, one can make use of the algorithms that are already available in order to reduce the risk of data protection and privacy violations. IoT research fields currently involve security and privacy because 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. These applications include things like cloud computing and fog computing devices. Devices for checking DNA sequences that rely on the internet of things also demand a high level of knowledge in the implementation of public-key cryptography. If one has a significant amount of processing power, it is theoretically possible to decipher any key by employing techniques known as brute force. Aside from that, the types of data encryption platforms that are utilised the most frequently include Raspberry Pi3 and Edge platforms, along with enormous data platforms, Tomcat platforms, platforms for pip and hSensor, and platforms for huge data. The AES algorithm is the one that is used the most frequently and should be learned by heart. According to the findings of recent research, AES has recently been improved through the utilisation of hybrid computing approaches that combine AES with DNA. In the next sections, an algorithmic approach to the problem's resolution is presented. The researcher may therefore conclude that a system that combines a communication mechanism and supporting software that permits encryption that ensures data protection while it is being transmitted can produce a more dependable telemedicine framework for an Internet of Things (IoT) system than either of these components taken on their own. In conclusion, it is hoped that this initiative will serve to guide researchers and other relevant authorities toward the growth of the telemedicine sector in this region through the expansion of the capabilities of the Internet of Things.

REFERENCES

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. and Liljeberg, P., 2018. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, *78*, pp.641-658.

Almulhim, M. and Zaman, N., 2018, February. Proposing secure and lightweight authentication scheme for IoT based E-health applications. In *2018 20th International Conference on Advanced Communication Technology (ICACT)* (pp. 481-487)..

Medvediev, I., Illiashenko, O., Uzun, D. and Strielkina, A., 2018, May. IoT solutions for health monitoring: analysis and case study. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 163-168)..

Chacko, A. and Hayajneh, T., 2018. Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, *4*(14).

Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N. and Farouk, A., 2018. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access*, *6*, pp.20596-20608.

Nausheen, F. and Begum, S.H., 2018, January. Healthcare IoT: Benefits, vulnerabilities and solutions. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 517-522).

Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R. and Thota, C., 2018. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems*, *82*, pp.375-387.

Salahuddin, M.A., Al-Fuqaha, A., Guizani, M., Shuaib, K. and Sallabi, F., 2018. Softwarization of internet of things infrastructure for secure and smart healthcare. *arXiv preprint arXiv:1805.11011*.

He, D., Ye, R., Chan, S., Guizani, M. and Xu, Y., 2018. Privacy in the Internet of Things for smart healthcare. *Communications Magazine*, *56*(4), pp.38-44.

Tao, H., Bhuiyan, M.Z.A., Abdalla, A.N., Hassan, M.M., Zain, J.M. and Hayajneh, T., 2018. Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet of Things Journal*, *6*(1), pp.410-420.

Atlam, H., Walters, R. and Wills, G., 2018. Fog computing and the internet of things: a review. *big data and cognitive computing*, *2*(2), p.10.

Kartheek, D.N. and Bhushan, B., 2020. Security issues in fog computing for internet of things. In *Architecture and Security Issues in Fog Computing Applications* (pp. 53-63). IGI Global.

lementing hybrid (Rsa & Aes) encryption algorithm. *In 2014 International Conference on Power, Automation and Communication* (INPAC) (pp. 146-149). IEEE.

Kumar, P. and Rana, S.B., 2016. Development of modified AES algorithm for data security. *Optik-International Journal for Light and Electron Optics*, 127(4), pp.2341-2345.

Shah, S.S.H. and Raja, G., 2015, October. FPGA implementation of chaotic based AES image encryption algorithm. In 2015 *IEEE International Conference on Signal and Image Processing Applications* (ICSIPA) (pp. 574-577).

Zhang, Q. and Ding, Q., 2015, September. Digital image encryption based on advanced encryption standard (aes). In 2015 Fifth International Conference on Instrumentation and Measurement, *Computer, Communication and Control* (IMCCC) (pp. 1218-1221).

Dandekar, A.K., Pradhan, S. and Ghormade, S., 2016. Design of AES-512 algorithm for communication network. IRJET-*International Research Journal of Engineering and Technology*, 3(5).

Aery, M.K., 2016. String Compression Technique with Modified AES Encryption. *International Journal of Advanced Computing and Electronics Technology* (IJACET), 3(1), pp.13-25.

Yogeswari, G. and Eswaran, P., 2016. Enhancing data security for cloud environment based on AES algorithm and steganography technique. *International Journal of Advanced Research Trends in Engineering and Technology*, 3.

Hoang, V.P., Dao, V.L. and Pham, C.K., 2016, September. A compact, ultra-low power AES-CCM IP core for wireless body area networks. *In 2016 IFIP/IEEE International Conference on Very Large Scale Integration* (VLSI-SoC) (pp. 1-4).

Panghal, S., Kumar, S. and Kumar, N., 2016. Enhanced security of data using image steganography and AES encryption technique. *International Journal of Computer Applications*, 42.

Yang, X. and Wen, W., 2017, January. Design of a pre-scheduled data bus for advanced encryption standard encrypted system-on-chips. *In 2017 22nd Asia and South Pacific Design Automation Conference* (ASP-DAC) (pp. 506-511).

Ibrahim, A. and Dalkılıç, G., 2017. An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, *proven on WISP. Journal of Sensors*, 2017.

Krishna, B.M., Khan, H., Madhumati, G.L., Lohitha, B., Bhavitha, E., Sri, P.T. and Kumar, B.A., 2017. FPGA implementation of DNA based aes algorithm for cryptography applications. *International Journal of Pure and Applied Mathematics*, 115(7), pp.525-530.

Alapatt, B.P. and Kavitha, A., 2018. An Enhanced Advanced Encryption Standard (Eaes) Algorithm For Secure Fiber Optic Communication. *International Journal of Advanced Research in Computer Science*, 9(1).

Moschos, A., Papadimitriou, G. and Nicopolitidis, P., 2018. Proactive encryption of personal area networks and small office-home office networks under advanced encryption standard application. *Security and Privacy*, 1(1), p.e10.

Wong, M.M., Wong, D.M., Zhang, C. and Hijazin, I., 2018. Circuit and system design for optimal lightweight AES encryption on FPGA.

Sharma, S.B.T., Kantak, M. and Vernekar, N., 2018. Novel approach to image encryption: using a combination of JEX encoding–decoding with the modified AES algorithm. *In Information and Communication Technology for Sustainable Development* (pp. 201-210). Springer, Singapore.

Kalsi, S., Kaur, H. and Chang, V., 2018. DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation. *Journal of medical systems*, 42(1), p.17.

Sabry, M., Hashem, M., Nazmy, T. and Khalifa, M.E., 2015, December. Design of DNA-based advanced encryption standard (AES). In *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)* (pp. 390-397). IEEE.

Bahig, H.M. and Nassr, D.I., 2019. DNA-Based AES with Silent Mutations. *Arabian Journal for Science and Engineering*, *44*(4), pp.3389-3403.

Al-Wattar, A.H., Mahmod, R., Zukarnain, Z.A. and Udzir, N., 2015. A new DNA based approach of generating key dependent MixColumns transformation. *International Journal of Computer Networks & Communications (IJCNC)*, *7*(2), pp.93-102.

Chanal, P.M. and Kakkasageri, M.S., 2019, July. Hybrid Algorithm for Data Confidentiality in Internet of Things. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5).

Article submitted 1 March 2023.

Accepted at 28 March

Published at 30 Jun 2023.