Securing IoT Data: A Hybrid Cryptographic Approach

Salman Ali
Department of Computer Science
Aligarh Muslim University
Aligarh, India
salmanali.amu@gmail.com

Faisal Anwer
Department of Computer Science
Aligarh Muslim University
Aligarh, India
faisalanwer.cs@amu.ac.in

***Abstract*— The Internet of Things (IoT) refers to a system of interconnected physical objects globally linked to each other through the internet. The IoT envisions connecting trillions of smart devices in our surroundings, generating a substantial volume of data that requires processing, transmission, and storage. Ensuring the security and privacy of data in IoT poses a formidable challenge, and it is regarded as the foremost priority for numerous present and upcoming applications. Devices like WSNs, RFIDs, smartphones, etc., constitute the primary elements of IoT networks, which are essentially resource-constrained devices. The implementation design of privacy and security management schemes for these devices is influenced by several factors such as optimal performance, minimal power usage, resilience against attacks, comprehensive end-to-end security, and protection against data tampering. Security systems for the IoT thwart unauthorized access to data by safeguarding against destruction or modifications. In this study, we proposed a confidentiality algorithm that combines DNA cryptography, Genetic Algorithm (GA), and Elliptic Curve Cryptography (ECC) to form a hybrid approach. The hybrid algorithm ensures robust data confidentiality during the transmission of information for IoT. Our proposed algorithm performs better regarding key generation, encryption, and decryption time with respect to the various file sizes.**

Keywords*— *IoT, Data confidentiality, Elliptic Curve Cryptography (ECC), Deoxyribonucleic acid (DNA), Genetic Algorithms (GA)

I. Introduction

The IoT is a worldwide network structure that connects virtual and physical objects by employing data capture and communication functionalities. This infrastructure incorporates both the current internet and other network components. IoT devices are distinguished by their significant autonomy in capturing data, transferring events, establishing network connections, and ensuring interoperability for the execution of independent collaborative applications and services. Within the IoT framework, there are billions of individuals, distinct devices, and services, all interconnected to share valuable and sensitive data [1].

The rapid surge in network and internet-driven applications has led to a substantial surge in data generation, accompanied by the identification of numerous security and privacy concerns. Within such a network, every component introduces vulnerabilities in terms of security and privacy. Exploiting these weaknesses, hackers take advantage, and from a statistical standpoint, in an environment encompassing billions of devices, these vulnerabilities and weaknesses may be maliciously exploited [2]. However, the absence of robust security measures could potentially render the IoT susceptible to attacks and malfunctions, thereby overshadowing its advantages [3]. Security and privacy concerns encompass crucial aspects such as confidentiality, authentication, validation, non-repudiation, and integration. Consequently, it is imperative for all IoT devices to incorporate robust security measures, including advanced capabilities for encrypting and decrypting confidential data. Ensuring the privacy and security of information is a significant challenge, with confidentiality being a key aspect that safeguards data from unauthorized access. Conventional confidentiality algorithms face numerous difficulties in effectively addressing this concern. Addressing the confidentiality concerns in the context of the IoT requires solutions that can handle the scalability, diversity among the essential components, and the limited resources of embedded devices, including energy and computational constraints. This paper suggests a novel approach to tackle these issues by introducing a hybrid confidentiality algorithm that combines DNA cryptography, GA, and ECC.

The remaining sections of this paper are structured as follows. Section II provides information on related works, while Section III outlines the background of the paper. The proposed work is detailed in Section IV, followed by a security analysis in Section V. Section VI delves into the implementation results, and the paper concludes in Section VII.

II. Related Work

In previous years, numerous scholars have suggested different approaches, incorporating the use of ECC, DNA-Cryptography, and GA to enhance the security of IoT. This section examines several of these methodologies over the last four years.

Devi et al. [4] proposed a method for improving the security of IoT devices by implementing an advanced Elliptic Curve Cryptography algorithm and malware detection through the utilization of Deep LSTM. The suggested method is implemented in two stages, including malware prevention and detection among IoT devices. Contextual anomaly detection, malware type prediction, and other phases comprise the three stages of the malware detection process. The IECC is used to transmit data securely as part of the malware prevention process. When identifying a node as normal or under attack, contextual features are considered. Using a Deep LSTM to identify four various forms of attacks, including anomaly, DOS, Probe, and R2L, the nodes that have been targeted are taken into account during the second stage of forecasting malware. While transferring files from each IoT device, they are encrypted for security reasons using an upgraded encryption method to limit malware access. The information of all the devices linked to the WSN is stored on cloud servers using IoT device data that has been encrypted.

Kumar et al. [5] describe a hybrid method by combining nature-inspired optimization algorithms such as the moth search algorithm (MSA) with ECC. The ECC encryption algorithm combines DNA encoding in the proposed encryption and decryption method. The mechanism of DNA-encoded ECC offered multi-level security with fewer processing resources. The experimental findings are assessed by considering factors such as encryption time, decryption time, data transfer rate, and the size of the security key in the model. This evaluation unmistakably demonstrates that the proposed approach offers a dual-layered security solution with minimal key size and reduced storage requirements.

Rostampour et al. [6] introduce an innovative and reliable approach to ensure secure communication between an IoT device and a cloud server, employing the secure authentication protocol based on Elliptic Curve Cryptography (ECCbAP). Initially, they assess four current authentication protocols, examine their resistance to man-in-the-middle and traceability attacks, and demonstrate their vulnerabilities. Next, they suggest a new scheme and test it for security against well-known IoT risks using both informal and formal methodologies. The results indicate that ECCbAP offers stronger security than the other protocols and is more resource-efficient, making it more suitable for constrained environments, such as Bluetooth Low Energy (BLE) or RFID tag sensors.

Arunkumar et al. [7] in their paper proposed a secure framework for IoT by employing Logistic Regression machine learning and leveraging Elliptical Curve Cryptography technology (LRECC) for the purpose of prevention, detection, and mitigation. The Elliptical Curve Cryptography (ECC) technique is utilized in this strategy to produce and disseminate security keys. Since the ECC technique uses a lightweight key, it reduces the overhead associated with routing. Additionally, the transmitter is chosen using the Logistic Regression machine learning technique based on insightful results. With minimal overhead, this method offers continuous, reliable routing paths. Additionally, route nodes work in conjunction with IoT to efficiently manage resources and reduce the 29.95% latency. Additionally, it will be used in WSNs built for the IoT to secure the application environment, such as in smart cities.

Yang et al. [8] proposed a study that looked into ways to ensure that confidential data related to data transmission in an industrial environment is encrypted, packed, and comes from legitimate devices. This research proposes an authentication approach for establishing trust between IoT terminal devices and backend servers. The method utilizes trusted tokens, ECC, and packet encryption through the TLS protocol. It is imperative to implement the recommended authentication mechanism prior to facilitating communication between backend servers and terminal IoT devices. The problem of attackers posing as terminal IoT devices and sending inaccurate data is addressed by taking this action. The method is designed to stop attackers from randomly tampering with IoT devices and relaying anomalous information that could result in data mistakes. Because tokens offer strong security, they can prohibit the disclosure of associated privacy information in IoT devices with relatively limited computational resources.

Di Matteo et al. [9] discuss the prevalent utilization of ECC within the realm of the IoT for ensuring security measures such as key exchange and digital signatures. However, to cater to the real-time demands of IoT applications, it becomes imperative to incorporate hardware acceleration for ECC-based algorithms, aligning with the prerequisites of minimal latency and power consumption. This scholarly article presents a swift and adaptable hardware accelerator meticulously crafted for NIST P-256/-521 elliptic curves, specifically conceived within the framework of the European Processor Initiative.

Qaid et al. [10] introduced a novel and lightweight encryption approach rooted in DNA sequences to better cater to IoT devices, ensuring both ease of use and robust communication security. Leveraging the inherent randomness of DNA sequences, a robust secret key has been generated to thwart potential attackers effectively. The proposed method exhibits notable advantages in terms of both efficiency and strength. Empirical tests and security evaluations affirm that this encryption system excels in encryption efficacy and resistance to known attacks and performs swiftly enough for practical IoT applications. The DNA-based key is applied for file encryption using straightforward and dependable techniques.

Surendiran et al. [11] introduce a novel approach to enhancing data security in fog computing through the combination of DNA-based Elliptic Curve Cryptography (ECC) and the RedFox Optimization algorithm for clustering (RF-DECC). The initial step involves using the RedFox Optimization algorithm to determine cluster heads. Once the clustering process is finished, the chosen cluster head takes on the responsibility of data encryption. This encryption utilizes DNA-Elliptic Curve Cryptography. By integrating DNA into ECC, the encryption process becomes more intricate due to the incorporation of DNA encoding. The RF-DECC method displays notable enhancements, gaining a 24% improvement in security.

Al-Husainy et al. [12] developed and implemented a versatile and efficient encryption system that employs straightforward substitution and rearrangement techniques for data encryption and decryption. This system is specifically designed to accommodate the limited processing capabilities found in IoT devices. Moreover, to attain a robust security level within the suggested system, we harnessed the DNA sequence to create three fundamental cryptographic keys. These keys are derived by pinpointing specific indices designated by the user along the DNA sequence. The experimental outcomes of our lightweight encryption system demonstrate its promising potential for deployment on any IoT device, irrespective of memory constraints, and exhibit favorable encryption speeds when compared to established cryptographic systems.

Al-Shargabi et al. [13] introduced a novel, efficient encryption algorithm rooted in DNA sequences tailored to suit the limited resources of IoT devices. This algorithm capitalizes on the inherent randomness of DNA sequences to create a highly secure secret key that poses a formidable challenge for potential attackers. This DNA-based key is employed for image encryption through two uncomplicated yet robust substitution and transposition operations, aligning perfectly with the computational constraints of IoT devices while ensuring the security of transmitted images.

Jain et al. [14] introduce a novel approach for implementing an Intrusion Detection System (IDS) in IoT applications. This approach leverages a genetic algorithm specifically designed for the task. The genetic algorithm's initial population and fitness calculations will be based on the KDD'99 cup dataset, originally introduced and generated by MIT Lincoln Labs.

Lin et al. [15] introduced a two-tier authentication protocol reliant on devices to counteract primary user emulation attacks (PUEA) in the context of IoT applications. Their approach incorporated a spectrum management technique to mitigate common security threats. To enhance the protocol's reliability, they suggested expanding its application to mobile objects based on the detection performance. In a separate study, Tiwari and Kim employed DNA and ECC to establish dual-layered security measures for cloud-based and mobile applications.

A significant obstacle in IoT applications involves the management of extensive data, requiring robust security measures for tracking, sensing, and capturing information. Ensuring the security and privacy of IoT data emerges as a crucial concern. Consequently, this paper focuses on tackling the issue of data confidentiality in IoT by employing a hybrid confidentiality algorithm.

III. Background

This segment provides a concise overview of the fundamental principles and primary procedures of genetic algorithms, DNA Cryptography, and Elliptic Curve cryptography. A comprehensive understanding of every algorithm is crucial for obtaining a complete perspective on the proposed solution.

A. Genetic Algorithm

A potent optimization method known as Genetic Algorithm (GA) utilizes a population-based approach to perform various operations such as selection, crossover, and mutation. These operations are employed to approximate a solution for optimization problems. Before applying the genetic algorithm's operators, an initial population of chromosomes (individuals) is randomly generated within the search space. Everyone in the population represents a potential solution to the problem within the search area. The fitness of each chromosome is assessed using a fitness function. Each chromosome comprises multiple genes, with each gene symbolizing a specific part of the solution. Afterward, the three operators are employed on the population to generate a fresh population (solutions). These operators are iteratively applied until a specified termination condition is satisfied [15]. The procedures for executing the tasks of the GA are outlined as follows:

- *Selection process:* This procedure aims to choose promising and highly-fit chromosomes as potential parents. The specific techniques for selecting these parents vary across different studies, but typically, there exist various approaches for making this selection. Nevertheless, individuals with a more suitable fitness score typically stand a better chance of being chosen as parents. This selection process ensures the continued exploration of potential solutions.

- *Crossover process:* The crossover operation, with a probability denoted as Pc, is utilized on the chosen chromosomes by exchanging specific genes between the parents, resulting in the generation of fresh offspring or new solutions. This operator is influenced by the concept that offspring inherit desirable characteristics from their parents. Crossover can be executed through various techniques such as single-point, two-point, and uniform methods, and it plays a role in influencing the diversity within a Genetic Algorithm (GA).

- *Mutation process:* To enhance the likelihood of generating novel and distinct offspring that differ from their parents, a specific procedure involves selecting certain genes within the chromosome at random and altering their values to other potential values within the search space. Typically, the mutation operation is performed with a lower probability (Pm) than Pc. The primary goal of mutation is to explore the nearby region, ultimately leading to increased genetic diversity.

B. DNA Cryptography-Biological Background

Eukaryotic organisms possess DNA as their genetic material, featuring a double-helix molecular configuration in which two single strands run alongside each other. DNA is often referred to as a polymer and is constructed from numerous small nucleotides. Every nucleotide is composed of three components: (i) nitrogenous bases, (ii) deoxyribose, and (iii) phosphorus.

DNA, short for deoxyribonucleic acid, is the fundamental genetic material for all living organisms. It constitutes a specific type of large biological molecule comprised of nucleotides. Each nucleotide consists of a solitary base, and there are four distinct bases: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G), which correspond to the four varieties of nucleotides found in DNA.

A single-stranded DNA molecule is arranged in a specific way, with two ends known as "5" and "3." In its natural state, DNA typically exists as double-stranded molecules. These two complementary DNA strands join together, creating a double helix structure by bonding hydrogen atoms between matching base pairs, such as A and T or C and G [16]. Fig. 1 shows the schematic diagram of DNA.

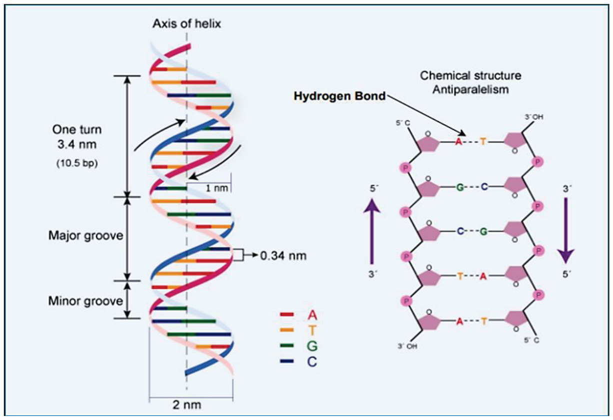

Fig. 1. DNA structure

C. DNA Cryptography Operation

Three commonly employed DNA cryptography techniques are as follows: (i) The Insertion method, (ii) The Substitution Method, and (iii) The Complementary Pair approach.

In each of the previously mentioned methods, a shared process for encoding and decoding is employed. Initially, the plain text is transformed into binary digits, after which these binary digits are further transformed into a corresponding sequence of DNA nucleotides. Subsequently, one of the DNA-based cryptographic techniques is employed for either encrypting or decrypting the data. In each of the previously mentioned methods, a shared process for encoding and decoding is employed. Initially, the plain text is transformed into binary digits, after which these binary digits are further transformed into a corresponding sequence of DNA nucleotides. Subsequently, one of the DNA-based cryptographic techniques is employed for either encrypting or decrypting the data. The binary code representation of DNA's four essential elements is as follows: Adenine (A) is denoted as 00, Thymine (T) as 01, Guanine (G) as 10, and Cytosine (C) as 11.

Take a DNA sequence that's accessible to the public and follow the previously explained method to transform it into binary code. Then, break this binary DNA sequence into smaller segments, each containing a variable number of bits greater than 2. Next, place each individual bit from the binary plaintext at the start of one of these segmented binary DNA sequences. Combine these inserted sequences to create an encoded binary sequence. Now, convert this encoded binary sequence back into nucleotides to generate a novel artificial (not naturally occurring, but derived through this process) binary sequence.

D. Elliptic Curve Cryptography

In 1985, Neal Koblitz and Victor Miller introduced the initial concept of Elliptic Curve Cryptography (ECC). The following mathematical expression characterizes an elliptic curve in the prime field GF(p):

$$y^2 = (x^3 + ax + b)\ mod\ p \tag{1}$$

In a prime field GF(p), the parameters a and b are both integers such that $4a^3 + 27b^2 (mod\ p) \neq 0$. An elliptic curve E defined over the finite field GF(p) is composed of a collection of points represented as P = (x, y), where both x and y belong to GF(p). Additionally, there is an additional point known as "the point at infinity," denoted as O. The group is formed by combining the set of points on an elliptic curve with the point at infinity. Within this group, we can establish the following group operation:

- *Point Addition (PA):* $P(x_A, y_A) + Q(x_B, y_B) = R(x_c, y_c)$

$$x_c = \left(\frac{y_B - y_A}{x_B - x_A}\right)^2 - x_A - x_B \tag{2}$$

$$y_c = \left(\frac{y_B - y_A}{x_B - x_A}\right)(x_A - x_c) - y_A \tag{3}$$

- *Point Doubling (PD):* $2P(x_A, y_A) = R(x_c, y_c)$

$$x_c = \left(\frac{3x_A^2 + a}{2y_A}\right)^2 - 2x_A \tag{4}$$

$$y_c = \left(\frac{3x_A^2 + a}{2y_A}\right)(x_A - x_c) - y_A \tag{5}$$

where $P(x_A, y_A)$ and $Q(x_B, y_B)$ are two points lies on the elliptic curve.

- *Point Multiplication (PM):* The primary operation in any cryptographic system relying on ECC is called Point Multiplication (PM). This operation is denoted as Q = kP and signifies the result of adding the point P to itself k times. Where P is the point on the Elliptic Curve.

$$Q = kP = \underbrace{P + P + P + \cdots + P}_{k\ times} \tag{6}$$

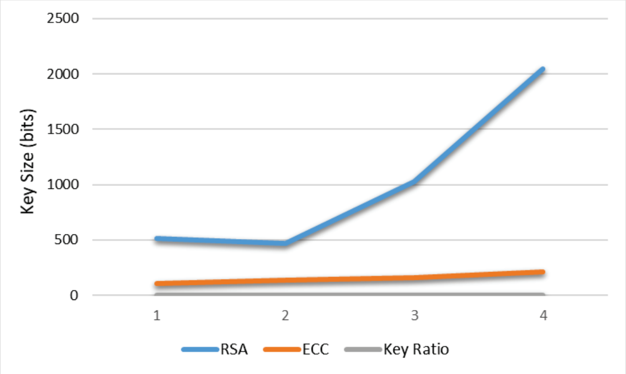

Fig. 2. Comparative Key Size

IoT employs public key and private key cryptography for data security during communication. Elliptic Curve Cryptography (ECC) is one of the well-known asymmetric key cryptographic methods used to enhance the security of IoT with the minimum usage of system resources. The main advantage of ECC is that it provides an equal amount of security with a small key size, as in Fig. 2.

TABLE I. EL-GAMAL ECC SCHEME

Process	Description
Parameter	Elliptic curve parameters over prime field GF(p) are given by the tuple T = (p, a, b, GE, n)
Key generation	Private key k: Select a random number ∈ (1, n) , Public key: $P_B = \mathrm{k}G_E$, where G_E is the global element.
Conversion of the message into a point on the elliptic Curve (PM)	Message as a number M, and R be the integer x-coordinate $x_j = MR + j$, where j=0,1,2,3…. Compute $S_j = x_j^3 + ax_j + b$, such that $S_j^{(p-1)/2}(mod\, p) = 1$ y-coordinate $y_j = \sqrt{S_j}$ The message M will now be depicted as: $P_M = (x_j, y_j)$
Encryption	Sender uses their public key: P_B Select a random number K, such that K∈ (1, n-1) Compute $C_1 = KG_E$ and $C_2 = P_M + K\ P_B$ Ciphertext $C = (C_1, C_2)$
Decryption	The receiver uses their private key k: Compute: $M_1 = kC_1$ Compute: $P_M = C_2 - M_1$ $= P_M + K\ P_B -\ kC_1$ $= P_M + K\ \mathrm{k}G_E -\ kKG_E = P_M$ Hence, the receiver received the same point P_M
Conversion of the point into message (M)	Compute M=floor(x_j/R)

E. Generalized El-Gamal ECC Algorithm

El-Gamal ECC is a fusion of generalized El-Gamal encryption methods and elliptic curve arithmetic. The comprehensive process of encrypting and decrypting is detailed in Table 1 [17]. This cryptographic approach harnesses the computational advantages of elliptic curves, which are algebraic structures defined over finite fields. By integrating El-Gamal encryption with elliptic curve arithmetic, El-Gamal ECC enhances the security and efficiency of cryptographic operations, making it a compelling choice for secure data transmission and communication. The utilization of an elliptic curve in cryptography is renowned for its ability to provide robust security with a relatively smaller key size.

IV. SUGGESTED HYBRID APPROACH FOR ENSURING DATA CONFIDENTIALITY

This section addresses the network architecture under consideration and suggests a confidentiality algorithm.

A. Network Architecture

The three-layer IoT architecture that we are taking into consideration for our suggested work is depicted in Fig. 3. This stratified method establishes the essence of IoT, and it proves suitable for evolving applications within the IoT domain. It consists of three layers: the perception layer, the network layer, and the application layer. The perception layer identifies individual devices and their respective roles within an IoT system. The most exemplary instances of perception layers are cameras, RFID tags, sensors, etc. The sensors sense and collect data regarding each thing within the network. In the realm of IoT, the core component is the network layer, which plays a pivotal role in establishing connections with various intelligent devices, servers, and network components. It also bears the responsibility for transmitting the perception layer data. The application layer guides the user to access converging IoT application services. It facilitates the implementation of IoT in diverse areas, including smart homes, smart cities, smart health, and smart agriculture monitoring, among other applications.

B. Proposed Algorithm for Ensuring Confidentiality

We explored the use of DNA cryptography, GA, and ECC algorithms to ensure the confidentiality of information. Encryption safeguards the plain text from unauthorized access or attacks by converting it into cipher text. If unauthorized individuals can obtain the private key, the cipher text is deemed ineffective. If an attacker consistently decrypts the ciphertext without possessing the private key, the cipher is considered to be partially compromised.

Various cryptographic algorithms have been suggested in the related work. These are inclusively referred to as calculations involving symmetric keys and ECC. It recommends that a key size of 160 bits ECC is sufficient instead of using a 1024-bit key in RSA to achieve an equivalent level of security. The computation combines the most advantageous features of both symmetric and asymmetric encryption techniques.

In the proposed methodology, the initial input message undergoes a unique transformation, commencing with its conversion into a DNA sequence via DNA encoding. This DNA-encoded message is then transmuted into binary format, where the genetic algorithm's crossover and mutation operations are executed sequentially. Subsequently, the binary representation is converted into its decimal counterpart. This resulting decimal value is then mapped onto an Elliptic Curve, effectively transforming it into a point on that curve. This point is further secured through an encryption process using the sender's public key in the framework of ECC. Finally, when received by the intended recipient, the ciphertext undergoes decryption, with the process unfolding in reverse order, employing the recipient's private key to reveal the original message. This innovative approach of three layers of security combines DNA cryptography, GA, and ECC to ensure a robust and secure message transformation and transmission. The outline of the confidentiality algorithm is depicted in Fig. 4.

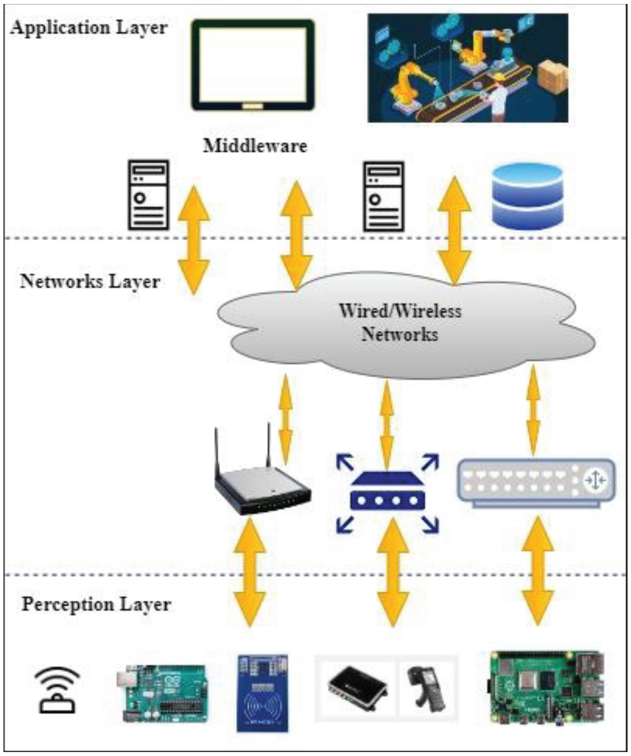

Fig. 3. 3-Layer IoT Architecture

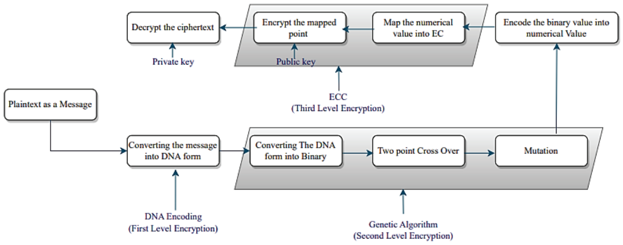

Fig. 4. High-level overview of the proposed method

The proposed algorithm's operational sequence is outlined as follows.:

Step 1: Input the message M as a plaintext.

Step 2: Encode the plaintext message into the DNA form using DNA nucleotides as specified in Table 2.

Step 3: The DNA-based message is transformed into binary code by associating binary values with DNA nucleotides, as outlined in Table 3.

Step 4: Divide the bit string into two equal segments and perform two points crossover on the binary string using a genetic algorithm.

Step 5: Apply genetic algorithm-based mutations to the binary string.

Step 6: Creating subsets consisting of 6-bit segments from the binary string.

Step 7: Each subset is converted into a decimal value.

Step 8: These numeric values are converted into a point on the Elliptic curve, as in Table 1.

Step 9: The sender encrypts this point with ECC using their public key, as depicted in Table 1.

Step 10: The receiver employs ECC decryption with their private key to decrypt the received point, as detailed in Table 1.

Step 11: The point is converted into message M, as outlined in Table 1.

The remaining step for the decryption algorithm is the reverse of an encryption algorithm.

TABLE II. DNA NUCLEOTIDE MAPPED WITH CHARACTERS

Character	DNA Subset	Character	DNA Subset	Character	DNA Subset
A/a	ACA	T/t	GGT	+	AAA
B/b	CCC	U/u	GTA	.	CGA
C/c	CCG	V/v	GTC	:	GGG
D/d	CCT	W/w	GTT	^	AAT
E/e	AAC	X/x	TAA	)	CCA
F/f	CGC	Y/y	TAC	,	ACC
G/g	ACT	Z/z	TAG	!	ACG
H/h	CGT	0	TAT	%	CGG
I/i	CTG	1	TCA	;	AGA
J/j	CTT	2	TCC	-	AGC
K/k	GAA	3	TCG	*	AGG
L/l	GAG	4	TCT	`	ATA
M/m	GAT	5	TGA	@	ATC
N/n	GCA	6	TGC	\	ATG
O/o	GCC	7	TGG	=	ATT
P/p	GCT	8	TGT	(space)	CAA
Q/q	GGA	9	CAC		
R/r	GGC	$	CAG		
S/s	AAG	(	CAT		

TABLE III. DNA NUCLEOTIDE TO BINARY CONVERSION

DNA Nucleotide Base	Binary Equivalent
Adenine (A)	00
Cytosine(C)	01
Guanine(G)	10
Thymine(T)	11

Example: Consider the elliptic curve E is given as:$y^2 = x^3 + 3x$, $k = 30$ and $p = 4177$.

- Consider the plain text "SAGE".
- Convert the message into DNA form according to Table 2: "AAG ACA ACT AAC"
- The DNA-mapped string is converted into binary form according to Table 3: "00 00 10 00 01 00 00 01 11 00 00 01".
- The binary string is divided into two equal parts:

  00 00 10 00 01 00
  00 01 11 00 00 01

- Execute the genetic algorithm's two-point crossover operation at positions 3 and 9.

  00 01 11 00 01 00
  00 00 10 00 00 01

- Conduct a mutation operation by interchanging the binary string within the context of genetic algorithms.

  00 00 10 00 00 01
  00 01 11 00 01 00

- Append both the string:

  000010 000001 000111 000100

- Create subsets from a binary string with 6 bits each, followed by the conversion of these subsets into decimal format.

$$\underbrace{000010}_{2}\,\underbrace{000001}_{1}\,\underbrace{000111}_{7}\,\underbrace{000100}_{4}$$

Therefore, the message is converted to decimal as: m=2174

- The equation of the curve is given as $y^2 = x^3 + 3x$, p=4177, k=30 and m=2174

$x = \{m * k + j\}$,   j=0,1,2…..

$x = \{2174 * 30, 2174 * 30 + 1, 2174 * 30 + 2, \ldots..\}$

At j=15, $x = 2174 * 30 + 15$, $x = 65235$

$x^3 + 3x$=$((65235)^3 + 3 * 65235)$(mod 4177)

=1444

=38^2

Therefore, the message m=2174 is encoded as a point

$(x,\sqrt{x^3 + 3x})$=(65235,38)

To decipher the original message "m," we need to perform a computation on the message point (65235, 38) located on E as: m= floor(65235/30)=2174

V. Security Analysis

The DNA-based elliptical cryptography approach utilizes established elliptical curve parameters and techniques. Previous studies on ECC demonstrated its resistance against timing and simple power analysis attacks [15]-[18]. Following the decryption procedure, ECC produces randomized data without the presence of a valid authentication key. The primary target for attacks on cryptosystems is the authentication key itself. A successful attack can occur when plaintext data is obtained through decryption attempts using a random key [19]. However, the susceptibility of these attacks can be reduced by encoding the pre-encryption data into non-repetitive patterns [20].

The research proposes incorporating DNA encoding before encryption to enhance the security of the current elliptical cryptography mechanism. The fifth section of the paper elaborates on the DNA-based mapping procedure. The method involves mapping each character to a six-bit sequence using DNA encoding. In this approach, message characters are mapped using subsets of DNA sequences with a length of 3. Each element within the DNA mapping subset can take on one of four values (A, C, G, or T). As a result, the total number of possible permutations in a subset with a length of three and four possible values is calculated as 4^3.

While conducting encoding, every nucleotide (A, C, G, & T) is associated with a two-bit binary code, resulting in each value having either 2^2 or 4 potential binary representations.

In the suggested system, the size of the subset is designated as 3. As a result, under this suggested approach, each character of the message could potentially possess possible binary values = $4^3 * 2^2 = 256$.

By employing DNA cryptography, the encryption of a random stream will result in an equally pseudorandom stream upon decryption. Therefore, due to a significant level of unpredictability, incorporating DNA encoding before encryption in the suggested scheme will provide greater resistance against attacks compared to conventional elliptical cryptosystems without DNA mapping.

VI. Implementation Results

We utilized the SageMath tool for our proposed approach and confirmed its effectiveness and uniqueness. In our implementation, we used Python's pycryptodome library and employed the brainpoolP256r1 elliptic curve that is pertinent to our method.

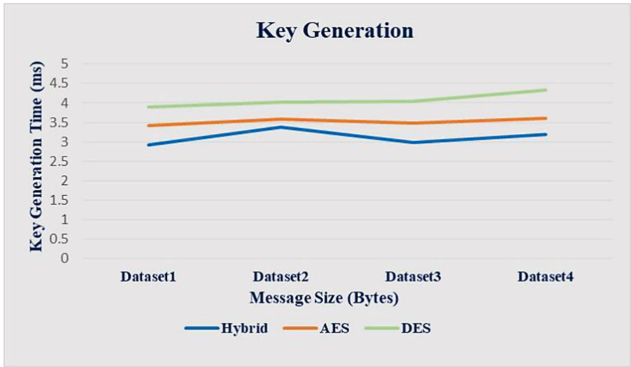

Fig. 5. Key generation time

We utilized four distinct datasets to evaluate our suggested technique against existing strategies. Consequently, we evaluated the time required for key generation, data encryption, and decryption. Our proposed method evidently outperforms other cryptographic algorithms regarding key generation time, encryption speed, and decryption speed. This reduction in time directly contributes to a lower computational burden on the system, thereby enhancing its efficiency. A visual representation of the comparisons for key generation, encryption, decryption times, and avalanche analysis can be found in Figures 5, 6, 7, and 8, respectively.

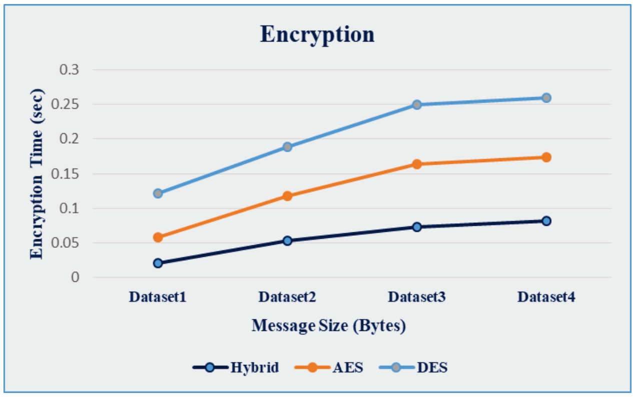

Fig. 6. Encryption time

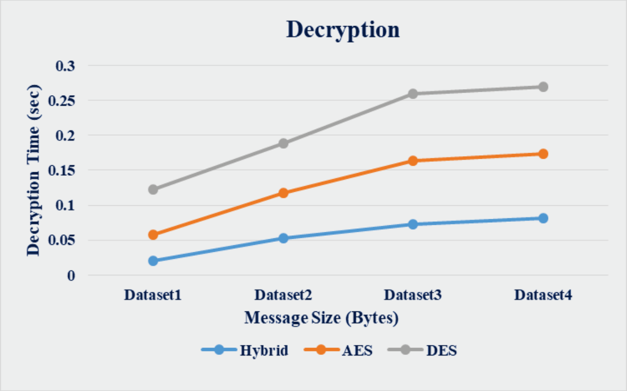

Fig. 7. Decryption time

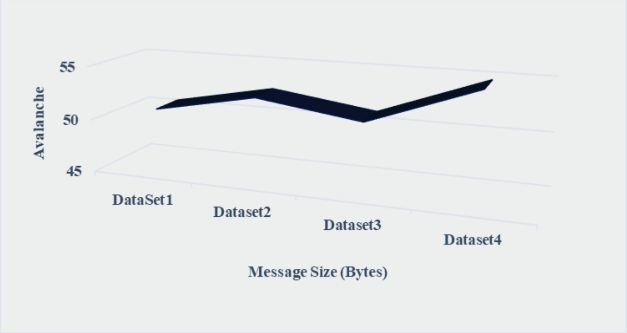

Fig. 8. Avalanche analysis

VII. Conclusion

Ensuring the secure transmission of data in IoT is a very challenging task. We proposed a hybrid algorithm to provide confidentiality to IoT data. We proposed a hybrid confidentiality algorithm, combining DNA cryptography, Genetic Algorithm (GA), and Elliptic Curve Cryptography (ECC). The hybrid algorithm enables robust data confidentiality during IoT data transmission. From the experimental results, our proposed algorithm performs better regarding encryption time and decryption time with respect to various file sizes.

In the future, we want to extend this method to IoT-based Cloud infrastructure, where each IoT device and cloud user will be properly authenticated. Then, only they will be able to read or write the data in the said system. The system will also maintain the digital signature of each and every party, whether IoT device or user, to make a more secure system.

References

[1] Y. Perwej, K. Haq, F. Parwej, M. Mumdouh, and M. Hassan, “The internet of things (IoT) and its application domains,” Int. J. Comput. Appl., vol. 975, no. 8887, p. 182, 2019.

[2] R. Imam, F. Anwer, and M. Nadeem, “An Effective and enhanced RSA based Public Key Encryption Scheme (XRSA),” Int. J. Inf. Technol., vol. 14, no. 5, pp. 2645–2656, 2022..

[3] O. M. Lawal, O. R. Vincent, A. A. A. Agboola, and O. Folorunso, “An improved hybrid scheme for e-payment security using elliptic curve cryptography,” Int. J. Inf. Technol., vol. 13, pp. 139–153, 2021.

[4] R. A. Devi and A. R. Arunachalam, “Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM,” High-Confidence Comput., vol. 3, no. 2, p. 100117, 2023.

[5] P. Kumar and A. Kumar Bhatt, “Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach,” IET Commun., vol. 14, no. 18, pp. 3212–3222, 2020.

[6] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, “ECCbAP: A secure ECC-based authentication protocol for IoT edge devices,” Pervasive Mob. Comput., vol. 67, p. 101194, 2020.

[7] J. R. Arunkumar, S. Velmurugan, B. Chinnaiah, G. Charulatha, M. R. Prabhu, and A. P. Chakkaravarthy, “Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT.,” Comput. Syst. Sci. Eng., vol. 46, no. 1, 2023.

[8] Y.-S. Yang, S.-H. Lee, J.-M. Wang, C.-S. Yang, Y.-M. Huang, and T.-W. Hou, “Lightweight Authentication Mechanism for Industrial IoT Environment Combining Elliptic Curve Cryptography and Trusted Token,” Sensors, vol. 23, no. 10, p. 4970, 2023.

[9] S. Di Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, and S. Saponara, “Secure elliptic curve crypto-processor for real-time IoT applications,” Energies, vol. 14, no. 15, p. 4676, 2021.

[10] G. R. S. Qaid, N. S. Ebrahim, and others, “A Lightweight Cryptographic Algorithm Based on DNA Computing for IoT Devices,” Secur. Commun. Networks, vol. 2023, 2023.

[11] R. Surendiran and K. Raja, “A Fog Computing Approach for Securing IoT Devices Data using DNA-ECC Cryptography,” DS J. Digit. Sci. Technol., vol. 1, no. 1, pp. 10–16, 2022..

[12] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, “Lightweight cryptography system for IoT devices using DNA,” Comput. Electr. Eng., vol. 95, p. 107418, 2021.

[13] B. Al-Shargabi and M. A. F. Al-Husainy, “A new DNA based encryption algorithm for internet of things,” in International Conference of Reliable Information and Communication Technology, pp. 786–795, 2020.

[14] V. Jain and M. Agrawal, “Applying genetic algorithm in intrusion detection system of iot applications,” in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), , pp. 284–287, 2020.

[15] O. M. Lawal, O. R. Vincent, A. A. A. Agboola, and O. Folorunso, “An improved hybrid scheme for e-payment security using elliptic curve cryptography,” Int. J. Inf. Technol., vol. 13, pp. 139–153, 2021.

[16] P. Barmana and B. Saha, “DNA encoded elliptic curve cryptography system for IoT security,” arXiv Prepr. arXiv2311.11393, 2023.

[17] H. D. Tiwari and J. H. Kim, “Novel method for DNA-based elliptic curve cryptography for IoT devices,” ETRI J., vol. 40, no. 3, pp. 396–409, 2018.

[18] I. Kabin, Z. Dyka, D. Klann, and P. Langendoerfer, “Horizontal Attacks against ECC: from Simulations to ASIC,” in Computer Security: ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26--27, 2019, Revised Selected Papers 2, , pp. 64–76, 2020

[19] M. Gupta and A. Sinha, “Enhanced-AES encryption mechanism with S-box splitting for wireless sensor networks,” Int. J. Inf. Technol., vol. 13, pp. 933–941, 2021.

[20] P. C. Sethi, N. Sahu, and P. K. Behera, “Group security using ECC,” Int. J. Inf. Technol., pp. 1–9, 2022.