Journal Européen des Systèmes Automatisés
Vol. 58, No. 6, June, 2025, pp. 1293-1304
Journal homepage: http://iieta.org/journals/jesa

A Lightweight DNA Inspired Logistic Leo Based Attribute Encryption Scheme for Mutual Authentication in Smart IoT Medical System

Somireddy Pavani*, Arun Sahayadhas

VELS Institute of Science, Technology and Advanced Studies, Chennai 600117, India

Corresponding Author Email: somi.phd@velsuniv.ac.in

https://doi.org/10.18280/jesa.580619

Received: 24 May 2025
Revised: 20 June 2025
Accepted: 25 June 2025
Available online: 30 June 2025

Keywords:
DNA PBC, embedded IoT devices, Internet of Things (IoT), logistic Leo

ABSTRACT

Securing the Internet of Things (IoT) devices remain a real challenge as it is susceptible to diverse security intimidations owing to its heterogeneous nature and infrastructure-less deployment. Therefore, ensuring the authenticity, honesty, and secrecy of sensitive data in the implemented region necessitates the establishment of a mutual authentication mechanism among linking components. Many approaches are proposed in the scientific literature to tackle threats to security in IoT smart healthcare environs. However, deploying existing methodologies in the IoT-based healthcare system requires high computation costs and less secure communication. It is therefore to develop an attribute encryption scheme that can safeguard the IoT devices against attacks in medical environments. This paper recommends a novel lightweight and secured protocol relying on the enhanced attribute-based encryption scheme operates based on the principle of DNA-based Chaotic Leo Attribute Encryption (DNA-CLAE) technique using the suggested architecture, authorized devices may unicast dynamic key authentication and change their keys for each transmission cycle, securely transferring private healthcare information from the source to the destination. Additionally, utilizing widely accepted conventional pairing-based cryptography libraries (PBC), the suggested architecture is implemented on embedded Internet of Things gadgets based on Raspberry Pi and ESP8266, and it is contrasted with other contemporary cutting-edge security proprieties. A thorough and formal verification of the suggested approach is conducted using the Automated Validation of Internet Security Protocol Application (AVISPA) to assess as well as analyze the security strength of the framework. Based on the findings, the suggested strategy has demonstrated strong protective qualities towards both proactive as well as passive threats.

1. INTRODUCTION

Over the past few years, the IoT has grown significantly in prominence. Intelligent agriculture, intelligent healthcare, disaster preparedness, defense tracking, and manufacturing automation are just a few of the practical scenarios for applications in the Internet of Things [1-3]. One such well-known area is the IoT-based healthcare infrastructure, which allows gadgets connected via the Internet to function and track patients' health conditions [4]. The IoT has undergone multiple advances and developments as a concept, making it appropriate for several applications and areas of business operations. Security flaws in the form of fraud, eavesdropping, and falsification can be exploited by persistent attackers or malicious internal groups to compromise the security of the cloud and its gadgets, despite the fact the current methods [5-11] offer robust defensive computations towards attacks [12]. Furthermore, malware, such as the Mirai virus [13], can compromise a variety of IoT gadgets, including IoT medical ecosystems [14-16], and disrupt the network's operations.

To deal with the issue, IoT networks must use solutions that offer privacy protection, denial of availability, integrity, confidentiality, authorization, and end-device security [17]. By creating an effective authentication procedure, a whole range of security techniques may be provided. Consequently, the authentication process serves as the primary initial line of defense against both passive and active threats. Hence, mutual verification and session-key agreement are the two tasks that a reliable verification protocol needs to do. By using identity verification, the validation procedure directs to confirm the legitimacy of any entities or equipment requesting access to the private computing system [18]. To accomplish session-key agreement, mutual verification, and defense against breach of security, authentication procedures often employ robust encryption technology. A device's and sensor's setup, as well as the measurement of electric power and energy consumption, are the primary factors in choosing the right encryption method.

It is therefore essential to adapt encryption methods within suitable authentication protocols to meet the demands of modern applications. With the increasing frequency of cyber-attacks, Attribute-Based Encryption Schemes (ABES) [19] have gained prominence as effective cryptographic solutions. Among these, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is widely used for enforcing fine-grained access control. However, applying CP-ABE in IoT environments introduces several challenges, including high computational overhead during encryption and decryption, large memory requirements for key management, and difficulties in managing dynamic user attributes. Furthermore, the need for frequent re-encryption when attribute sets change increases the complexity, making CP-ABE less practical for lightweight and real-time IoT deployments.

In addition, existing ABE schemes suffer from limitations such as high memory consumption, and issues like packet loss. These drawbacks are particularly problematic in IoT systems, where devices are resource-constrained and low-latency communication is critical. All these factors make the existing ABE schemes unsuitable for the IoT systems.

Induced by the current pitfall, this paper presents the unique ABES lightweight authentication protocol based on Chaotic Evoked Panthera Leo Optimization technique to ensure the highest security strength of medical sensitive data. Additionally, the proposed model also introduces DNA encoding which makes the algorithm lighter weight with improved performances over the other existing methodologies. The research study's primary contribution are as follows.

The paper introduced a novel lightweight authentication approach based on a bio-inspired attribute encryption scheme with the high defensive characteristics provided by the hybrid principle of Panthera Leo and Logistic map principles.

The research outlined the DNA encoding technique in place of conventional operations such as permutations and diffusion. This improves the encryption performances over the other existing algorithms in terms achieving the low computational overhead.

Communication costs for several IoT device categories are computed to evaluate the performance of the suggested strategy. This crude parameter allowed us to compute the operating cost of the suggested plan and compare it with more modern methods. Comparing the two reveals that the suggested plan has a lighter design and needs fewer overhead expenses.

We implemented the program for the recommended approach in a widely used Automated Validation of Internet Security Protocol and Application (AVISPA) tool [20] to verify the precision of spontaneous safety assessments.

An analysis and comparison, like existing ABES systems, demonstrate that the proposed technique achieves a reliable design that is more central, productive, and secured against all active and passive attacks [21].

The subsequent sections of the research paper are organized as follows: Many ABES protocols put forth by multiple authors are represented in Section 2. In Section 3, the basic synopsis of DNA encoding methods, logistic chaotic maps, and panther Leo optimization are covered. In Section 4, the suggested model's operation, the key generation procedure, and the authentication procedure are explained in detail. Section 5 provides the theoretical analysis of the proposed protocol by evaluating its mathematical formulation, structural design, and logical foundations. Section 6 presents the comparative analysis, security analysis, and testing validation. Section 7 offers a last reflection on the paper's potential improvements.

2. RELATED WORKS

A cloud-based authentication method that makes use of the benefits of cloud computing was proposed by Fan et al. [22]. This method refreshes authentication data by timestamp and encrypts authentication data using permutations. The security characteristics of the timestamp-permutation protocol are demonstrated by a security study. In a cloud setting with a mixed level of trust, the protocol can safeguard the privacy of the tags. This framework's principal benefit is a decrease in storage and transmission costs, and it also manages the tag's growing processing overhead. However, this framework's disadvantage has been noted as taking more time to process [22].

The Timestamp-permutation protocol for IoT applications was examined by Adeli et al. [23], who demonstrated that their system is susceptible to a disclosure attack. They then advanced the Xperbp Lightweight Authentication Protocol for Internet of Things applications. Put more accurately, the protocol essentially makes the secrets of the tag visible. Executing any other attack is made simple by the tag's secrets. However, this framework's main flaw is increased communication overhead.

An IoT device application security system was introduced by Diwan et al. [24] and it makes use of encryption, integrity checking, and mutual authentication to provide secure communication over insecure communication channels. The multi-layer IoT security architecture that has been proposed demonstrates its resilience with exactness to identify malicious activity. This model also demonstrated that it was simple and required minimal communication resources.

A secure Fog-based Social Industrial IoT system was presented by Ben Amor et al. [25]. Using a trust key agreement, this framework ensures mutual authentication. Since this system simply employs hash functions, bitwise XOR operations, and symmetric cryptography, it is appropriate for the socially resource-constrained Internet of Things (IoT). Regarding security considerations, effectiveness, social awareness, and decreased computing overheads, this approach offers several benefits. But to sustain its performance, it needs more resources [25].

To make certain that individuals only become linked to the Internet of Things (IoT) after completing numerous authentication processes, Gagana et al. [26] are focusing on developing middleware programs that stand among users and the IoT environment. This means that regardless of the event that an attacker manages to obtain the covert key and is incapable to gain access to the verification keys, even though they're inactive, the method of authentication will remain secure. The real-time frameworks weren't covered by this framework, which virtually covered the authentication approaches.

With the help of a limited application protocol, Oliver et al. [27] suggested a reliable and compact authentication technique for client-server mutual authentication. Through this approach, by keeping message packet sizes small, sending few messages, and processing time on connected devices to a minimum, the authentication overhead between the devices is significantly decreased. Its time-consuming nature is its weakest feature.

Chen and Liu [28] examined the upcoming IoT remote protocol. It was discovered using the above structure that not every security attack can defeat the protocol. To solve the problems, this framework created a three-factor surveillance system based on biologic data. This structure showed that the protocol was reliable and secure using BAN logic and ROR testing. Better outcomes are provided by this paradigm in terms of both time and communication costs. However, this approach raised the overhead for authentication.

For IoT-based cloud systems, Zargar et al. [29] introduced a simple and safe authentication technique. By utilizing secret parameters and biometrics, the suggested approach may survive different assaults and offer safe mutual authentication and anonymity. To achieve the most energy efficiency, lightweight crypto modules are used. This paradigm provides more energy-efficient outcomes. However, there will be an extra delay if each edge/fog node authenticates the devices separately, which is unacceptable for real-time service.

A lightweight cryptographic algorithm-based solution is being developed by Kalpana et al. [30] to cater a safe reciprocal authentication technique linking the sensor node and the gateway. For the above framework, a light encryption technique was used to develop the protocol using symmetric-key cryptography, hash-based authentication of messages code and hash algorithm. Better results in terms of authentication time are provided by this architecture. However, the primary restriction found in this system is communication cost as data size grows.

A safe, portable, and anonymous authentication technique created by Son et al. [31] and colleagues is appropriate for IoT contexts. During the authentication process, only hash and exclusive-or operations are used. This framework prevented extra security features and thwarted several attempts. This framework can help improve energy efficiency and cut expenses by providing high security and cheap computing costs. However, this framework's primary drawback is its communication overhead.

Using the Internet of Things, Sivaselvan et al. [32] proposed SUACC-IoT, a novel Secure Universal Authentication and Access Control System Capabilities, which are regarded as tokens representing the ability to grant privileges to those with authorization in the network, form the basis of this framework. This architecture operates superior when it comes to of memory use, processing load, and communication cost. The maximum message conveyed with the protocol has a tolerable transmission cost of 872 bits. However, its excessive energy utilization is the main issue here.

3. PROPOSED METHODOLOGY

This section discusses about the working mechanism of Panther Leo Optimization, Logistic Chaotic maps and DNA encoding techniques.

3.1 Panthera Leo Optimization (PLO)

Panthera Leo Optimization is inspired by the hunting nature of lion’s pride. Lions are socially organized and confronts with the others with high level of aggression. Lions typically live and hunt in groups called Pride(Q). In every Q, specific number of hunting lions follow the encircling strategy (Shown in Figure 1) from the diverse points to hunt its targeted prey. During hunting, every lioness adjusts its location depending on its own or other partner’s location. By understanding the positions, hunter lions in Q circle the prey and strike it from the opposing location, which is mathematically, Opposition-Based Learning (OBL). For an effective hunting process, female lions in the Q are classified into three groups. The best hunter lions (Q”) are placed at the center wings, while the other lions(Q’) are located at left and right wings respectively. The position of each lion in each group is expressed mathematically as

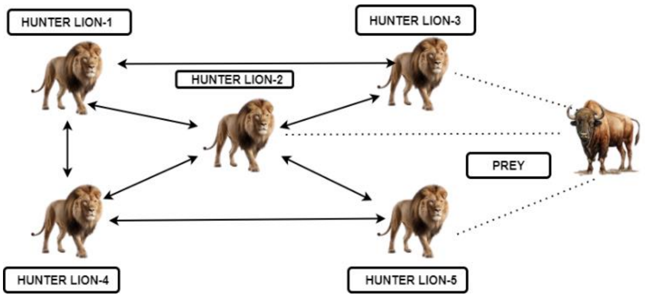


Figure 1. Panthera Leo's Pride's encirclement of its prey (Q)

$$Q' = \begin{cases} rand\big((2 \times P - Q), P\big), (2 \times P - Q) \\ rand\big((2 \times P - Q)\big), (2 \times P - Q) \end{cases} \tag{1}$$

The position of the center lions is expressed mathematically as

$$Q'' = \begin{cases} rand(P), Q \\ rand(P, Q) \end{cases} \tag{2}$$

After forming hunting groups, each group follows different prey to catch. The prey of each subgroup is selected randomly from the best position of all pride members. The fitness function for forming:

$$P = Q'' + rand(0,1) \times ZI \times (P - H) \tag{3}$$

where, *P* denotes the location of prey, *H* is the new location of the lions, which attacks the prey, and *ZI* is the percentage of enhancement in the hunter's fitness. The random numbers between 0 to 1 is selected. This mechanism gives a circle-shaped neighborhood around the prey, which makes the hunters step nearer to the prey from different directions.

3.2 Chaotic Panthera Leo Optimization

As mentioned in Eq. (3), adjustment of lion’s fitness leads to the failure in capturing its prey. This leads to the time consumption process to achieve its target. To increase the fitness position of hunter lions, Chaotic theory has been introduced for aligning the lion’s fitness in accordance to distance of the prey.

These maps possess dynamic capabilities that enable you to break free from your current setting while accelerating your search efforts. A deterministic process that resembles randomness emerges in nonlinear, period-less, dynamic systems that are finite and non-converging. It is also sensitive to beginning values. The behavior of a complex system is extremely unpredictable when it displays chaos properties. Chaotic systems show deterministic dynamical structures that produce random behavior and act as randomness generators. The chaos-based optimization algorithm utilizes chaotic sequences created from chaotic maps as design variables within the global optimization process rather than random sequences.

In this research, Logistic Chaotic Maps are employed in PLO to overcome time consumption problem by achieving the high capturing efficiency. As discussed, all random positions rand are replaced with the chaotic variables RC which is derived from the logistic maps.

The position of each lion in each group is expressed mathematically as

$$Q' = \begin{cases} R_c((2 \times P - Q'), P), (2 \times P - Q') \\ R_c((2 \times P - Q')), (2 \times P - Q') \end{cases} \quad (4)$$

The position of the center lions is expressed as

$$Q'' = \begin{cases} rand(\ P), Q'' \\ rand(P, Q") \end{cases} \quad (5)$$

New fitness function is formulated by considering the chaotic variables as

$$P = QZ + rand(0,1) \times QZI \times (P - Hunter) \quad (6)$$

The integration of logistic maps in deciding the position of the hunter lions gives an omni-directional trapping round the prey, which makes the hunters step nearer to the prey in any direction with high speed and less time.

3.3 DNA computing process-An brief overview

Table 1. Pairing conditions of DNA

	1	2	3	4	5	6	7	8
AD	00	00	11	11	01	10	01	10
TH	11	11	00	00	10	01	10	01
CY	10	01	10	01	00	00	11	11
GU	01	10	01	10	11	11	00	00

Table 2. Rules of DNA addition

	1	2	3	4
AD	AD	TH	GU	CY
TH	TH	CY	GU	AD
CY	GU	AD	CY	TH
GU	CY	GU	TH	AD

Table 3. D-XOR conditions

	1	2	3	4
AD	AD	TH	GU	CY
TH	TH	AD	CY	GU
CY	GU	AD	CY	TH
GU	CY	TH	GU	AD

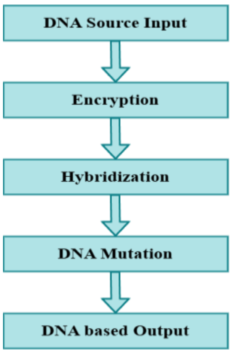


Figure 2. Flowchart of the DNA computing process

A DNA computing involves the use of four nucleotides — “Adenine” ("AD"), "Guanine” ("GU"), "Cytosine" ("CY"), and "Thymine” ("TH") as fundamental elements of encoding. According to biological pairing rules, ‘AD’ pairs with ‘TH’, and ‘GU’ pairs with ‘CY’. These pairing relationships form the basis for encoding both encryption keys and plaintext data into DNA sequences.

The encryption scheme utilizes Tables 1 to 3 to perform logical operations on these encoded sequences. Table 1 presents the DNA pairing conditions that help establish binary representations of each nucleotide, allowing for secure bit-level transformations during encoding. Table 2 defines the rules for DNA Addition, a modular operation that contributes to data diffusion and strengthens resistance against statistical attacks. Table 3 outlines D-XOR conditions, enabling a non-linear transformation that ensures confusion and unpredictability in the cipher structure. Together, these DNA operations are applied in algebraic dimensions such as D-Addition, D-Subtraction, and D-XOR to achieve high entropy and enhance randomness. These operations play a vital role in generating secure cryptographic keys and producing robust encrypted outputs.

Figure 2 illustrates the step-by-step transformation from source input through encryption, hybridization, and mutation to produce the final DNA-based output. This process ensures secure and randomized encoding for cryptographic applications.

4. SYSTEM MODEL

Figure 3 displays the system model taken into consideration for IoT topology. The suggested model consists embedded IoT devices linked to a single gateway. Only via the gateways, which use wireless communication protocols like WiFi, LORRA, and BLE, may any gadget interact with any other gadget. Bothe the 8-Bit and 32-bit based IoT devices are involved in the experimentation process. The shared secret key could be manually configured by an administrator into gateway and IoT equipment. IoT devices and gateways must function without the aid of a third party (TTP). In the non-volatile memory of embedded controllers, that are deemed as the brains of the Internet of Things, are all the private keys, device IDs, and gateway IDs. To carry out interactions between the gadget and gateway, a few megabytes (MB) of RAM are also essential. For updating the current session key, RAM is utilized to retain all the data that was sent during the prior networking session. Since attackers cannot physically access the gadgets, the entire architecture deliberates that the suggested protocol network structure is installed in a secured location. In that manner, they are unable to find the secret keys that are set up and kept on the gadgets.

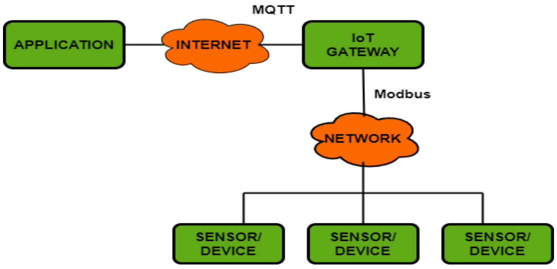


Figure 3. IoT and gateway system model used in the research proposal

4.1 Security prerequisites

Every unprotected device linked to the Internet might act as a point of entry for cyberattacks as there is an explosive growth of IoT devices. This is because weaknesses are more likely to arise with this growth. A new IoT paradigm must be designed to overcome the security issues and offer unparalleled authentication data integrity and secrecy, since security is now deemed to be of the utmost importance in IoT gadgets. To address these security concerns, the suggested protocol has been created.

4.2 Key generation using proposed ABE scheme

The proposed ABE schemes used for key generation and data encryption is based on key-policy ABE schemes. In this encryption system, the user selects the attributes and encrypts the plain text to pair them. In short, the cipher text is linked with the set of attributes and access policy is linked with the private keys. The decryption process is evoked based on the private keys generated at other side(transmitter) and same can be used for authentication mechanism. The following steps are incorporated for generating the keys using proposed ABE schemes.

4.2.1 Initialization phase

In the initialization process, attributes from the sensors are connected to the IoT devices. The best fit attributes are selected based on the functions of CEPLO as mentioned in Eq. (6). Algorithm-1 presents the initialization stage

Step	Algorithm-1 // Process in the Initialization Phase
1	Input: Sensor Values U from IoT devices
2	Output: Chaotic PLO Sequence generation
3	Start
4	Collect and Store the Sensor data from the devices
5	Preprocess the Data stored
6	Select the sensor data in accordance to the Eq. (1) and Eq. (2)
7	Calculate the global best using Eq. (6)
8	If the global best is equal to Eq. (6)
9	Fix the attributes as the initial conditions of Logistic Maps
10	Else
11	Go to Step 6
12	End
13	End

4.2.2 Encryption phase

The double-layered encryption process is adopted to obtain the strong encrypted data to mitigate the different attacks on the IoT networks. In the first layer, attributes selected from Eq. (6) are encrypted with the Chaotic maps (*K*) to form the intermediate encrypted data $\boldsymbol{E_I}$. Then the formed intermediate data is again encrypted with chaotic maps (*K*) to form the final encrypted data $\boldsymbol{E_m}$. In the both layers, permutations and diffusions are replaced with DNA encoding techniques. In the first layers, DNA subtraction is performed between the selected attributes and keys while DNA XOR operation is adopted in the second layer. Mathematically, the encryption process is expressed as follows

The first layer of encryption process is expressed as

$$E_I = mod(byte\{ (U_{attributes})DNA(K)(input), 16\}) \tag{7}$$

Final encryption process is expressed as

$$E_m = mod(byte\{ (E_I)DNA(K)(input),16\}) \tag{8}$$

In Eqs. (7) and (8), $U_{attributes}$ denotes the user-selected attributes, and *K* represents the chaotic key generated from the map. The operator *DNA(input)* refers to the DNA-based encoding operation, including subtraction and XOR. The *byte{}* function converts the encoded data into byte format, and mod (16) ensures normalization within the 4-bit DNA space.

4.2.3 Proposed mutual authentication protocol

Amongst IoT devices, gateways, and users, the recommended protocol offers a safe mutual authentication method. The Internet of Things network's security resilience is improved. An intermediary gateway is placed in connection with the sensors, gateways, and users, as stated in the System Architecture. These characteristics characterize the suggested protocol: (i) The gateways and Internet of Things devices may securely authenticate each other using this protocol. (ii) Both the primary secret keys that the protocol uses—the dynamic chaotic key (Lk) and the encryption data (Em) utilized throughout mutual authentication phases. The disorganized features introduced into the key construction alter the keys continuously beyond a specified transaction interval. All the potential credentials never switch to networks since they are kept in storage by the gadgets and gateway during deployment. (iii) The suggested procedure, which operates based on logistic chaotic oriented ABE strategies, is new and lightweight authentication mechanism. The initial conditions are formulated using ABE schemes and consequently the key which is formulated will exhibit the high randomness nature which prevents the attackers to get the information. Device ID hashes and Gateway ID hashes are saved in the respective devices to improve overall security on the network. Ensuring strong security throughout the common authentication process is facilitated by the inclusion of suggested chaotic keys and their storage in relevant devices. (iv) When it comes to energy usage and transmission of messages times throughout mutual authentication and data transfer, the suggested protocol is being created among IoT gadgets, gateways, and users. Table 4 provides an inventory of the acronyms utilized in the present research.

Table 4. List of all the acronyms utilized in the text

Sl.No.	Notations	Description
1	E_m	IoT gateways and devices permanently keep the encryption key
2	L_k	Updated for Every Session in the Whole
3	$H(I_i)$	keys hashed for the devices
4	$H(G_i)$	keys hashed that were created for the gates
5	$Session_{(T)}$	Update the key during this session
6	$Session_{(T+1)}$	The next time's session for changing the key
7	$Seq_{\{i\}}$	Sequence produced at random for the updating of the session time key
8	$Seq_{\{i+1\}}$	The session {i+1} time-key update is created using a random sequence
9	L	The key length
10	C1, C2	Sequences that are produced at random for every task
11	D-LLAES	DNA based Leo Logistics Based AES

4.2.4 Mutual authentication phases

The 3 steps that make up this phase of the process are covered in the following discussion.

Step-1: IoT devices --→ Gateway:

By providing the gateway with a generated at random task C1 and the hash of the gadget ID, the Internet of Things gadgets within the network can initiate the mutual authentication procedure. We use a key Lk to encrypt the first authentication message. All IoT devices use the initial update key to compute the total amount of time needed to send the message to ensure message validity and authenticity.

Step-2: Gateway -→ IoT devices:

When the IoT device sends a message to the gateway asking for mutual authentication, it decrypts it first, then checks the decrypted IDs it receives with the identities it has stored. The following stage, the authentication procedure, is initiated if both IDs are equivalent. The authentication procedure is unsuccessful otherwise. For the subsequent communication, IoT gadgets choose a set of numbers that represent sequences Seq{i} to be utilized when updating the session key, the newly produced challenge C2, the already established session duration Session(T), N1, besides the hash value of its ID (Hash (Device ID)), all of which are encrypted with (Ek)which uses Ec to determine the RSSI (msg2) and transmits to IoT gadget.

Step-3: IoT-Devices -→ Gateway:

After decrypting communication and matching it against the previously saved hash, the sensor examines the second message it got from the gateway. If both hashes match, the process for authentication is carried out by comparing the RSSI with the threshold RSSI (-100dBm). IoT devices authenticate gateways and verify that the gateway has selected the proper option for data transfer if the data meets the threshold RSSI. Authorization fails if RSSI doesn't meet the criteria. An Internet of Things gadget computes the hash of C2, random number sequences Sen{j+1}, session time (S+1), and RSSI for the entire message, encrypts it with key (Ek), and sends it to gateway to validate that it was able to receive the message from the gateway.

4.2.5 Communication between the IoT devices and gateways

Upon receiving message 3 from a gateway, the sensor authenticates h(Gid) and MACKik (msg4) by decrypting the message. When message 3 gets delivered by the gateway effectively, the mutual authentication procedure is said to be completed if it is legitimate.

5. SECURITY STRENGTH ASSESSMENT

To assess thee suggested protocol's security resilience, conceptual security evaluation is provided in this part. When higher chaotic keys are provided, the suggested protocol's resilience is increased and shown to be more resilient. The results of the security study demonstrate the fact that the protocol can resist a variety of assaults, including impersonation, brute force, and Man-in-the-Middle attack scenarios.

5.1 Man-in-the-middle attack (MIM)

An active attacker surreptitiously acquires data among both sides using a protected communication channel assault called "Man-in-the-Middle attack." Invaders can read, write, interrupt and even destroy data, closing off the transmission route. The attacker must possess the encryption keys to decipher and alter the information contained in this suggested protocol if he manages to intercept messages among IoT gadgets. Since the high randomness chaotic keys are used for the encryption, attackers are unlikely to extract the information in the communication channel. Attackers are unable to gain all the keys since there is rarely any key exchange over the network, even when two separate chaotic keys are utilized. The data cannot be decrypted and altered by an attacker as a result. Therefore, the suggested technique can fight off MIM assaults.

5.2 Brute force attack (BFA)

An assault known as a "brute force" occurs when an attacker attempts to crack a password or secret key used to decode a communication. One is unable to execute a brute force attack against this suggested practice for all 3 causes listed. Firstly, the great degree of unpredictability in the keys makes it challenging to find using a brute force assault. Secondly, no private keys are ever shared via the network; instead, the secret keys are kept in the memory of the gateway and IoT gadgets. As a result, an assailant would find them extremely challenging to find. Finally, the attacker cannot initiate the mutual authentication process, since the process involved is kept on the darker side of the communication channel. Thus, the proposed protocol can be defended against the brute force attacks.

5.3 Impersonation attack

The attacker's purpose in this type of attack is to imitate a valid user address. To achieve self-duplication, the attacker must understand each stage of the mutual authentication system, which they cannot uncover. Thus, the proposed protocol can withstand identity-based attacks.

5.4 Data integrity and confidentiality

When there is no duplication, placement, alteration, or rearrangement of the messages, the information's integrity verifies that they have been received exactly as sent. The usage of CEPLO technique in the proposed research can provide both data integrity and confidentiality. To manipulate the process of sending messages, hackers must disrupt the dynamic, chaotic chains that forms between the sender of the message and the recipient. This is still a daunting challenge for the intruder.

5.5 Replay attacks

In a replay attack, a hacker listens to real communications transmitted throughout the authentication process and then replicates those conversations to an authorized participant to begin the authentication process.

Table 5. Strengths of different works

Attacks	[28]	[29]	[30]	[31]	[32]	Proposed Model
MIM Attacks	----	----	----	----	E	E
BF Attacks	----	-----	-----	-----	E	E
Replay Attacks	-----	----	E	E	E	E
Impersonation Attacks	----	---	E	---	E	E
Confidentiality	E	----	----	E	E	E
Integrity	E	----	----	E	E	E
DoS Attacks	E	------	----	---	----	E

Notes: E=Efficient Detection

The proposed protocol's comparison study with the other cutting-edge procedures, as stated in references, is summarized in Table 5, which proves that the model proposed can defend against any attacks.

6. EXPERIMENTATION

In this section, security and lightweight characteristics are analyzed using the Communication Cost, and encryption time. Additionally, AVISPA and tools are also used to authenticate the security strength of the suggested protocol. Embedded C programming is adopted for deploying the proposed protocol in the Arduino and ESP8266 based IoT applications where as python is used for raspberry and creating the various test environments. Tos implements the proposed ABE schemes; it is mandatory to install PBC (pairing based cryptography) library on Arduino and raspberry pi. Randomness of the keys and encrypted data uses NIST STS version 2.1.2 which was developed by Python 3.19. For AVISPA simulation, specific parameters were used to control the analysis behavior and execution. These are summarized in the following Table 6:

Table 6. Simulation settings

Parameter	Description	Details
-t	Time limit for execution	200 secs
-n	Number of parallel sessions	3
-fs	Enable/disable finite session model	on

These simulation settings ensure consistent and controlled security verification across multiple sessions, helping to validate the protocol’s resistance to various attack models.

6.1 Communication cost

Assuming that there are five to ten sensors inputs per IoT device and that the integrated microcontroller serves as the device's brain, the suggested protocol’s communication cost is assessed. Based on the sensor inputs, communication cost is calculated on the authentication process. The suggested ABES is used throughout this endeavor to encrypt all credentials used for authentication beforehand sending them to the recipient. The number of bits communicated in the complete process of validation is used to calculate communication cost. Table 7 illustrates the hardware specification used for the experimentation.

Table 7. Experimental setup for the calculation of communication cost

Sl.No	IoT Devices Used	Specification
1	Embedded Hardware	8-bit/32-bits
2	Number of Sensors	5
3	Type of Sensors	Health care
4	IoT transceivers	WIFI

Table 8. No of bits transmitted during the authentication protocol (Assuming 8-bit IoT devices with 5 sensors)

Sl.No	Authentication Stages	Total Bits Transmitted
1	Process 1(p1, p2)	(36+256)=292
2	Process 2(p3, p4)	(292+256)=548
3	Process 3(p4, p5, p6)	548+40=622
4	Process 4(p7, p8)	256+180=436

Table 8 and Table 9 provide a detailed breakdown of the total number of bits exchanged during each stage of the authentication protocol for 8-bit and 32-bit IoT devices equipped with five sensors respectively. In Table 8, the 8-bit devices transmit a cumulative total of 1720 bits, distributed across four stages involving multiple message exchanges. Similarly, Table 9 shows that the 32-bit devices incur a higher communication overhead, totaling 1048 bits, due to wider data widths per transmission. These values reflect the cost of securely exchanging encrypted attributes and authentication hashes between the IoT devices and the gateway. This stage-wise breakdown highlights the communication efficiency of the proposed protocol across different hardware architectures. The suggested protocol requires a lower communication cost compared to references [29, 30], and references [31, 32], as outlined in Table 10. This efficiency is further illustrated in Figure 4, which compares the total communication bits of different approaches and clearly shows that the proposed protocol achieves the least overhead. Thus, from the standpoint of resource-constrained environments, the suggested protocol proves to be more suitable for Internet of Things devices.

Table 9. Total bits transmitted during the authentication protocol for 32-bit IoT devices

Sl.No	Authentication Stages	Total Bits Transmitted
1	Process 1(p1, p2)	(256+256)=512
2	Proecess 2(p3, p4)	(512+256)=768
3	Process 3(p4, p5, p6)	768+40+40=848
4	Process 4(p7, p8)	848+200=1048

Table 10. Communication bits analyis

Sl.No	Approaches	Total Communication Bits
1	Ref [29]	1910
2	Ref [30]	1734
3	Ref [31]	1934
4	Ref [32]	2006
5	Proposed Model	1720

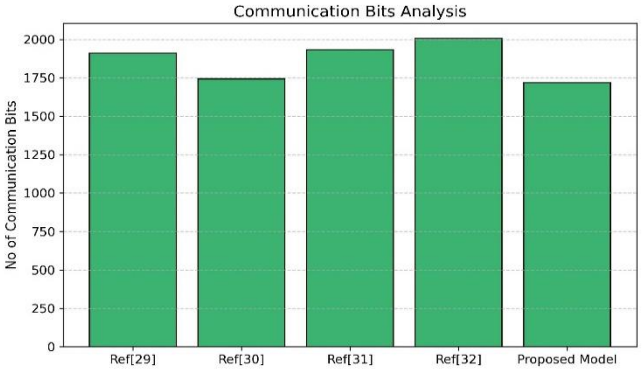


Figure 4. Comparison of total communication bits between different approaches

6.2 Authentication performance analysis

As the number of processes increases, the time required for key creation, encryption, and decryption is estimated. For every stage of authentication, execution time is calculated for the varying iterations. For these experimentations, attributes are increased randomly and time consumption for each iteration is calculated. Figures 5 and 6 shows the execution involved in encryption, decryption and authentication process for distinct embedded processors.

From the Figures 5 to 8, it is clearly identified that the time consumption is increasing linearly with the varying iterations and increasing attributes. The most time consumption process is key management and authentication process. As the iteration increases, average encryption time in raspberry pi is 8.7secs for 60 iterations whereas Arduino +esp8266 takes only 5.3secs for completing the entire process. For the same number of iterations, raspberry pi's decryption time is 8.8secs and 8-bit system requires only 4.2secs. Furthermore, key generation and authentication phases consumes 37.34secs and 27.45secs in raspberry and other low end embedded systems. From this experimentation, the time consumption for each stage is quite low which can be suitable for porting in the resource constraint IoT devices.

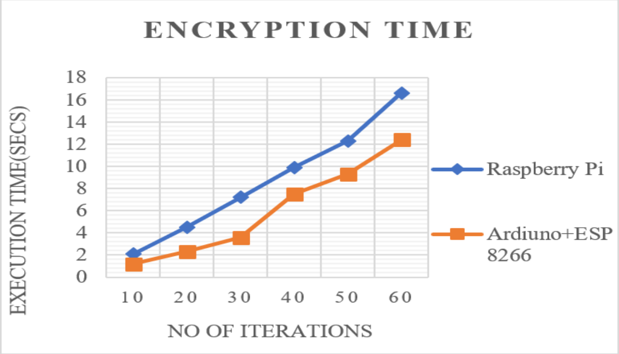


Figure 5. Time consumption analysis for encryption process using the proposed protocol

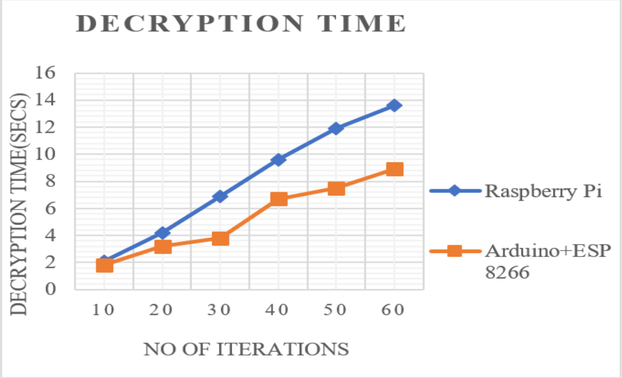


Figure 6. Time consumption analysis for decryption process using the proposed protocol

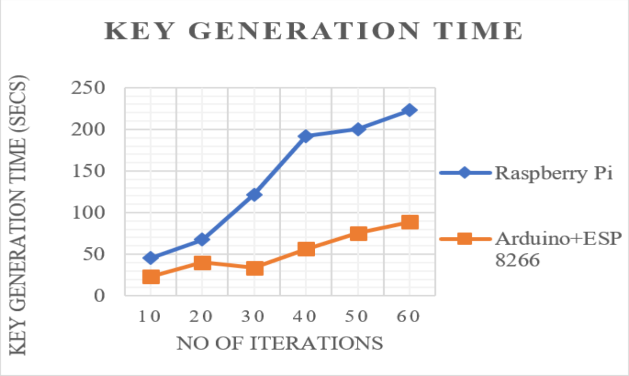


Figure 7. Time consumption analysis for key generation process using the proposed protocol

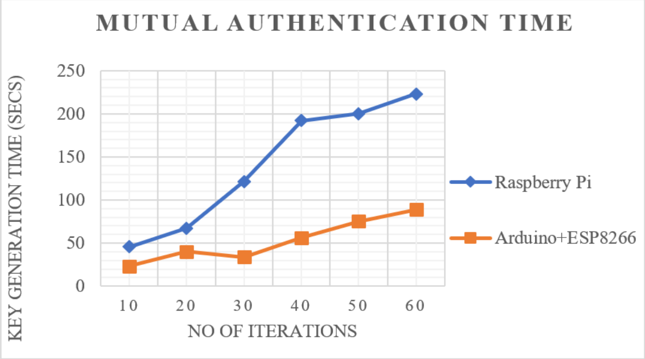


Figure 8. Time consumption analysis for authentication process using the proposed protocol

6.3 Security analysis

The key utilized to encode and decode the communications is closely related to the security features of any cryptography system. Owing to the symmetric nature of the encryption system, the gadget is susceptible to various attacks once the attacker obtains the key. Thus, it is imperative that we guarantee the key generator's genuine randomness and prevent it from approaching.

An adversary cannot anticipate the next output bit in a sequence generated for cryptographic applications, even if they know the arbitrary numbers in the sequence. This means that pseudorandom numbers created for cryptographic applications must also be unaffected. To verify that a particular random or pseudo-random generator may be expended for cryptography. National Institute of Standards and Technology (NIST) describes a series of statistical assessments for the randomness of the sequences of numbers. Sensing any difference from randomness in each binary sequence is the goal of the approaches discussed here. A poor-quality generator primarily explains the variance. To demonstrate that the keys are highly random, the study project employs almost a variety of numerical tests as outlined by NIST. The experiments are conducted on a sample size of 100 iterations, with a sampling frequency of 1 kHz. Using MicroPython modules installed on embedded boards, the keys generated at each iteration are transformed into binary format and subjected to statistical tests.

6.3.1 Frequency monobit test

Throughout the test, the percentage of ones and zeros is what matters most. To ascertain that a sequence has about the same number of ones and zeros as predicted for random sequence, this test examines that question. The test evaluates how closely the ratio of ones to ½ is kept to a minimum—namely, how nearly equal the number of zeros and ones in a series occur. This test's success is a must for completing all others. The test gives a value of -1 to zeros and a value of +1 to ones. These values are then added up to generate cumulative numbers, the total computation of which is outlined below:

$$S = ||S(n)||/n^{0.5} \tag{9}$$

In this case, n is the sum of samples, and S(n) is the sum of values obtained. P-value is determined by the mathematical equation, when the sum of the individual numbers is calculated.

$$P=\mathrm{erfc}(S/2)^{\wedge 0.5} \tag{10}$$

Table 11. Frequency monobit test performance

Iteration Count	Nature of Test	Rule Decision	Randomness (P)	Key Test
1	Frequency Monobit	P>0.01	0.0678900	PASS
2			0.056493	
3			0.076503	
4			0.067633	
5			0.046789	
6			0.025653	
7			0.035542	
8			0.074589	
9			0.675302	
10			0.542300	

Table 12. Frequency block test performance

Iteration Count	Nature of Test	Rule for Decision	Randomness (P)	Key Test
1	Frequency Blockbit	P>0.01	0.10125	PASS
2			0.29022	
3			0.30290	
4			0.20982	
5			0.20865	
6			0.19852	
7			0.15689	
8			0.19078	
9			0.20892	
10			0.30201	

The parameters which are obtained during the frequency monobit tests are tabulated in Table 11

The proposed model has produced keys that have demonstrated genuine randomness in all ten rounds, indicating their appropriateness for robust encryption and potential protection against network assaults.

6.3.2 Frequency block test

The purpose of this test is to determine if the frequency of those in a K -bit block is approximately k/2, regardless of the assumption of randomness. Frequency (Monobit) test, test 1, is the degenerate test for block size k=1. In this test, the randomness of each repetition of K-bit encryption is determined by the mathematical formula, which divides it into K/2.

$$P = igamc(\frac{N}{2}, \frac{¥^{0.5}(obs)}{2}) \qquad (1)$$

where, $igamc$ is the gamma function used for calculation of randomness,

$$¥ = \text{statistical randomess value which is given by the mathematical expression}$$

For every single key created and analyzed under two conditions, the randomness value is more than 0.01 in the entire iterations tested. The mean score from the tests conducted in the key blocks is displayed in the Table 12.

6.3.3 Run test

A sequence test measures the number of continuous identical series of bits called runs. When you see a run of length k it means there are k identical bits separated by bits of the other value. The runs test checks if the number of runs of ones and zeros of different dimensions matches that of what we assume from a random sequence. (Table 13). The purpose of this test is to specifically assess how quickly or gradually the oscillation between these zeros and ones vacillates.

The frequency test is made necessitous for this exam by the instances that have been completed before. A randomness analysis of the key's continuation is conducted which is mentioned in reference [33].

When there are numerous changes in the bit streams, quicker oscillations—which are defined as a switch from one to zeros—occur in this test, as identified by V(n)(Obs). Therefore, for the bit generated by the suggested ABE maps, strong pseudo randomness is used.

6.3.4 Longest run test

The main objective of the criterion is the longest run of M-bit blocks. To determine whether the length of the longest run of ones in the sequence under test is consistent with the length of the longest run of ones that one would anticipate in a random sequence, this test is intended to do. It should be observed that an anomaly in the longest run of ones' predicted length suggests existence of an abnormality in the longest run of zeroes' expected length as well. Table 14 illustrates the intermediate results of this test. From the Table 14, proposed scheme has produced the high random keys that can grant the defensive properties against the multiple attacks.

6.3.5 DFT Test

Peaks in the sequence's Discrete Fourier Transform are the focus of this exam. This test's objective is to identify recurrent characteristics in a chronological sequence under test indicating departure from the assumption of randomness. Table 15 demonstrates the DFT test performance of the proposed model. From the Table 15, the proposed model met the DFT test and produced the most random bits in its experimental iterations.

Table 13. Runtest performance

Iteration Count	Nature of Test	Rule for Decision	Randomness Measurement	Key Test
1	Run test	P>0.01	0.11278	PASS
2			0.67829	
3			0.12909	
4			0.45262	
5			0.67829	
6			0.12678	
7			0.12456	
8			0.29082	
9			0.23561	
10			0.290192	

Table 14. Longest run test performance of the proposed schemes

Iteration	X	X1	X2	D1	P	Key Test (P>0.1)
1	100	45	67.3	-2.456298	0.56472	PASS
2	100	46.4	65.5	-4.5890	0.9876	
3	100	45.3	76.0	-7.46789	0.78362	
4	100	45	54.0	-1.8930	0.45678	
5	100	47.2	78.0	-4.5789	0.53637	
6	100	54	65	-2.5700	0.1789	
7	100	43	66	-2.7650	0.25678	
8	100	57	68	-3.8902	0.5234	
9	100	58	69	-4.6782	0.9876	
10	100	43	65	-1.9087	0.12892	

Table 15. DFT test performance of the recommended scheme

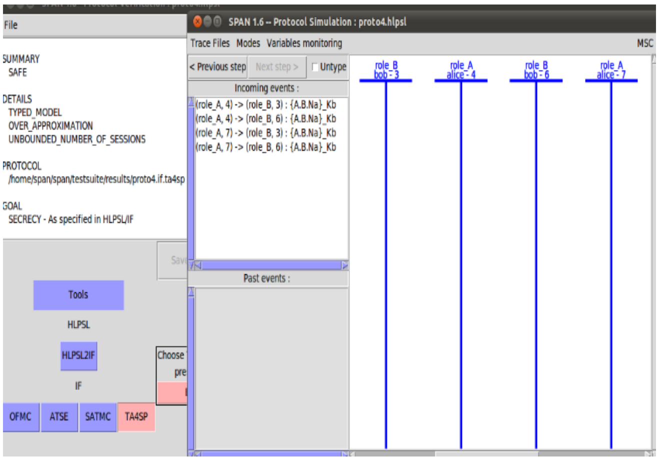
Iteration	N	N1	N2	D1	P	Key Test (P>0.1)
1	100	45	67.3	-2.456298	0.56472	PASS
2	100	46.4	65.5	-4.5890	0.9876	
3	100	45.3	76.0	-7.46789	0.78362	
4	100	45	54.0	-1.8930	0.45678	
5	100	47.2	78.0	-4.5789	0.53637	
6	100	54	65	-2.5700	0.1789	
7	100	43	66	-2.7650	0.25678	
8	100	57	68	-3.8902	0.5234	
9	100	58	69	-4.6782	0.9876	
10	100	43	65	-1.9087	0.12892	

The key displays considerable pseudo randomness in every iteration when the d value is small and P is greater than 0.01.

6.4 Protocol validation phase

The protocols are validated over AVISPA by modelling through CAS++ and HLPSL. The protocols are validated for the security attacks feasible on them. Figures 9 to 11 shows the simulation results under Messaging Servers that run at the backend.

Simulation results demonstrate that recommended protocol can defend against any attacks and solve the defense challenges of an IoT environment.



SPAN 1.6 -- Protocol Simulation : proto4.hlpsl

SUMMARY
SAFE

DETAILS
TYPED_MODEL
OVER_APPROXIMATION
UNBOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
/home/span/span/testsuite/results/proto4.if.ta4sp

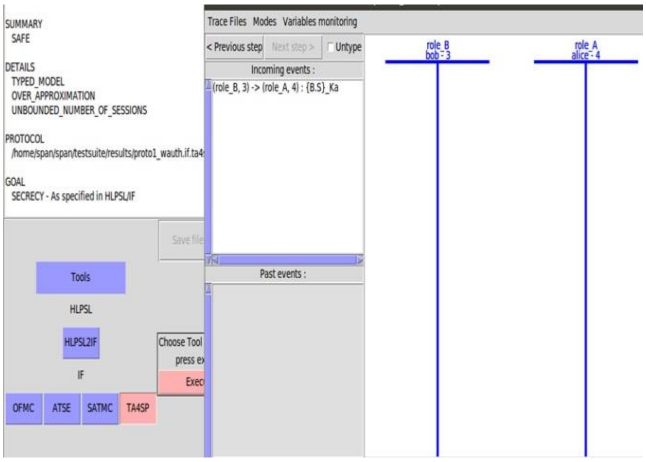
GOAL
SECRECY - As specified in HLPSL/IF

Incoming events :

```
(role_A, 4) -> (role_B, 3) : {A.B.Na}_Kb
(role_A, 4) -> (role_B, 6) : {A.B.Na}_Kb
(role_A, 7) -> (role_B, 3) : {A.B.Na}_Kb
(role_A, 7) -> (role_B, 6) : {A.B.Na}_Kb
```

Past events :

Figure 9. HLPSL file programmed for the proposed authentication protocol



SUMMARY
SAFE

DETAILS
TYPED_MODEL
OVER_APPROXIMATION
UNBOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
/home/span/span/testsuite/results/proto1_wauth.if.ta4

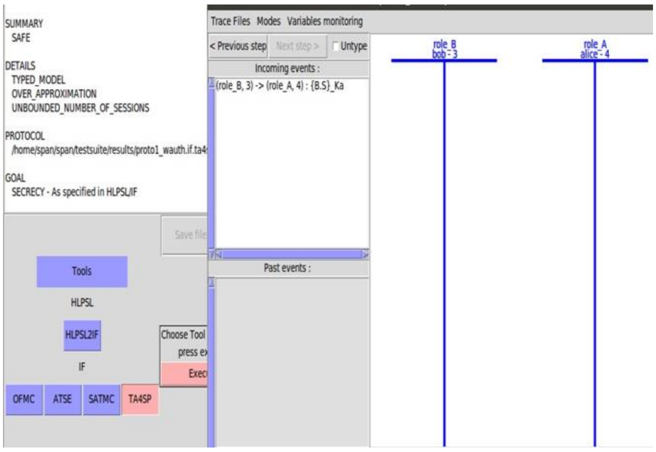
GOAL
SECRECY - As specified in HLPSL/IF

Incoming events :

```
(role_B, 3) -> (role_A, 4) : {B.S}_Ka
```

Past events :

Figure 10. CAS++ programs simulated in AVISPA-SPAN environment



SUMMARY
SAFE

DETAILS
TYPED_MODEL
OVER_APPROXIMATION
UNBOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
/home/span/span/testsuite/results/proto1_wauth.if.ta4

GOAL
SECRECY - As specified in HLPSL/IF

Incoming events :

```
(role_B, 3) -> (role_A, 4) : {B.S}_Ka
```

Past events :

Figure 11. Mutual authentication programs simulated in AVISPA-SPAN environment

6.5 Statistical analysis

To analyze the effectiveness of the proposed optimization techniques, a statistical comparison was performed using standard fitness metrics, including best, worst, mean, median, standard deviation (SD), and variance. Table 16 presents the outcomes of different optimizers such as Binary Whale Optimization (BWO), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Random Search Optimization (RSO), and the proposed Optimization. Among all, suggested framework emerged as the best-performing method, demonstrating the highest fitness score with minimal variation.

Table 16. Statistical results of fitness function between different techniques

Algorithm	Best	Worst	Mean	Median	SD	Variance
BWO	0.7490	0.6435	0.72008	0.022819	0.06532	$7.38x10^{-6}$
PSO	0.730330	0.63525	0.69034	0.020202	0.07033	$6.390x10^{-6}$
ACO	0.7523	0.6763	0.65372	0.027820	0.068903	$5.892x10^{-5}$
RSO	0.77435	0.6902	0.71239	0.02039	0.054637	$4.1288x10^{-4}$
Proposed Model	0.99763	0.81202	0.8564	0.06344	0.03763	$2.28933x10^{-4}$

7. CONCLUSION AND FUTURE ENHANCEMENT

In the context of this research, CP-ABE based authentication protocol for resource constraint IoT device is presented. To overcome the existing problems in the security protocols, this paper introduces the novel light weight authentication process based on CP-ABE s for an IoT devices deployed for the smart health care applications. To diminish the complexity and to ensure the confidentiality, integrity and security, the hybrid amalgamation of DNA encoding, Panthera Leo Optimization and Logistic Chaotic maps has been proposed for designing the mutual authentication process between the IoT gadgets. This protocol prevents the intruders to steal the data, since the usage of optimized chaotic principles in the encryption, decryption, key generation and authentication process. The extensive experimentations are carried out in different embedded IoT devices and performance are measured and evaluated. Outcomes presented that the suggested process has exhibited the superior performance over the other authentication process based on

CP-ABE systems. As the future direction, the proposed scheme requires more improvisation in terms of achieving the energy efficient and latency aware protocol so that it can be tailored for any resource constraint IoT devices.

REFERENCES

[1] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access, 7: 82721-82743. https://doi.org/10.1109/ACCESS.2019.2924045

[2] Liu, X., Zhao, M., Li, S., Zhang, F., Trappe, W. (2017). A security framework for the Internet of Things in the future internet architecture. Future Internet, 9(3): 27. https://doi.org/10.3390/fi9030027

[3] Mahmood, Z., Ning, H., Ghafoor, A. (2016). Lightweight two-level session key management for end user authentication in internet of things. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, pp. 323-327. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.78

[4] Annamalai Renu, S., Gupta, A. (2025). A Blockchain-IoT framework for preventing counterfeit medical supplies via ride-sharing networks. Journal Européen des Systèmes Automatisés, 58(2): 225-236. https://doi.org/10.18280/jesa.580204

[5] Mallik, A. (2018). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2): 109-134. https://doi.org/10.22373/cj.v2i2.3453

[6] Joh, H., Yang, I., Ryoo, I. (2016). The internet of everything based on energy efficient P2P transmission technology with Bluetooth low energy. Peer-to-Peer Networking and Applications, 9(3): 520-528. https://doi.org/10.1007/s12083-015-0377-4

[7] Joh, H., Ryoo, I. (2015). A hybrid Wi-Fi P2P with bluetooth low energy for optimizing smart device's communication property. Peer-to-Peer Networking and Applications, 8(4): 567-577. https://doi.org/10.1007/s12083-014-0276-0

[8] Rabiah, A.B., Ramakrishnan, K.K., Liri, E., Kar, K. (2018). A lightweight authentication and key exchange protocol for IoT. In Workshop on Decentralized IoT Security and Standards San Diego, CA, USA, 2018: 1-6. https://doi.org/10.14722/diss.2018.23004

[9] Jain, A., Joshi, A.M. (2019). Device authentication in IoT using reconfigurable PUF. In 2019 2nd IEEE Middle East and North Africa Communications Conference (MENACOMM), Manama, Bahrain, pp. 1-4. https://doi.org/10.1109/MENACOMM46666.2019.8988545

[10] Kalpana, P., Almusawi, M., Chanti, Y., Kumar, V.S., Rao, M.V. (2024). A deep reinforcement learning-based task offloading framework for edge-cloud computing. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, pp. 1-5. https://doi.org/10.1109/ICICACS60521.2024.10498232

[11] Ban, H.J., Choi, J., Kang, N. (2016). Fine-grained support of security services for resource constrained Internet of Things. International Journal of Distributed Sensor Networks, 12(5): 7824686. https://doi.org/10.1155/2016/7824686

[12] Khan, S., Ebrahim, M., Khan, K.A. (2015). Performance evaluation of secure force symmetric key algorithm. In Proceedings of International Multi-Topic Conference (IMTIC).

[13] Li, S., Tryfonas, T., Li, H. (2016). The Internet of Things: A security point of view. Internet Research, 26(2): 337-359. https://doi.org/10.1108/IntR-07-2014-0173

[14] Aruna, E., Sahayadhas, A., Kalpana, P., Khan, S.B., Quasim, T., Almusharrf, A., Asiri, F. (2025). A web 3.0 integrated blockchain enabled access system augmented by meta-heuristic cognitive learning framework for mitigating threats in IoT enabled consumer electronic devices. IEEE Transactions on Consumer Electronics, 71, (1): 1201-1210. https://doi.org/10.1109/TCE.2025.3553741

[15] Kalpana, P., Tappari, S., Smitha, L., Madhavi, D., Naresh, K., Vijayalakshmi, M. (2025). A novel end-to-end privacy preserving deep Aquila feed forward networks on healthcare 4.0 environment. Discover Internet of Things, 5(1): 65. https://doi.org/10.1007/s43926-025-00157-x

[16] Kalpana, P., Narayana, P., Smitha, L., Madhavi, D., Keerthi, K., Smerat, A., Nazzal, M.A. (2025). Health-fots-a latency aware fog based iot environment and efficient monitoring of body's vital parameters in Smart Health Care Environment. Journal of Intelligent Systems & Internet of Things, 15(1): 144-156. https://doi.org/10.54216/JISIoT.150112

[17] Xie, F., Chen, H. (2016). An efficient and robust data integrity verification algorithm based on context sensitive. International Journal of Security and Its Applications, 10(4): 33-40.

[18] Wang, H., Meng, J., Du, X., Cao, T., Xie, Y. (2022). Lightweight and anonymous mutual authentication protocol for edge IoT nodes with physical unclonable function. Security and Communication Networks, 2022(1): 1203691. https://doi.org/10.1155/2022/1203691

[19] Shi, W., Gong, P. (2013). A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. International Journal of Distributed Sensor Networks, 9(4): 730831. https://doi.org/10.1155/2013/730831

[20] He, D., Kumar, N., Chen, J., Lee, C.C., Chilamkurti, N., Yeo, S.S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 21(1): 49-60. https://doi.org/10.1007/s00530-013-0346-9

[21] Yu, S., Lee, J., Lee, K., Park, K., Park, Y. (2018). Secure authentication protocol for wireless sensor networks in vehicular communications. Sensors, 18(10): 3191. https://doi.org/10.3390/s18103191

[22] Fan, K., Luo, Q., Zhang, K., Yang, Y. (2020). Cloud-based lightweight secure RFID mutual authentication protocol in IoT. Information Sciences, 527: 329-340. https://doi.org/10.1016/j.ins.2019.08.006

[23] Adeli, M., Bagheri, N., Sadeghi, S., Kumari, S. (2023). χ perbp: A cloud-based lightweight mutual authentication protocol. Peer-to-Peer Networking and Applications,

16(4): 1785-1802. https://doi.org/10.1007/s12083-023-01467-z

[24] Diwan, T.D., Choubey, S., Hota, H.S. (2022). A lightweight lot application security system to ensure secure authentication, integrity and secure session among Iot devices. Journal of Positive School Psychology, 6(5): 3007-3019.

[25] Ben Amor, A., Jebri, S., Abid, M., Meddeb, A. (2022). A secure lightweight mutual authentication scheme in Social Industrial Iot Environment. Preprint (Version 1) Research Square. https://doi.org/10.21203/rs.3.rs-1669550/v1

[26] Gagana, M.C., Chandana, K.J., Divyashree, N., Affan, M., Kumar, V.R., Kayarga, T. (2021). Secure authentication and security system for IoT environment. International Journal of Engineering Research & Technology (IJERT), 10(7): 131-135.

[27] Oliver, S.G., Purusothaman, T. (2022). Lightweight and secure mutual authentication scheme for IoT devices using CoAP protocol. Computer Systems Science & Engineering, 41(2). https://doi.org/10.32604/csse.2022.020888

[28] Chen, C.M., Liu, S. (2021). Improved secure and lightweight authentication scheme for next-generation IoT Infrastructure. Security and Communication Networks, 2021(1): 6537678. https://doi.org/10.1155/2021/6537678

[29] Zargar, S., Shahidinejad, A., Ghobaei-Arani, M. (2021). A lightweight authentication protocol for IoT-based cloud environment. International Journal of Communication Systems, 34(11): e4849. https://doi.org/10.1002/dac.4849

[30] Kalpana, P., Kodati, S., Smitha, L., Sreekanth, N., Smerat, A., Ahmad, M.A. (2025). Explainable AI-Driven gait analysis using Wearable Internet of Things (wiot) and human activity recognition. Journal of Intelligent Systems & Internet of Things, 15(2): 55-75. https://doi.org/10.54216/JISIoT.150205

[31] Son, S., Park, Y., Park, Y. (2021). A secure, lightweight, and anonymous user authentication protocol for IoT environments. Sustainability, 13(16): 9241. https://doi.org/10.3390/su13169241

[32] Sivaselvan, N., Bhat, K.V., Rajarajan, M., Das, A.K., Rodrigues, J.J. (2023). SUACC-IoT: Secure unified authentication and access control system based on capability for IoT. Cluster Computing, 26(4): 2409-2428. https://doi.org/10.1007/s10586-022-03733-w

[33] National Institute of Standards and Technology (NIST). (2010). NIST special publication 800-22 Rev. 1a: A statistical test suite for random and pseudorandom number generators for cryptographic applications. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf.