International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/21 Volume 11, Issue 3, May – June (2024)

RESEARCH ARTICLE

Broken-Stick Regressive Lightweight Speck Cryptographic Constrained Application Protocol for Data Security in IoT Aware Smart Home

Subhashini R
Department of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India.
✉ subhashini050@gmail.com

Jyothi D G
Department of Artificial Intelligence and Machine Learning, Bangalore Institute of Technology, Bangalore, Karnataka, India.
jyothi.bitcse@gmail.com

Received: 24 February 2024 / Revised: 06 June 2024 / Accepted: 20 June 2024 / Published: 30 June 2024

Abstract – A smart environment aims to enhance the quality of human life by improving simplicity and efficiency. IoT tools are general in nowadays computer networks. The IoT paradigm has recently evolved into a technology for creating smart environments. However, during this transmission, IoT devices are susceptible to cyber-attacks. Therefore, security as well as privacy is main concerns at real-world smart home environment applications. The major aim of manuscript is to propose Broken-Stick Regressive Lightweight Speck Ephemeral Cryptography-based Constrained Application Protocol (BRLSC-CoAP) for enhancing data security with minimal computational cost. First, the smart devices (i.e. IoT) deployed in homes to gather huge number of real-time information as well as broadcast it into authentic user. In order to improve data transmission with higher security, the proposed BRLSC-CoAP technique includes registration, encryption, authentication, and decryption. During the registration process, clients provide their information to server, and after that generates congruential ephemeral symmetric key. The encryption process employs the lightweight speck ephemeral cryptography algorithm to encrypt data with the help of a congruential ephemeral symmetric key. This algorithm is a lightweight symmetric key encryption designed to enhance the CoAP protocol in smart home applications. When the client accesses the data, authentication is performed before decryption. Forbes indexive Broken-stick regression is employed for user authentication. Normal clients access the data using the congruential ephemeral symmetric key, ensuring secure data communication with higher data confidentiality in the smart home. An experimental assessment of BRLSC-CoAP compared through conventional works and evaluated with respect to authentication accuracy, precision, confidentiality rate and computation cost. Also two comparison charts of lightweightness in terms of delay and overhead are measured to validate the entire process. The results indicate that the performance of BRLSC-CoAP increases 5% accuracy, 5% precision and higher 5% confidentiality rate with minimum 10% computation cost, 30% delay and 29% overhead than the conventional methods.

Index Terms – IoT, Smart Home, Constrained Application Protocol (CoAP), Data Security, Lightweight Speck Ephemeral Cryptography, Authentication, Forbes Indexive Broken-Stick Regression.

1. INTRODUCTION

IoT is recognized as disruptive mechanism through an enormous effect on daily lives. Several extensively employed smart homes and so on. IoT tools are associated with Internet to gather as well as swap information. Through the advancement in communication technologies, smart homes represent a promising paradigm of the IoT, wherein smart tools namely smart screens and so on are remotely controlled from any location at any time. In smart home environments, users have the benefit of novel elegant functionalities as well as elevated stage of services aimed at improving the quality of life.

Various conventional techniques, namely lightweight encryption, cryptography methods, lightweight mutual authentication were utilized for data transmission on IoT tools, raising numerous safety threats and effectiveness problems in scheme. However, attacker was entrée information among tool as well as user communication. However, gathered information from these smart tools becomes vulnerable to compromise when malicious attackers gain access to receptive data about legitimate users, containing their everyday behavior for illegal purposes.

At the application layer, CoAP is primarily employed for safe communication among constrained smart IoT tools and servers. However, several limitations regarding the session key generation, multi-cast data multi-cast data communication are presented in CoAP. To enhance the performance of the

RESEARCH ARTICLE

CoAP protocol, there is a need for the development of lightweight cryptography techniques adapted for IoT communication.

LMAS-SHS was developed [1] to facilitate secure transmission between participants using ECC. The designed scheme prioritized lightweight attributes, aiming for minimal computation and communication costs. However, it failed to perform the automatic corroboration of internet safety protocols for authentication, thus limiting its ability to enhance data confidentiality. Robust two-factor user authentication system was introduced in [2] for smart home applications. The scheme demonstrated reliable performance, addressing storage, communication, and computation costs. However, it did not highlight more accurate attack detection to ensure security.

An authentication framework was developed in [3] for smart home systems (SHSs) to enable legitimate users for data communication. However, it failed to improve the authentication rates. Secure as well as lightweight three-factor authentication method was introduced [4] for IoT-enabled smart home, aiming to enhance security. However, issue of accurately detecting the attacks remained unsolved.

ECC-based CoAP was developed in [5]. However, the model failed to include machine learning-based authentication to achieve a higher confidentiality rate. A secure user authentication system was developed in [6] utilizing physical unclonable functions (PUF) to enhance security and mutual authentication. However, it failed to present suitable authentication system suitable for IoT-aware smart home surroundings.

A malware detection and prevention method was developed in [7] utilizing deep learning and an enhanced ECC algorithm for safe data broadcast. It achieved higher accuracy in malware detection with increased precision. However, a significant challenge is the higher computation cost associated with data transmission. A lightweight authentication scheme was implemented in [8] to mitigate potential attacks from the home network and controller device. However, the employed authentication technology proved ineffective in significantly enhancing security.

A smart card-based secure authentication system was developed in [9] to safeguard elegant home IoT network. However, it faced challenges in minimizing the overhead within the secure authentication system. A gateway-based two-factor authentication scheme was developed in [10] to improve safety of IoT device organization. However, it proved inefficient in searching more safe as well as effective framework for IoT organization.

A novel BRLSC-CoAP is introduced to overcome the issues identified from the existing with the following novel contributions.

- A BRLSC-CoAP has designed to enhance safety of data communication. This is achieved through the integration of Broken-Stick Regression and Lightweight Speck Ephemeral Cryptography.
- To enhance the accuracy of attack detection, BRLSC-CoAP utilizes the Forbes Indexive Broken-Stick Regression to analyze client details and distinguish between normal and anomalous behavior. This approach improves the true positive rate in attack detection while minimizing the false positive rate, thereby enhancing overall precision.
- To improve data confidentiality, Lightweight Speck Ephemeral Cryptography performs data encryption and decryption using a congruential ephemeral symmetric key and it allows only authorized client access to the data samples.
- To provide a comparison chart in terms of two lightweights parameters, delay and overhead.
- Lastly, inclusive experiment assessments performed to compute results of BRLSC-CoAP and other techniques with different parameters.

1.1. Structure of the Manuscript

Manuscript is structured as follows: Section 1 explains introduction of IoT and smart homes and its contribution. Section 2 gives in detail review of conventional literature and comparison of different works. It summarize by recognizing methodological gaps as well as highlighting need for proposed method. Section 3 offers concise explanation of BRLSC-CoAP. Section 4 explains experimental setup, database details, performance metrics and statistical test of BRLSC-CoAP and conventional techniques are compared using various parameters. Section 5 presents discussion and Section 6 summarizes the manuscript.

2. LITERATURE REVIEW

A provably secure authentication method was introduced in [11] for the smart home environment to effectively prevent insider attacks. Real or Random model was employed to confirm the safety. It reduces storage cost. However, smart home authentication schemes proved inefficient in performing authentication when a large number of people were present.

A security system was designed in [12]. It comprises a getaway board, node, and APP modules. Multi-tiered ANN Model was developed in [13] for detecting security attacks with high accuracy. Optimal hyperparameter selection was employed to minimize overhead. However, the model was related to a high computational cost.

A threshold and password-based mutual authentication protocol were developed in [14] for a smart home environment, with reduced computation and communication

RESEARCH ARTICLE

costs. A secret sharing algorithm as well as a bilinear map was espoused to offer resistance beside offline assaults. An On-the-fly model checker was employed to execute verification. However, mutual authentication was not achieved.

A lightweight authentication protocol based on symmetric keys was designed in [15] to minimize computation time. User, controller, smart tools, and data authentication were offered by using key establishment and authentication. However, the authentication process did not achieve higher accuracy.

An anonymous lightweight authentication approach was introduced in [16] for SDN-enabled smart homes to enhance security. BAN logic was utilized to examine safety characteristics. However, computational cost was higher. A Privacy-Preserving approach was introduced in [17], utilizing blockchain technology for smart homes to enhance confidentiality and integrity. The authentication scheme was integrated with attribute-based access control. However, it failed to conduct a comprehensive analysis to achieve enhanced solitude protection with no mislaying accuracy.

An enhanced scheme utilizing symmetric key functions was introduced in [18] with higher authentication efficiency. However, it incurs slightly higher computation and communication costs. A consortium blockchain and lightweight authentication scheme were designed in [19]. Enhanced pairing-free certificateless aggregated signature scheme was introduced to guarantee security. However, it failed to consider effective message authentication systems.

A modified honey encryption model was developed in [20], which utilizes Elliptic Curve Cryptography (ECC) for implementing access control in smart home communications. User and device data were preserved with Modified Honey Encryption for creating keys with ECC scheme Encryption and decryption times were lower.

Secure as well as lightweight security protocol was introduced [21] to improve confidentiality. However, it failed to reduce the delay. Smart home authentication as well as access control method was utilized in [22] for enhancing the accuracy. Capability-based access control scheme was utilized for performing authentication. Three-Factor Mutual Authentication Protocol was designed in [23] with higher security. It was combined with PUF and ECC.

Lightweight authentication and encryption mechanisms were employed in [24] with less resource consumption with Transport Layer Security (TLS) authentication algorithm. But, the computation cost was not minimized. Lightweight and efficient authentication framework named ESCI-AKA was developed in [25] for achieving secure communication. Random oracle model was utilized to increase the integrity. But, the confidentiality was not enhanced.

Proposed method is compared through recent conventional work, summary table is presented in Table 1. Most of the work was utilized to discover attacks for higher computational cost and time. Compared to existing methods, BRLSC-CoAP method achieved high accuracy for attack detection with lesser computational cost. The novelty of congruential ephemeral symmetric key is created for every registered client. Data encryption and decryption were performed by using a lightweight Speck ephemeral cryptography algorithm. The client was discovered as normal or an attack with the novelty of Forbes indexing broken-stick regression for improving confidentiality. The summary is shown in Table 1.

Table 1 Comparison of Proposed and Related Works

Method	Contribution	Merits	Demerits
LMAS-SHS [1]	LMAS-SHS introduced for secure transmission	Computation cost was reduced	data confidentiality was not increased
Robust two-factor user authentication scheme [2]	Robust two-factor user authentication scheme was developed in smart home	Storage cost was decreased	Precise attack detection was not obtained
Authentication framework [3]	An authentication framework was examined to secure data transmission	Computational complexity was minimized	Authentication rate was not measured
Secure and lightweight three-factor authentication	Secure and lightweight three-factor authentication	Security was increased	Failed to correctly finding attacks

RESEARCH ARTICLE

method [4]	method was designed for IoT-enabled smart home		
ECC-based CoAP [5]	ECC-based CoAP was discussed for authentication	Secure communication was obtained	ML-based authentication method was not considered
Secure user authentication system [6]	Secure user authentication system was introduced with higher security and mutual authentication	Storage cost was not decreased	Appropriate authentication scheme not concentrated
Malware detection and prevention method [7]	Malware detection and prevention method was investigated for secure data transmission.	Accuracy was improved	Computation cost was not minimized
Lightweight authentication scheme [8]	Lightweight authentication scheme was performed for finding attacks	Delay was minimized	Security was not achieved
Smart card-based secure authentication system [9]	Smart card-based secure authentication system was to discover different attacks	Security was attained	Overhead was not decreased
Gateway-based two-factor authentication scheme [10]	Gateway-based two-factor authentication scheme was introduced for user authentication	Authentication efficiency was higher	Secure communication was not sufficient
Proposed BRLSC-CoAP method	BRLSC-CoAP method is introduced for secure data transmission to find attacks	Computational cost was lesser	Different dataset was not considered

2.1. Require of Proposed Method

Proposed method is necessary to mention censorious demands in IoT-aware smart home, aiming to enhance accuracy and lesser computation cost. The congruential ephemeral symmetric key is created for each registered client with minimum delay. A lightweight Speck ephemeral cryptography algorithm is utilized for executing data encryption and decryption. Forbes indexive broken-stick regression is for examining clients as normal or attack with higher confidentiality. The proposed model is to increase overall performance of attack detection for IoT enabled smart homes.

3. PROPOSED METHODOLOGY

Computer networks at present inherit devices generally known as IoT tools are typify as objects which linked to internet. These devices are present in smart homes and so on. But, networks of IoT tools are prone to cybersecurity

RESEARCH ARTICLE

attacks. This section describes the process of designing and implementing the proposed BRLSC-CoAP in smart home applications. CoAP is a specialized web transfer protocol designed for secure, lightweight, and scalable communication among constraint smart IoT tools and servers. Security is a crucial aspect, especially in IoT smart home environments where devices handle sensitive information. The Broken-Stick Regressive Lightweight Speck Ephemeral Cryptography-based CoAP ensures that only authorized devices access and interacts with the smart home network. The designed BRLSC-CoAP also achieves better versatility, meaning the designed protocol has the ability to adopt different functions such as key generation, encryption, authentication, and decryption to enhance the security strength in a smart home environment.

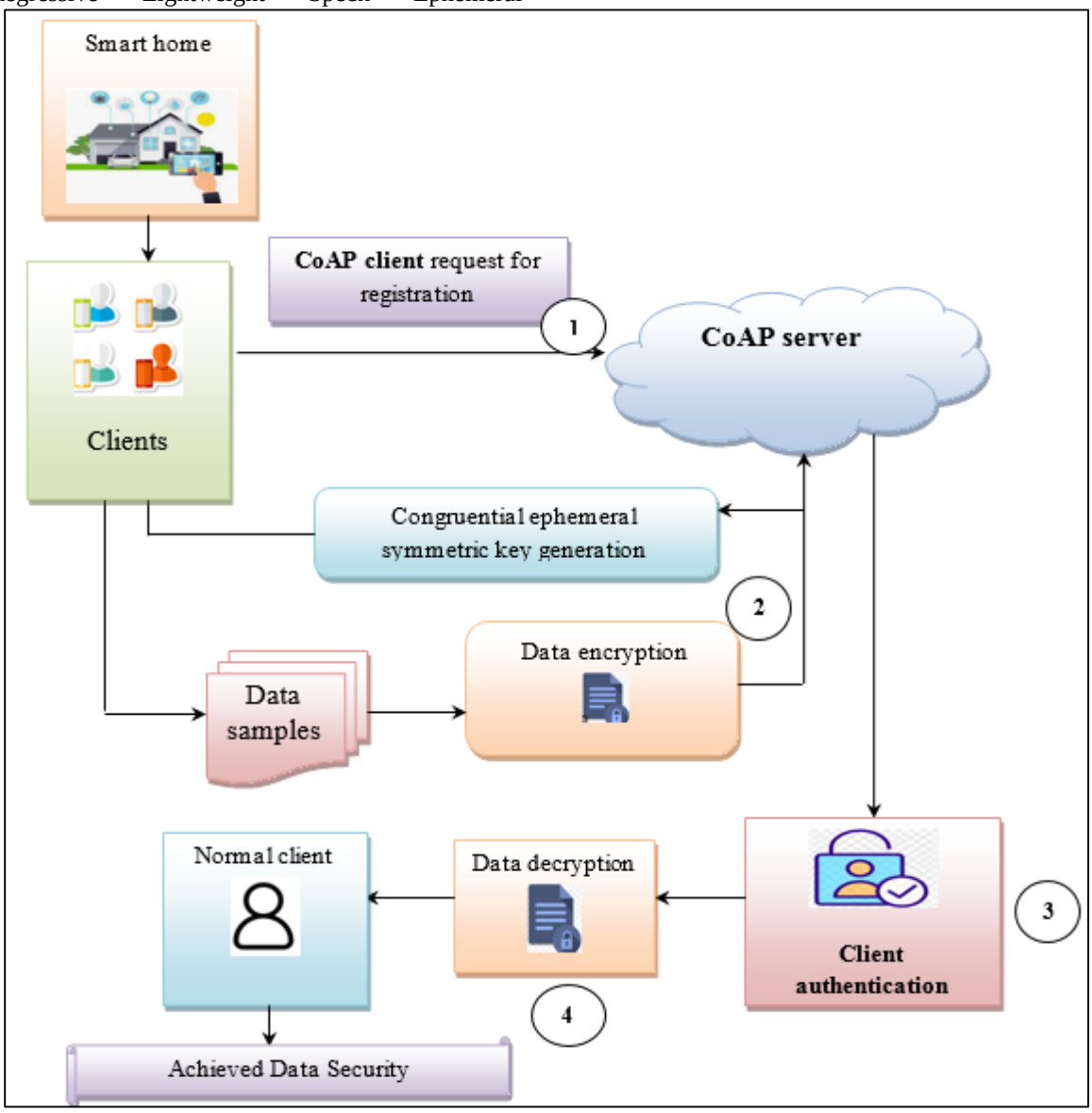

Figure 1 Architecture Diagram of Proposed BRLSC-CoAP

Figure 1 depicts structural design of proposed BRLSC-CoAP for secure data communication at smart home environment.

3.1. System Model

In this model, consists of two entities namely CoAP Client 'CL' and CoAP server 'CS'. IoT devices $D_i = D_1, D_2, D_3, \ldots, D_k$ employ a variety of sensors to monitor different aspects of home environments. This device is used to collect the data such as temperature, humidity, motion, light levels, and etc. After collecting the data, the CoAP Client sends a request 'Rq' to perform the registration into a server 'CS'. Then the server responds 'Rs' and generates the

RESEARCH ARTICLE

Congruential ephemeral symmetric key 'SK' for each registered client. First, 'CL' performs data encryption 'DE' and sends to 'CS'. When client access the data, authentication is performed. If the client is authorized, the server is allowed to decrypt 'DD' the data with 'SK' and obtain the original information. This helps to enhance the security of data transmission.

3.2. Client Registration Phase

The client registration phase refers to a process in which a client device or IoT device registers details to a CoAP server. The client 'CL' initiates the registration process by sending 'Rq' to 'CS'.This request contains information about the details like name, date of birth, mail ID, etc. It is defined by equation (1),

$$CL \overset{Rq}{\Rightarrow} CS \quad (1)$$

Upon receiving the registration request, the server verifies the information provided by the client. This verification process includes checking the client's identity. The server sends a response message 'Rs' to the client, indicating the success or failure of the registration processas given by equation (2).

$$CL \overset{Rs}{\Leftarrow} CS \quad (2)$$

After completing the registration process, the server generates the Congruential ephemeral symmetric key for each successful registration using Lightweight Speck Cryptographic technique.

A congruential ephemeral symmetric key is generated for each registered client. A congruential generator is applied for ephemeral symmetric key generation at the start of any communication session. It is a type of linear generator that generates a key as followed by equation (3),

$$SK = Q_i + e.\ mod\ P \quad (3)$$

In equation (3), SK indicates a congruential ephemeral symmetric key, Q_i denotes initial value, P represent prime number, and multiplier e is ancomponent of elevated multiplicative order modulo P.

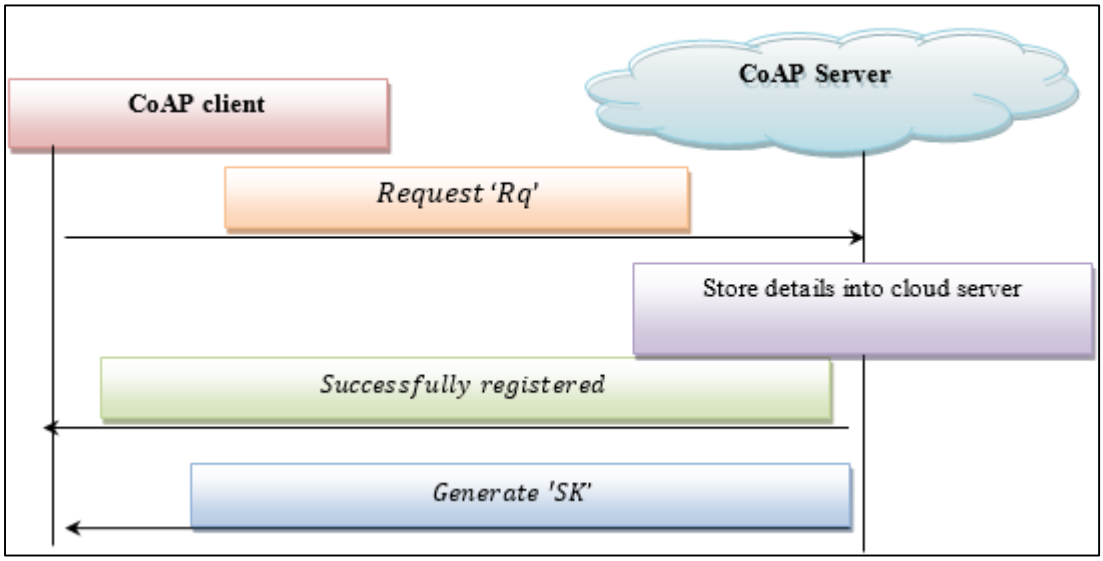

Figure 2 Flow Process of Client Registration Phase

Figure 2 depicts the flow process of the registration as well as key generation in smart home application. At first, CoAP client sent registration request to server. Then server react to request as well as generates the form has to fill out the registration details.

It includes the information about the name, age, date of birth, Mail ID, etc. Then the client enters the details and submits to the server. The server sends the acknowledgement message into a client as 'successfully registered'. Following by, the server generates the symmetric key for safe information communication at smart home environment.

3.3. Encryption

The second process of BRLSC-CoAP technique i encryption for enhancing security by preventing the unauthorized access. Encryption is a procedure of translating information to a cipher text to defend sensitive information as of the unauthorized parties. It acts crucial role at maintaining confidentiality and privacy of sensitive data. Moreover, encryption is performed at the sender's side or CoAP client side. The proposed BRLSC-CoAP utilizes the Lightweight Speck Ephemeral Cryptographic technique. Speck is block lightweight encryption method. It is greatest lightweight

RESEARCH ARTICLE

cipher benchmarks. It is a symmetric key encryption which means similar key is employed for encryption as well as decryption of the data. In this process, secret keys are securely shared between the communicating parties. The encryption was based on the block and key sizes. The speck is introduced to offer excellent performance in both hardware and software.

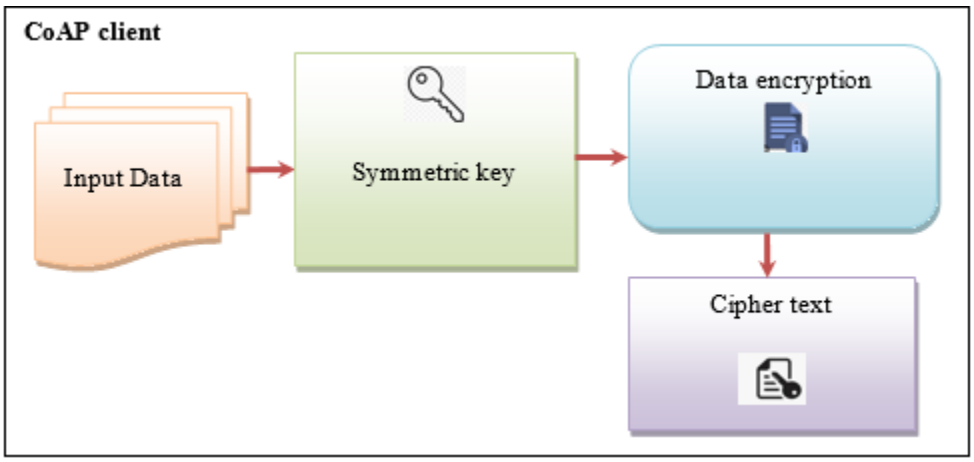

Figure 3 Block Diagram of the Encryption

Figure 3 depicts block diagram of encryption to convert input information to cipher text. Let us assume number of data is $DT_1, DT_2, DT_3, \ldots DT_n$. First CoAP client performs data encryption with the help of a congruential ephemeral symmetric key. The Lightweight Speck Ephemeral encryption algorithm involves the use of three operations such as bitwise XOR ($\oplus$), addition, and S_a and S_{-b} .

Figure 4 illustrates the process of lightweight Speck ephemeral encryption algorithm to generate the cipher text 'C_l' and 'C_r' respectively. Each of which is characterized by its block size $2n$ and symmetric key size mn. Here the SPECK32/64 block cipher is used and it refers to block size 32 bits as well as key size 64 bits.

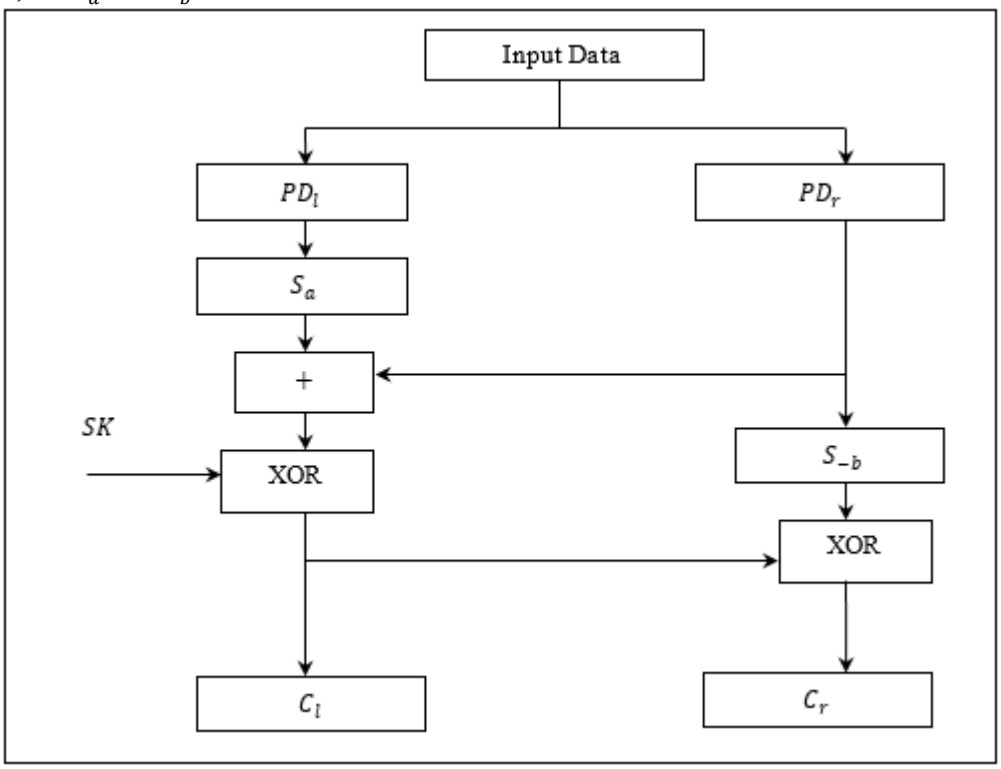

Figure 4 Encryption Process of Lightweight Speck Ephemeral Algorithm

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/21 Volume 11, Issue 3, May – June (2024)

RESEARCH ARTICLE

First, the input plaintext or data is divided into two halves bit data namely Left (l) and Right (r) and defined by equation (4),

$$PD \rightarrow \ PD_l \,||PD_r \qquad (4)$$

In equation (4), PD denotes aninput plaintext or bits of data, PD_l consists of MSB of bits, PD_r consists of LSB of bits. The function 'S' has two operations such as S_a and S_{-b} indicates left circular shift and right circular shift respectively where a and b indicate rotation constants. Apply the function S_a on the PD_l as followed by equation (5),

$$Q = \ S_a\ (PD_l) \qquad (5)$$

The resultant output function 'Q' of the previous stage and $PD_r$is applied to aaddition '+' in equation (6),

$$Z = (Q + \ PD_r) \qquad (6)$$

The resultant output function 'Z' of the previous stage is XOR-ed with the corresponding round symmetric key 'SK'as followed by equation (7).

$$C_l = Z \oplus SK \qquad (7)$$

Therefore the cipher text 'C_l' on the left side is obtained by using the above equation (5) (6),

$$C_l = (S_a\ (PD_l) + \ PD_r) \oplus SK \qquad (8)$$

Similarly, the cipher text 'C_r' on the right side is obtained as followed by equation (9),

$$C_r = (S_{-b}\ (PD_r)) \oplus \ C_l \qquad (9)$$

In this way, the cipher texts are obtained and it sends to the CoAP server.

3.4. Forbes Indexive Broken-Stick Regression Based Authentication

When the CoAP client entrée information as of server, authentication is performed at the server side before the decryption. The proposed technique utilizes Forbes indexive Broken-stick regression for user authentication. Authentication confirms the user. User authenticating is extremely vital, as dissimilar kinds of assaults are based on user's privacy. Broken-stick regression is ML method used to measure relationship among a variable with the help of the Forbes index function.

The Forbes index is a similarity measure between the variables. Based on the similarity measure, the regression partitions the clients into different groups such as normal client and anomalous or assaults. Client login to scheme through proper key. The server first verifies its database to see whether the Client has provided a proper key to decrypt the data. The Forbes indexive is employed to confirm authenticity and is given by equation (9).

$$FI = k * \frac{SK_R \cap SK_E}{|SK_R||SK_E|} \qquad (9)$$

Where FI indicates a Forbes index, k denotes the number of keys stored in the server database, SK_R denotes a secret key at the time of registration, SK_E denotes a currently entered key for decryption. $|SK_R|$ and $|SK_E|$ indicates a number of elements present in the keys. The index returns the output from '0' to 1 and it is followed by equation (10).

$$FI \ = \begin{cases} 1, & NC \\ 0, & Attack \end{cases} \qquad (10)$$

In equation (10),FI returns '1' indicates a normal client (NC), and '0' indicates an anomalous or attack. Therefore, server grants information access to normal client to enhance security in smar home environment.

3.5. Decryption

After verifying the authenticity, the server is allowed to provide the data to authorized client. The Lightweight Speck Ephemeral decryption algorithm is employed for obtaining the plain text or original data. Decryption is procedure of converting encrypted information back to original form. It is reverse process of encryption, that done to protect sensitive information and ensure its confidentiality during data transmission.

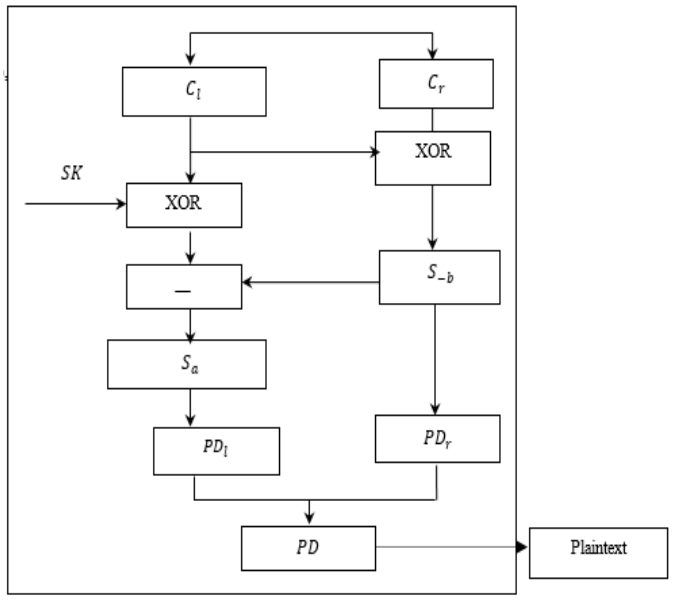

Figure 5 Decryption Process of Lightweight Speck Ephemeral Algorithm

Figure 5 illustrates the process of decryption to attain plaintext. Initial, input cipher text is provided to decryption. Inverse of round function, essential for decryption, uses modular subtraction as an alternative of modular addition as follows:

RESEARCH ARTICLE

Therefore the plain text 'PD_l' on left side is obtained as followed by equation (11),

$$PD_l = S_a\ ((C_l \oplus SK\ ) - \ (S_{-b}\ (C_l\ \oplus C_r\ )) \qquad (11)$$

Similarly, the plain text 'PD_ron the right side is obtained as followed by equation (12),

$$PD_r = S_{-b}\ (C_l\ \oplus C_r\ ) \qquad (12)$$

Finally, the obtained results 'PD_l' and PD_r are combed or concatenated '||' to provide the final original plaintext 'PD'.It is estimated by equation (13),

$$PD\ \leftarrow\ PD_l \parallel PD_r \qquad (13)$$

These aids to improve the safety of data transmission at smart home application therefore it improve the confidentiality rate. The algorithmic process BRLSC-CoAP as follows:

Input: Number of CoAP Client $CL_1, CL_2, CL_3, \ldots . CL_n$, CoAP server '$CS$', Data $PD_i = PD_1, PD_2, \ldots PD_m$

Output: Enhance the security

Begin

\\ Registration phase

1. For each client CL_i
2. CS ask to enter the details
3. CL_i enters their details and submit to 'CS'
4. CS send successfully registered message to CL_i
5. CS generates Symmetric key 'SK'
6. End for

\\ Encryption

7. For each registered client CL_i
8. Perform data encryption
9. Partition data into PD_l and PD_r
10. Encrypt the data using symmetric key using (8) (9)
11. Send Ciphertext 'C_l' and 'C_r' to CS
12. End for

\\ Authentication

13. For each registered client CL_i
14. CS Verifies the authenticity using (9)
15. If ($FI = 1$) then
16. Normal client 'NC'
17. else
18. Anomalous or attack
19. End if
20. End for

\\ Decryption

21. For each normal client NC'
22. CS allows to decrypt the data
23. NC' Obtain the original data using (13)
24. End for

End

Algorithm 1 Broken-Stick Regressive Lightweight Speck Ephemeral Cryptography-Based Constrained Application Protocol (BRLSC-CoAP)

Algorithm 1 outlines the processes designed to enhance the safety of information transmission at smart home environment. Initial phase involves user registration, followed by the congruential ephemeral symmetric keys generated for each registered user. Subsequently, an encryption process is executed to transform the original data into ciphertext, utilizing the congruential ephemeral symmetric key. The resulting ciphertext is then transmitted to the server. When a client wants access to smart home data as of server, server primary confirm client's authenticity using the Forbes index. If the keys get matched, the regression function identifies the client as normal. Otherwise, the regression function identifies the client as anomalous or DoS attack. Finally, the server allows the decryption of data for normal clients, ensuring a higher level of confidentiality rate in data communication.

4. COMPARATIVE PERFORMANCE ANALYSIS

Performance result study of BRLSC-CoAP and LMAS-SHS [1] and Robust two-factor authentication scheme [2] are discussed through dissimilar metrics.

4.1. Experimental Setup

An experimental assessment of BRLSC-CoAP and LMAS-SHS [1] and Robust two-factor authentication scheme [2] has been compared. The experiment is implemented using Python with system specifications Windows 10 OS, 8GB RAM, 1TB Hard disk, and Internet Protocol.

4.2. Dataset Description

To carry out the experiment, the DS2OS traffic traces dataset was utilized, which was collected from https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces. This dataset comprises traces detained in IoT, utilizing IoT sites through light controllers, thermometers and so on. Every site had dissimilar association and diverse number of services. Dataset was created specifically for evaluating anomaly

RESEARCH ARTICLE

detection algorithms. The dataset size is 5 MB. It contains 13 features, 357,952 data samples collected from the main simulation access traces.

Attributes in the dataset include source ID, source Address, destination Address, and destination Type and so on. To conduct the experiment, data ranges of 10,000, 20,000, 30,000... 100,000 are extracted from the dataset.

4.3. Performance Metrics

The dissimilar parameters such as Accuracy, precision, data confidentiality, and computation cost are utilized to measure the experiments by using proposed and existing methods. Also comparison chart of lightweightness parameters in terms of delay and overhead are included. Data samples range of 10,000, 20,000, 30,000... 100,000 are employed for conducting the experiments. Ten iterations are conducted by each parameter for proposed and existing methods.

Accuracy: it is referred number of data samples correctly authenticated as normal or anomalous divided by the total number of data samples. It is expressed in equation (14),

$$A = \left(\sum_{i=1}^{m} \frac{CAD}{PD_i}\right) * 100 \qquad (14)$$

In equation (14), A denotes an accuracy, 'CAD' represents number of data samples properly authenticated as normal or anomalous, PD_i denotes total number of data samples. It is calculated in unit of percentages (%).

Precision: Precision refers to the fraction of authenticated data samples that are correctly identified as either normal or anomalous. It is calculated by equation (15),

$$PRE = \frac{tp}{tp+fp} * 100 \qquad (15)$$

In equation (15), PRE denotes precision, tp indicates a true positive (data samples correctly predicted as normal or anomalous). fp denotes a false positive (data samples incorrectly predicted as normal or anomalous). It is measured in percentage (%).

Confidentiality Rate: It is calculated as ratio of number of data samples only entréethrough authorized users. It is computed as below equation (16),

$$CR = \sum_{i=1}^{m} \frac{PD_{AAC}}{PD_i} * 100 \qquad (16)$$

In equation (16), CR indicates data confidentiality rate, 'PD_{AAC} symbolizes number of data samples accessed by authorized users. It is calculated in percentage (%).

Computation Cost: it is measured as time taken to carry out encryption, authentication and decryption. It is formulated as followed by equation (17),

$$CC = \sum_{i=1}^{m} PD_i * T\,[KG + E + A + D] \qquad (17)$$

In equation (17), CC denotes a computation cost, T denotes a time for key generation 'KG', encryption 'E', authentication 'A' and decryption 'D'.

Finally, lightweightness in our work is arrived on the basis of delay and overhead. Delay and overhead here refers to the time delay involved in secure data transmission whereas overhead refers to the memory consumed in performing secure data transmission. Delay and overhead are estimated by below equations (18) and (19),

$$Delay = Time(Source \rightarrow Destination) \qquad (18)$$

$$Over = Mem(Source \rightarrow Destination) \qquad (19)$$

From the above equations (18) and (19) the end to end delay '$Delay$' and overhead '$Over$' are measured based on time delay involved in secure data transmission between source and destination and the corresponding memory consumed during the process of IoT aware data security in smart home.

Table 2 Comparison of Accuracy

Number of data samples	Accuracy (%)		
	BRLSC-CoAP	LMAS-SHS	Robust two-factor authentication scheme
10000	94.32	91.32	89.33
20000	93.72	90.61	88.27
30000	93.68	89.51	87.07
40000	92.13	88.52	87.13
50000	92.71	88.21	86.20
60000	92.42	89.42	87.61
70000	92.22	89.79	87.50
80000	93.56	90.56	88.82
90000	93.74	91.22	89.17
100000	93.12	90.22	88.65

Table 2 and Figure 6 depict performance outcomes of Ausing three different methods, namely BRLSC-CoAP, LMAS-SHS [1], and the robust two-factor authentication scheme [2]. The x-axis of Figure 6 represents the number of data samples, while the y-axis represents accuracy. The overall A performance is notably higher using BRLSC-CoAP compared to conventional techniques. For assessment, a range of 10,000 to 100,000 data samples were considered. Taking 10,000 data samples for the initial assessment, BRLSC-CoAP achieved an accuracy of 94.32%. In comparison, the accuracy of conventional techniques [1] and [2] was found to be 91.32% and 89.33%, respectively. Similar various results

RESEARCH ARTICLE

were observed for various samples. The overall performance results indicate that the BRLSC-CoAP achieved better accuracy by 4%, and 6% when compared to [1] and [2]. This enhanced accuracy is achievedby the application of the Forbes indexive Broken-stick regression for authentication. The regression function analyzes both the entered congruential ephemeral symmetric key and the key generated during registration. This analysis enables the accurate authentication of data samples as normal or anomalous.

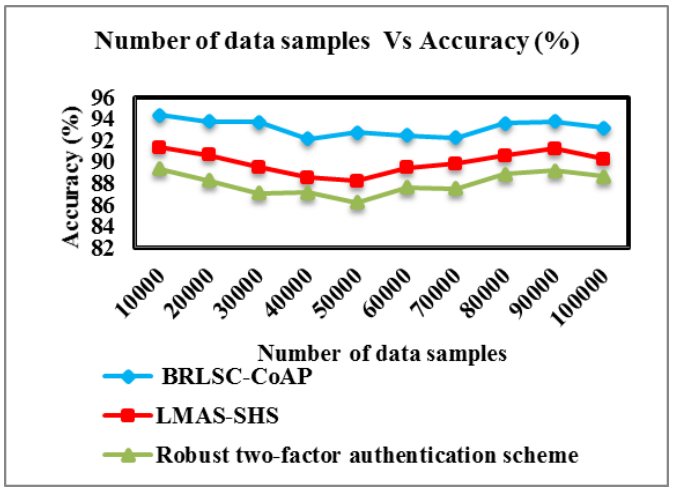

Figure 6 Performance Analysis of Accuracy

Table 3 Comparison of Precision

Number of data samples	Precision (%)		
	BRLSC-CoAP	LMAS-SHS	Robust two-factor authentication scheme
10000	93.75	90.66	88.03
20000	92.33	88.75	87.23
30000	91.42	87.45	86.21
40000	90.45	86.22	85.22
50000	91.57	87.05	84.65
60000	91.02	88.21	85.65
70000	90.89	87.43	86.45
80000	91.84	88.65	86.74
90000	91.22	89.56	87.2
100000	91.65	88.12	86.14

Table 3 and Figure 7 depict the performance outcomes of precision in identifying normal or anomalous data samples across varying sample sizes using three distinct methods namely BRLSC-CoAP, LMAS-SHS [1], and the robust two-factor authentication scheme [2]. The x-axis represents the number of data samples, while precision is observed on the y-axis. Overall, BRLSC-CoAP exhibits higher precision compared to the existing methods. The assessment covers a range of 10,000 to 100,000 data samples. For the initial assessment involving 10,000 data samples, precision was found to be 93.75% using BRLSC-CoAP. In contrast, conventional techniques [1] and [2] were found to be 90.66% and 88.03%, respectively. Similar results were observed across a variety of data samples. The overall performance results indicate that BRLSC-CoAP outperformed [1] and [2] by 4% and 6% in precision, respectively. This superiority is achieved by BRLSC-CoAP for accurate detection of normal or anomalous samples through the symmetric key matching Forbes indexive Broken-stick regression. This capability enhances the true positive rate while minimizing the false positive rate.

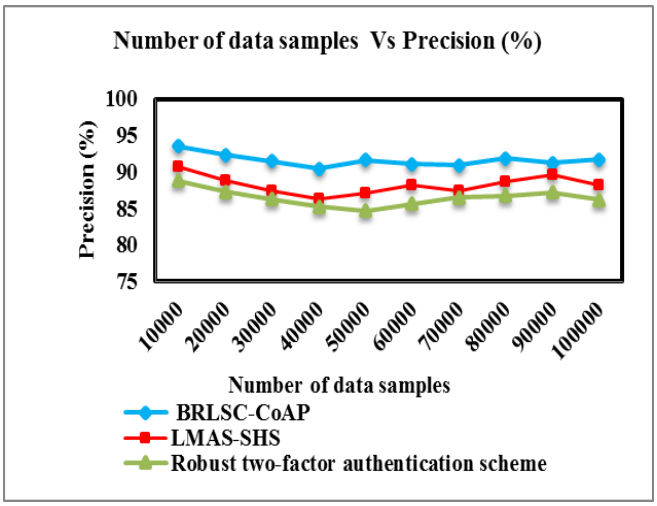

Figure 7 Performance Analysis of Precision

Table 4 Comparison of Data Confidentiality Rate

Number of data samples	Data confidentiality rate (%)		
	BRLSC-CoAP	LMAS-SHS	Robust two-factor authentication scheme
10000	92.15	90.1	88.32
20000	92.83	89.27	87.77
30000	91.51	89.51	87.74
40000	92.13	89.63	86.40
50000	91.64	88.65	86.5
60000	92.72	88.77	86.42

RESEARCH ARTICLE

70000	91.60	89.34	87.50
80000	91.54	88.69	85.94
90000	92.33	89.51	86.94
100000	91.86	88.75	86.59

Table 4 and Figure 8 depict performance analysis of CR versus data samples. For every technique, ten distinct results of CRwere observed and reported in the graph. As depicted in Figure 8, performance outcomes CRusing BRLSC-CoAP are notably higher than the existing methods. For instance, in the first iteration, 10,000data samples were taken for experimentation, and CRusing BRLSC-CoAP was found to be 92.15%. In contrast, applying [1] and [2] resulted in data confidentiality rates of 90.10% and 88.32%, respectively. Different outcomes were observed for each method concerning the number of data samples.

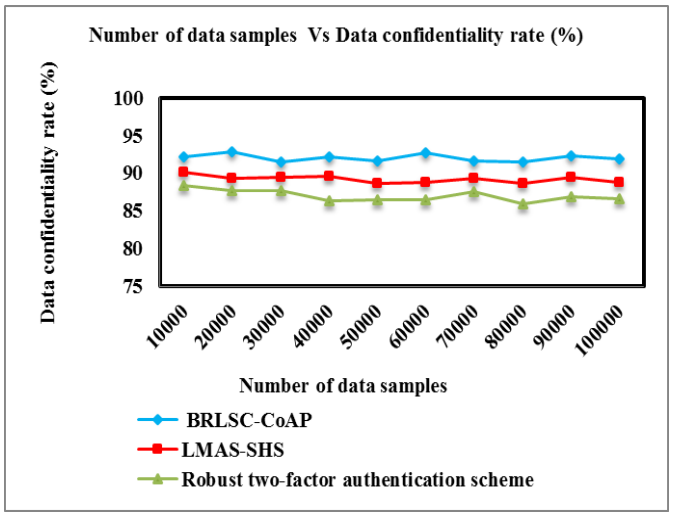

Figure 8 Performance Analysis of Data Confidentially Rate

In conclusion, outcomes of BRLSC-CoAP method were compared to conventional results. Average of these comparison outcomes indicates which analyses of data confidentiality rates were improved by 3% and 6% using [1] and [2], respectively. This is because of the application of the lightweight Speck ephemeral cryptography algorithm. Initially, data encryption is performed with a congruential ephemeral symmetric key, which is then sent to the receiver. Subsequently, authentication is conducted to enable data decryption only for the normal client. This, in turn, enhances the data confidentiality level in the smart home environment.

Table 5 and Figure 9 show performance outcomes of computation cost. In the graph, the y-axis represents computation time, while the x-axis indicates the number of data samples. The figure clearly shows BRLSC-CoAP better than [1] and [2]. As number of data samples enhances, the computation cost also enhances. For instance, when number of data samples is 10,000, the computation time for the BRLSC-CoAP technique was found to be 24 ms, whereas [1] and [2] have computation times of 28 ms and 32.4 ms, respectively. The overall computation time for encryption, authentication, and decryption is reduced by 6% and 14% when using BRLSC-CoAP compared to [1] and [2]. This improvement is due to the application of the lightweight Speck ephemeral cryptography algorithm and Forbes indexive Broken-stick regression. The proposed lightweight cryptography algorithm efficiently handles data encryption and decryption, enhancing safety of data broadcast among source and destination. Forbes indexive Broken-stick regression is employed for accurate client authentication, contributing to improved data confidentiality. This process consumes lesser amount of time thereby minimizing computation costs.

Table 5 Comparison of Computation Cost

Number of data samples	Computation cost (ms)		
	BRLSC-CoAP	LMAS-SHS	Robust two-factor authentication scheme
10000	24	28	32.4
20000	30.4	32	36
30000	33	36	39
40000	37.2	39.2	44
50000	42.5	45	47.5
60000	45	48	52.8
70000	50.4	52.5	56
80000	52.8	55.2	57.6
90000	55.8	58.5	65.7
100000	58.2	62	66

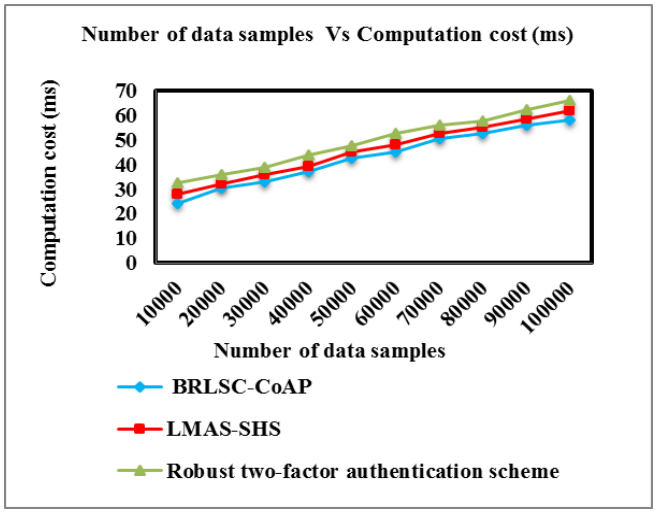

Figure 9 Performance Analysis of Computational Cost

RESEARCH ARTICLE

Table 6 Comparison of Delay

Number of data samples	Delay (ms)		
	BRLSC-CoAP	LMAS-SHS	Robust two-factor authentication scheme
10000	15.25	21.55	33.25
20000	19	25.45	35.55
30000	23.15	29	39
40000	25	31.35	42.15
50000	28	33	45
60000	25.35	30.55	42
70000	22.15	27.25	40
80000	25	29	42.35
90000	28.35	31.55	45
100000	26.15	29.15	40

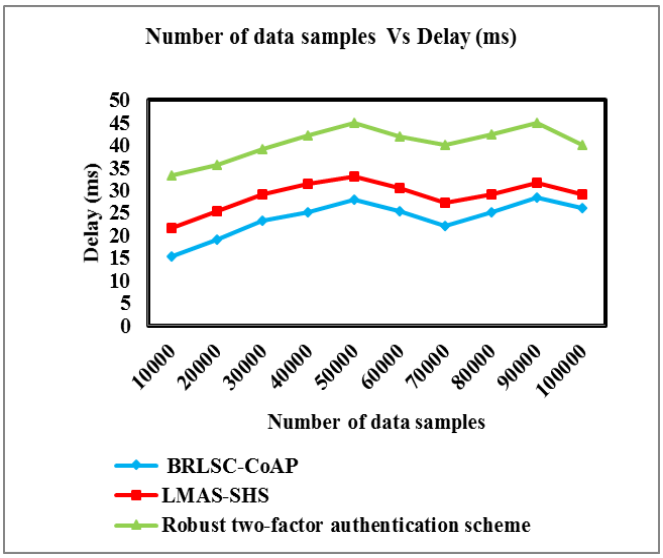

Figure 10 Performance Analysis of Delay

Table 6 and Figure 10 show the lightweightness in terms of delay involved in ensuring data security in IoT-aware smart homes. From the above figure blue color denotes the proposed BRLSC-CoAP method's lightweight in terms of delay, brown color denotes the LMAS-SHS [1] method lightweights in terms of delay and green color denotes the Robust two-factor authentication scheme [2] lightweightness in terms of delay. From the above analysis, it is assumed which delay concerned in ensuring information transmission between users using the BRLSC-CoAP method is said to be reduced upon comparison to [1] and [2]. The reason was due to the application of Lightweight Speck Ephemeral Cryptography that in turn performs data encryption and decryption using a congruential ephemeral symmetric key and permits only authorized client access to the data samples, therefore reducing the delay considerably. The delay employing the BRLSC-CoAP method was found to be minimized by 18% and 42%than the [1],[2] respectively.

Table 7 Comparison of Overhead

Number of data samples	Overhead (KB)		
	BRLSC-CoAP	LMAS-SHS	Robust two-factor authentication scheme
10000	12	17	21
20000	15	19	25
30000	21	25	33
40000	25	30	38
50000	30	35	45
60000	30	35	45
70000	25	30	42
80000	22	28	40
90000	20	25	35
100000	22	28	40

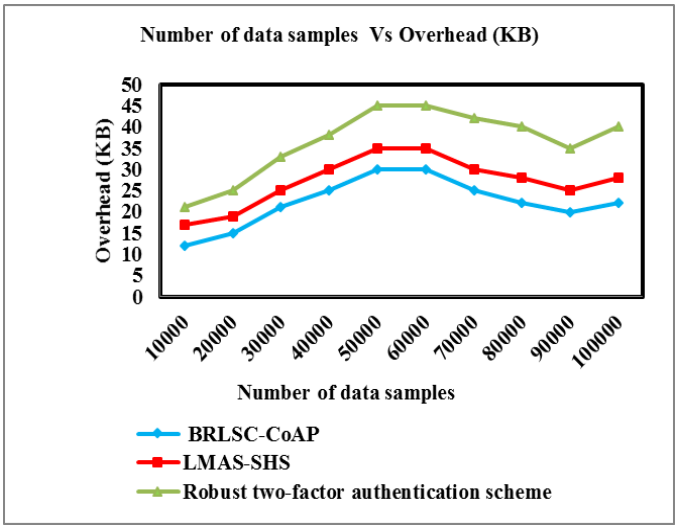

Figure 11 Performance Analysis of Overhead

Finally, the second lightweightness performance metric in terms of overhead is illustrated Table 7 and Figure 11. Neither an increase nor a decreasing trend is observed in terms of

RESEARCH ARTICLE

overhead for increasing samples. This infers that even with the increased data sample size the overhead does not increase therefore corroborating the objective of enhancing the overall precision. Also from the figure it is assumed which overhead observed by BRLSC-CoAP method is relatively lesser than [1] and [2].

The minimum overhead using the BRLSC-CoAP method was due to the Forbes Indexive Broken-Stick Regression that analyzes client details using the Forbes index to verify the authenticity. This in turn reduces the overhead incurred in ensuring data security between users using the BRLSC-CoAP method by 19% and 39% than the [1],[2].

4.4. Two-Way ANOVA Test

It is a statistical test employed to compare mean difference among groups. It is partitioned into two independent variables. Each level of an independent variable is combined to find the mean value of the quantitative subordinate variable.

Table 8 Comparison of Two Way ANOVA Test BRLSC-CoAP, LMAS-SHS [1], and the Robust Two-Factor Authentication Scheme [2]

Two Way ANOVA test			
Parameters	BRLSC-CoAP	LMAS-SHS [1]	Robust two-factor authentication scheme [2]
Accuracy (%)	93.16	89.93	87.97
Precision (%)	91.59	88.21	86.42
Confidentiality rate (%)	92.03	89.22	87.01
Computation cost (ms)	42.93	45.64	49.34
Delay (ms)	23.74	28.78	40.43
Overhead (KB)	22.2	27.2	36.4

Table 8 reveals a comparison of the Two Way Anova test for proposed and existing methods. The output indicates that, at accuracy, precision, computation cost, delay, and overhead 93.16%, 91.59%, 42.93 ms, 23.74 ms, 22.2 KB using proposed BRLSC-CoAP method than the two algorithms such as [1] and [2]. The overall obtained result of the proposed BRLSC-CoAP method offers better performance than other state of art methods.

5. DISCUSSION

Smart home applications acts as vital role in IoT usage. IoT integration is the process of connecting devices with each other by smart home. The security is one of the biggest challenges in smart home. The analysis suggests that the BRLSC-CoAP improves attack detection performance in smart home scenarios. This is accomplished by considering registration, encryption, authentication, and decryption. As a result, attack detection performance and security are enhanced.

Additionally, the Congruential ephemeral symmetric key is used to make the key for registration .Lightweight Speck ephemeral cryptography algorithm is to perform data encryption and decryption. Forbes indexive broken-stick regression is to determine client as normal or attacked. This leads to efficient secure data transmission. The result of BRLSC-CoAP is provided to achieve better performance of higher accuracy by 5%, precision by 5%, confidentiality by 5%, and reduced computation cost by 10%, delay by 30%, and overhead by 29% compared to existing technologies.

6. CONCLUSION

Smart home scheme assures to create the home life uncomplicated as well as contented. But, because of openness of IoT, security and privacy are huge demands of smart home schemes applicability. In this paper, a BRLSC-CoAP technique has been developed for smart home surveillance to address security challenges arising from openness of IoT network. The lightweight Speck ephemeral cryptography algorithm, in conjunction with CoAP, is employed to establish secure transmissions. The Forbes indexive broken-stick regression in the BRLSC-CoAP technique efficiently authenticates data samples, enhancing data confidentiality. The cloud user employs encryption using the linear congruential ephemeral Encryption algorithm to secretly store sensitive data with higher confidentiality. It suggests that the BRLSC-CoAP protocol is versatile and it handle various functions, enhancing security in a smart home environment by incorporating key generation, encryption, authentication, and decryption. A comprehensive experimental evaluation is conducted with different performance metrics concerning number of data samples generated by the IoT device. Also detailed lightweightness performance metrics in terms of delay and overhead are also measured. The entire performance results demonstrate which BRLSC-CoAP technique attains superior 5% accuracy, 5% precision, 5% confidentiality rate, and minimum 10% computation cost, 30% delay, and 29% overhead compared to conventional methods. In future, proposed technique will be further enlarged to consider different factors such as recall and F-measure by using novel cryptography methods for secure data communication in IoT-aware smart homes.

REFERENCES

[1] S.U. Jan, I. A. Abbasi, M. A. Alqarni , “LMAS-SHS: A Lightweight Mutual Authentication Scheme for Smart Home Surveillance”, IEEE Access , vol. 10, 2022, pp. 52791 – 52803. DOI: 10.1109/ACCESS.2022.3174558

RESEARCH ARTICLE

[2] S. Zou, Q. Cao, C. Wang,Z. Huang,G. Xu, "A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT", IEEE Systems Journal ,vol. 16, no. 3, 2022, pp. 4938 – 4949. DOI: 10.1109/JSYST.2021.3127438
[3] N. Amraoui & B. Zouari, "Anomalous behavior detection-based approach for authenticating smart home system users", International Journal of Information Security, Springer, vol. 21, 2022, pp.611–636.https://doi.org/10.1007/s10207-021-00571-6
[4] S. Yu, N. Jho, Y. Park, "Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes", IEEE Access ,vol. 9, 2021, pp. 126186 – 126197. DOI: 10.1109/ACCESS.2021.3111443
[5] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan & M. Dasgupta, "ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things", Wireless Personal Communications, Springer, vol. 116, 2021, pp. 1867–1896. https://doi.org/10.1007/s11277-020-07769-2
[6] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF", IEEE Access, vol.10, 2022, pp. 101330 – 101346. DOI: 10.1109/ACCESS.2022.3208347
[7] 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 Computing, Elsevier, vol. 3, no. 2, 2023, pp. 1-14. https://doi.org/10.1016/j.hcc.2023.100117
[8] V. Kumar, N. Malik, J. Singla, N. Z. Jhanjhi, F. Amsaad and A.Razaque, "Light Weight Authentication Scheme for Smart Home IoT Devices", Cryptography , vol. 6, no.3, 2022, Pages 1-15. https://doi.org/10.3390/cryptography6030037
[9] P. Kumar & L. Chouhan, "A secure authentication scheme for IoT application in smart home", Peer-to-Peer networking and Applications, Springer, Volume 14, 2021, pages 420-438. https://doi.org/10.1007/s12083-020-00973-8
[10] H. Luo , C. Wang , H. Luo, F. Zhang, F. Lin , and G. Xu, "G2F: A Secure User Authentication for Rapid Smart Home IoT Management", IEEE Internet of Things Journal, vol. 8, no.13, 2021, pp. 10884 – 10895. DOI: 10.1109/JIOT.2021.3050710
[11] T-Y. Wu, Q. Meng, Y-C. Chen, S.Kumari and C-M Chen, "Toward a Secure Smart-Home IoT Access Control Scheme Based on Home Registration Approach", Mathematics, vol. 11, no.9, pp. 1-15. https://doi.org/10.3390/math11092123
[12] C. Sisavath and L. Yu, "Design and implementation of security system for smart home based on IOT technology", Procedia Computer Science, Elsevier, vol. 183, 2021, pp. 4-13. https://doi.org/10.1016/j.procs.2021.02.023
[13] S. Sohail, Z. Fan, X. Gu, F. Sabrina, "Multi-tiered Artificial Neural Networks model for intrusion detection in smart homes", Intelligent Systems with Applications, Elsevier, vol. 16, 2022, pp. 1-14. https://doi.org/10.1016/j.iswa.2022.200152
[14] A. Huszti, S. Kovács, N. Oláh, "callable, password-based and threshold authentication for smart homes", International Journal of Information Security, Springer, vol. 21, 2022, pp. 707–723. https://doi.org/10.1007/s10207-022-00578-7
[15] W. Iqbal, H. Abbas, B. Rauf, Y. Abbas, F. Amjad, A. Hemani, "PCSS: Privacy Preserving Communication Scheme for SDN Enabled Smart Homes", IEEE Sensors Journal, vol. 22, no. 18, 2022, pp.17677 – 17690. DOI: 10.1109/JSEN.2021.3087779
[16] S. Yu, A. K. Das, and Y. Park, "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes", IEEE Access, vol. 9, 2021, pp. 49154 - 49159. DOI: 10.1109/ACCESS.2021.3068723
[17] A. Qashlan, P. N. X. He and M. Mohanty, "Privacy-Preserving Mechanism in Smart Home Using Blockchain", IEEE Access, vol. 9, 2021, pp. 103651 – 103669. DOI: 10.1109/ACCESS.2021.3098795
[18] B. A. Alzahrani, A.Barnawi, A. Albarakati, A.Irshad , M. A. Khan , and S. A. Chaudhry, "SKIA-SH: A Symmetric Key-Based Improved Lightweight Authentication Scheme for Smart Homes", Wireless Communications and Mobile Computing, Hindawi, vol.2022, 2022, pp. 1-12. https://doi.org/10.1155/2022/8669941
[19] B. Liu, X. Yao, K. Guo, P. Zhu, "Consortium Blockchain Based Lightweight Message Authentication and Auditing in Smart Home", IEEE Access ,vol. 11, 2023, pp. 68473 – 68485. DOI: 10.1109/ACCESS.2023.3293401
[20] S. Uppuluri and G. Lakshmeeswari, "Secure user authentication and key agreement scheme for IoT device access control based smart home communications", Wireless Networks, Springer, vol. 29, 2023, pp.1333–1354. https://doi.org/10.1007/s11276-022-03197-1
[21] H. E. Makhtoum, Y. Bentaleb, "Secure and Lightweight Authentication Protocol for Smart Metering System", International Journal of Advanced Computer Science and Applications(IJACSA), vol. 13, no. 11, 2022, pp. 1-8. DOI: 10.14569/IJACSA.2022.0131191
[22] X. Zhao, B. Zhong and Z. Cui, "Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes", Electronics, vol. 12, no. 15, 2023, pp. 1-20. https://doi.org/10.3390/electronics12153334
[23] M. Fariss, H. E. Gafif, A.Toumanari, "A Lightweight ECC-based Three-Factor Mutual Authentication and Key Agreement Protocol for WSNs in IoT", International Journal of Advanced Computer Science and Applications (IJACSA),vol. 13, no. 6, 2022, pp. 1-11. DOI: 10.14569/IJACSA.2022.0130660
[24] S. Amanlou, K. A.A.Bakar, "Lightweight Security Mechanism over MQTT Protocol for IoT Devices", International Journal of Advanced Computer Science and Applications (IJACSA),vol. 11, no. 7, 2020, pp.1-6. DOI: 10.14569/IJACSA.2020.0110726
[25] H.Alasmary, and M. Tanveer, "ESCI-AKA: Enabling Secure Communication in an IoT-Enabled Smart Home Environment Using Authenticated Key Agreement Framework", Mathematics, vol.11, no. 16, pp. 1-25. https://doi.org/10.3390/math11163450.

Authors

Ms. Subhashini R is a Research Scholar in the Department of Computer Science and Engineering at Bangalore Institute of Technology, Bangalore, Karnataka. Subhashini is a graduate in Information Science and engineering from Visvesvaraya Technological University, Karnataka and has pursued her Master's M.Tech. in Digital Communication and Networking from Visvesvaraya Technological University, Karnataka. Her research focuses on finding lightweight approach for providing security and preserving data integrity in the Application layer protocol of IoT. Ms. Subhashini has authored and co-authored several papers in peer-reviewed journals. She has presented her work at various national and international conferences. In addition to her research, Subhashini is actively involved in mentoring undergraduate students and has conducted several workshops and delivered expert talk on IoT. She is a member of multi-disciplinary engineering professional society - Institute of Engineers, India.

Dr. D. G. Jyothi is a prominent academic and researcher serving as the Head of the Department of Artificial Intelligence and Machine Learning (AI&ML) at Bangalore Institute of Technology (BIT), Bangalore, Karnataka, India. She has significantly advanced AI and ML through her leadership, research, and dedication to education. Throughout her career at BIT, she has held various academic roles and played a crucial part in developing the AI&ML department by integrating innovative teaching methods and promoting cutting-edge research. Dr. Jyothi's research focuses on artificial intelligence and machine learning applications, with numerous publications in reputed journals and conferences. Her work addresses practical applications,

RESEARCH ARTICLE

solving real-world problems with technological advancements. As the department head, she has demonstrated exceptional leadership in curriculum design, industry collaboration, and fostering a research-oriented culture. Recognized for her academic contributions, she frequently speaks at conferences and has led her department to significant achievements, including successful student placements and groundbreaking research projects.

How to cite this article:

Subhashini R, Jyothi D G, "Broken-Stick Regressive Lightweight Speck Cryptographic Constrained Application Protocol for Data Security in IoT Aware Smart Home", International Journal of Computer Networks and Applications (IJCNA), 11(3), PP: 335-350, 2024, DOI: 10.22247/ijcna/2024/21.