A lightweight security framework for electronic healthcare system

Ravi Raushan Kumar Chaudhary1 · Kakali Chatterjee1

Received: 28 February 2022 / Accepted: 29 June 2022 / Published online: 22 July 2022
© The Author(s), under exclusive licence to Bharati Vidyapeeth’s Institute of Computer Applications and Management 2022

Abstract Electronic healthcare systems (EHS) are the most emerging field of today’s digital world which is used for remote health monitoring, evidence-based treatment, disease prediction, modeling, etc. Many internet of things (IoT) devices and body sensors are involved in such systems for data collection. Every time a cloud-based solution is adopted to collect and preserve collected personal health information. Secure data transmission is a big challenge in such an environment as the devices are memory and power-constrained. This research focuses on a lightweight ciphering mechanism that can be used to secure an electronic healthcare system. Traditional cryptographic solutions are not suitable due to the operational complexity. Some popular lightweight block ciphers which includes SIMON, HEIGHT, LEA, etc. are used in IoT device to increase the speed. Hence, in this paper, we have proposed a lightweight security framework with a flexible key structure to protect the data in the electronic healthcare system. The proposed scheme increases the speed by minimum 4% with compared to existing literature. Our experimental analysis shows that the proposed technique also have a low computational and communicational load. The brief security analysis using automated validation of internet security protocols and applications (AVISPA) tool shows that the proposed scheme can withstand all network attacks.

Keywords Lightweight cryptography · Authentication · Security · IoT based technology

1 Introduction

Today IoT-based healthcare architecture is used in different places like smart cities, smart agriculture, smart health projects etc. Among these projects, one of the essential fields is smart healthcare which has a bigger scope of development in its many intelligent services. These services include user health monitoring, routine health checkup, emergency healthcare, diagnosis etc. It provides easy and fast processing of medical facilities, reducing the time and cost of treatment. Realtime health monitoring can be performed using the internet through a wireless sensor network (WSN) [1]. Wireless body sensor-based healthcare applications are used in the health sector for remote health monitoring. This may reduce huge hospitalization costs also. This type of monitoring system is a part of IoT-based healthcare which can be used for remote health services. IoT-based systems are made up of three layers: perception, network, and application. The perception layer is responsible for data collection from different sources. The network layer is for communication between the perceptions layer and the application layer. The application layer is responsible for different user applications in this scenario. The Internet of Things may connect with diverse devices, and networks in the field of healthcare for different services. There are many security attacks such as Impersonation attack, Replay attacks, Man-in-middle attack etc makes the system vulnerable to remote health monitoring service. Hence security and privacy threats are big challenges in this network. Trusted cryptography, such as a public key or symmetric key cryptography, as well as RSA or ECC-based cryptography, is a common
solution for such challenges. However, problems such as limited processing resources, increased implementation time, and high computational cost were discovered. Some lightweight cryptographic algorithms such as SIMON [2], SPECK [3] and HEIGHT [4] etc are available in this area. The structure of these ciphers depends upon blocksize, keysize, round number and S Box construction. With the help of these techniques, the sensitive data can be securely stored in the medical server so that the user can access the data after authentication. Some works [5–9] have been found which focused on secure framework for remote monitoring in COVID 19 situations. Also some work in elliptic curve cryptography(ECC) based techniques have been found which uses a smaller key size to provide the equivalent security [10]. Another ECC-based public key approach for the generation of the certificate [11] is also found. Major issue in such framework is a complex key generation and encryption process which degrades the device performance. As the devices used in such a network have less memory and power, so the complex algorithm is not suitable in such a scenario. Kumari et al. [12] discussed a biometric-based security framework for authentication in IoT systems. Another certificate-less authentication scheme [13] based on ECC has been found. These frameworks may resist some network attacks but the computational and communication cost increases. Hence to reduce the cost we have used a new lightweight block cipher technique that is suitable for IoT devices. In this framework, the encrypted data will be stored in the server and the user will access the data from the server, after strong authentication.

The major contributions in this paper are as follows:

- The proposed lightweight security framework is constructed based on a three factor based authentication technique to resist different network attacks.
- A new lightweight cipher technique (LWC) is proposed for data security of IoT devices. This technique is used to encrypt data while transfer from sensor node to cloud server.
- The Proposed LWC has flexible key structure to enable adaptive security in IoT devices.
- The proposed framework uses public key encryption algorithm for data protection during data access from cloud.
- The performance comparison shows that the cipher is efficient with high throughput and low computational load.

The rest of the paper is organized as follows: Sect. 2 presents Related Works, Sect. 3 provides Describes the proposed framework Sect. 4 presents Performance of the proposed scheme; Sect. 5 discusses Security Analysis; finally, concluded in Sect. 6.

2 Related works

Several approaches were found to solve the security problems in IoT-based e-healthcare systems. The main focus of IoT based e-healthcare system is to collect health information from different users and shared it among them to provide various healthcare-related services. As different types of users are participating in this system, there must be robust authentication techniques to control users’ access. Alaba et al. [14] proposed Internet of Things security framework which has four types of IoT security taxonomy such as application, architecture, communication and data. Innovative healthcare suffers threats and attacks such as data misuse, loss of data etc. The most commonly used security techniques that are considered with the use cases in this application domain are authentication, authorization exhaustion of resources and trust establishment. Zouka et al. [15] introduced IoT-based E-healthcare using fuzzy logic. In this paper, they proposed healthcare architecture which has basically two parts: Firstly, computer hardware is defined and secondly, artificial neural network technology defines under fuzzy logic. Security framework have three phases registration phase, login phase and authentication phase. Dhananjay et al. [16] introduced IoT-based e-healthcare in wireless body sensor networks where challenges, issues of Wireless Body Area Network (WBAN) are discussed. Pasha et al. [17] introduced framework for E-health system in IoT-Based Environments using CoAP(constraint application protocol) which has a built-in-service mechanism. CoAP is established between IoT devices and IoT gateway in an internet environment. Islam et al. [18] proposed e-healthcare system using processors and sensors. Here the healthcare monitor system has three-stage architecture features such as a sensor- module, data-processing module and web user interface. Tamilsevi et al. [19] introduced health monitor IoT-based e-healthcare using Arduino Uno device. The system can use a temperature sensor, spo2 sensor, heartbeat sensor and eye blink sensor and Arduino Uno as a processing device. Acharya et al. [20] introduced IoT based electronic healthcare monitoring using raspberry pi 3 model B as a health monitoring kit on the internet of Things environment. Here the IoT-based e-healthcare system is used to monitored some parameters of human health like heart rate, body temperature and respiration etc. Li et al. [21] talked about how to secure the bootstrap phase of a wireless body sensor network by using group pairing. A received signal strength-based authentication system has been proposed by Zeng et al. [22]. Lower/physical layer features are discussed in this study as a possible security option. EKG-based key agreement system is proposed by Ali et al. [1]. Key sharing by making the shared key with discrete wavelet transform (DWT), is discussed in [10]. ECC-based cryptography was used to create the IoT-based EHS. A certificate handshake has been proposed between sensors and end-users in this concept. All discussed works are summarized in Table 1. In all the above-discussed authentication schemes, authentication is mainly performed...
3 Proposed framework

In this section the proposed framework is discussed. Before explaining the scheme, encryption technique and the system network model is discussed first (Fig. 1).

3.1 Proposed structure of LWC

The proposed structure of LWC is shown in Fig. 2. The proposed encryption process has the following steps:

1) The First 128 bit of plaintext is divided into four message sub-blocks of 32 bits each.
2) Next, each sub-block is passed through an expansion D Box which will produce 64-bit pro blocks
3) The next two pro blocks B1 and B2 are XORed to get output M12 and M34 which will be XORed with keys K1 and K2 each having 64 bits to produce an intermediate cipher.

A total of 32 rounds are performed to get the highest avalanche effect. The proposed algorithm is shown below

### Algorithm 1 Encryption process in the LWARX

1: procedure Input:(Plaintext PT 128 bit and first round K12(64 bits))
2: OUTPUT: Ciphertext CT 128 bit
3: A = Addrondkey(PT,K₁₂)
4: B = Addrondkey(PT,K₁₂)
5: for x from 16 to 128 do
6: T = \( S_{b_0}(x) \)
7: B=XOR(T)
8: A₁ = Addrondkey(B.K₁₂)
9: B₁ = Addrondkey(B,K₃₄)
10: for
11: return ciphertext CT=X

3.2 Key update in the LWC

For key update, following steps are followed:

- \( K_{i+1}[128 : 123] = S_b(K'[128 : 123]) \)
- \( K_{i+1}[122 : 85][K_j[41 : 0] = S_b(K'[122 : 85][K_j[41 : 0]) \)
- \( K_{i+1}[81 : 42] = S_b(K'[81 : 42]) \oplus RC \)
- \( K_{i+1}[256 : 225] = S_b(K'[128 : 123]) \)
- \( K_{i+1}[224 : 193] = S_b(K'[122 : 85]) \)
- \( K_{i+1}[224 : 193][K_j[66 : 60] = S_b(K'[81 : 42]) \)
- \( K_{i+1}[88 : 82] = S_b(K'[88 : 82]) \)

The proposed structure of the lightweight block cipher supports key sizes 128 bit to 256 bit key sizes. The flexible key structure is shown in Fig. 2. In the starting point, start signal will be ‘1’ and 128 bit plaintext applied in the Cryptosystem. The round function is operated with key schedule. The control signal is used to set the key. Key can be 128 bit or 256 bit accordingly control signal will set the circuit. If the control signal is used to set the key. Key can be 128 bit or 256 bit with high computational loads.

Some of the schemes are based on asymmetric techniques, which are more robust than symmetric schemes with high computational loads.

To solve the above problems, we have proposed a lightweight cryptographic scheme (LWC), which is mainly based on S Boxes to produce the required confusion and diffusion in the cipher. Proposed LWC has a flexible key structure (128 bit to 256 bit). Due to this changing key structure, proposed LWC can have adaptable implementations to enable adaptive security in IoT devices.
Table 1: Related works with advantages and disadvantages

| S.no | References       | Year | Description                                                                 | Advantages                                                                 | Disadvantages                                                                 |
|------|------------------|------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 1    | Xue et al. [23]  | 2012 | This paper discussed key management in authentication protocol for E-healthcare system | Introduced WSN key management using temporal credential and mutual authentication among the nodes | Communication cost is very high                                            |
| 2    | Turkanovic et al. [24] | 2014 | Introduced user authentication for heterogeneous ad hoc WSN.                 | An user can have a session key with the desired sensor node                 | Key storage can easily compromised                                          |
| 3    | Das et al. [25]  | 2015 | Authentication scheme using smart card                                       | Supports the easy password change and efficient authentication.              | Many network attacks can be performed                                        |
| 4    | He et al. [26]   | 2015 | Introduced IoT based e-healthcare using RFID authentication scheme           | ECC based Radio Frequency design(RFID) authentication scheme using health function operation | It increases power consumption and cost gate area                            |
| 5    | Yeh et al. [27]  | 2016 | Internet of things based healthcare systems with a body sensor network       | Body Sensor Network (BSN) communicates with double authentication using the IoT environment | Cost increases due to double authentication                                  |
| 6    | Alaba et al. [14] | 2017 | A survey has been performed with IoT security                               | The taxonomy of the current security threats in contexts of application, architecture is presented | Only explore the threats, provide no security solution                      |
| 7    | Elhoseny et al. [28] | 2018 | This model use steganography technique with hybrid encryption scheme         | Hide the confidential userdata into a transmitted cover image                | Introduce more complexity                                                   |
| 8    | Moosavi et al. [29] | 2018 | A state of art service having used the data communication process in IoT-EHS | Present dtls scheme                                                         | Limited resources                                                            |
| 9    | Banerjee et al. [30] | 2018 | A biometric-based smart card authentication scheme using the perfect id in multiserver environment | Seven major attacks can be resisted by the authentication scheme            | Communication cost is high                                                  |
| 10   | Dhanvijay et al. [16] | 2020 | Present a detailed analysis of recent state-of-the-art IoT healthcare methods with objectives, metrics and classification, strength | Explain IoT based e-healthcare Service, application, technology, changellage | Challenges are provided. But existing solutions are not discussed           |
| 11   | Islam et al. [18] | 2020 | Smart healthcare monitoring system using IoT with different condition        | Real time patient data analysis for different conditions                    | Suffers with data redundancy and network congestion                         |
| 12   | Tamilsevi et al. [19] | 2020 | IoT based healthcare system testing with Arduino uno                         | Measure heart rate, Blood pressure, eye movement and oxygen level using sensors | The test cases are very limited                                              |
| 13   | Archarya et al. [20] | 2020 | IoT- EHS environment with Raspberry Pi, Heart rate sensor, ECG sensor, Raspiration and B.p Sensor | Real time health monitoring                                                 | Increase with high response time                                            |
The logical structure of S Box is shown in Fig. 3 where 8 AND gates and 12 XOR gates are present.

### 3.3 System network model

The proposed encryption technique is applied in IoT environment where each IoT device and user node (mobile node) is registered first. After registration when the user node wants to access the server data, the authentication took place. Here the user node is the mobile device where the data is gathered. In large scale IoT devices implanted in a network for healthcare faces many challenges. One major challenge is authentication of the devices which are accessing the server for patient data. Hence the system network design not only addressed the data confidentiality problem, but also authentication issue is also handled. Figure 4 is mainly addressed the authentication between the user nodes and medical server. In Fig. 4, the user node is the mobile device which is responsible to transfer the data to the medical server. The authentication process is explained below. There are symbols used notation Table 2.

![Proposed LWC technique](image-url)
3.4 User registration phase

In user registration phase, following steps are involved:

- **Step 1:** The patient first generates a digital identity $PID_y$, a biometric identity $BPID_y$, an identity for the mobile device $MID_y$ and a password $PS_p$. Then, he/she generates five random numbers $N_1, N_2, N_3, N_4, N_5$ and computes $PX_1 = h(PID_y \oplus MID_y) || N_1)$ and $PX_2 = h(BPID_y || N_1)$. In addition, the user computes two pseudo-random identities $RPID_y = h(PX_1 || PX_2 || PS_p || N_2)$ and $SPID_y = h(PS_p || N_1 || N_2)$. It also generates

---

Fig. 2 Flexible key structure

Fig. 3 Low cost structure of 32 bit S Box

Springer
the public key where $p$ is the base point zero $P$ of the elliptic curve. After that, he/she sends parameters \{RPID, SPID, PU, N\} via a secure medium to the medical server.

- Step 2: Once receiving the user parameters for registration the server computes $Y_1 = h(SID) || N_1 || K_P$, using its own identity SIDy. Then computes $Y_2 = \text{RPID}_y \oplus Y_1$, its public key $PU_s = K_P \text{and} Y_3 = h(\text{RPID}_y || Y_1 || PU_s || N_3)$. Next, Server, the server generates a random number $\beta$ and select secret key $a$ to be used in the challenge - response protocol. In order to create the first challenge $Ch_1$, the server computes $(Enc(a) \bigoplus N_2 \beta)$. Finally, it sends to the patient the message $\{Y_2 \parallel Y_3 \parallel PU_s \parallel Ch_1\}$ via a reliable channel.

- Step 3: The patient stores the parameters \{N, N_2, N_3, N_4, Y_2, Y_3, Ch_1\} in his/her mobile device and then terminates the registration phases. All messages transferred in this phase is shown in Table 3.

3.5 Login and authentication phase

Once the registration process is successfully completed the user is able to use his/her mobile device to communicate at any time with the medical server. Figure 5 shows all steps of login and authentication phase.

- Step 1: To login, the patient enters his/her identity PIDy, a biometric identity BPID, and a password $PS_p$, while verifying that the current mobile device belongs to the legitimate user, we proceed as follows. First stored randoms $N_1, N_2, N_3$ are retrieved from the memory of the mobile device in order to compute $PX_1 = h(\text{PID}_y \oplus \text{BPID}_y) || N_1$, $PX_2 = h(\text{BPID}_y || N_1)$ and $\text{RPID}_y = h(\text{PID}_y || \text{SPID}_y || \text{PU}_p || N_2 || N_3)$. Further more, the parameters $\{Y_2, Y_3, N_5, PU_s\}$ are also retrieved from the memory to calculate $Y_1^* = Y_2 \oplus \text{RPID}_y$, $PU_s = Y_1^* \cdot P$ and $SPID_y = h(PS_p || N_1 || N_2) \cdot Y_3^* = h(\text{RPID}_y || Y_1^* || PU_s || N_3) \oplus \text{SPID}_y$. At that moment, the param-

![Table 2 Notations used in this protocol](image1)

| Symbol     | Description               |
|------------|---------------------------|
| SIDy       | Server identity           |
| MIDy       | Mobile device’s identity   |
| PIDy       | Patient biometric identity |
| BPID       | Patient password          |
| PSp        | Patient password          |
| Ks         | Private key of server     |
| Kp         | Private key of patient    |
| $\beta$    | Server’s randoms          |
| $N_1, N_2, N_3, N_4, N_5$ | Patient randoms number |
| PU, PU_s   | public key of patient and server |
| EC         | Elliptic curve            |
| Y          | Base point of elliptic curve |
| Enc(.)/Dec(.) | Symmetric-key encryption/ decrytion using k |
| $h(.)$     | hash operation            |
| SK_s       | Shared session key        |
| $\oplus$   | Xor operation             |
| $\parallel$| Concatenation             |
| $V_1, V_2$ | Verifiers                 |
| SK_t       | Session key               |
| $c_{on}$   | Challenge series          |

![Table 3 Message flow in registration phase](image2)

| Steps | Flow | Message | Description |
|-------|------|---------|-------------|
| 1     | UN   | S_j     | $\{\text{RPID}_y || \text{SPID}_y || \text{PU}_p || N_2 || N_3\}$ |
| 2     | S_j  | UN      | $\{Y_2 \parallel Y_3 \parallel PU_s \parallel Ch_1\}$ |
Table 4  Message flow in login and authentication phase

| Steps | Flow     | Message               | Description                                                                 |
|-------|----------|-----------------------|-----------------------------------------------------------------------------|
| 1     | UN → SJ  | Login_Msg1            | \{ V₁ \parallel V₂ \parallel N₁ \parallel Kᵣ \}                         |
| 2     | SJ → UN  | Login_Msg2            | \{ Y₂ \parallel Y₆ \parallel SK \parallel Au₁ \}                         |
| 3     | UN → UN  | Login_Msg3            | SK = h(Pᵦ₁ \parallel Y₂ \parallel n₅ \parallel N₂ \parallel m₆ \parallel Tₓ), and authentication verifier |
|       |          |                       | Au₂ = h(Vₚ₁ \parallel V₁ \parallel SK)                                    |

Fig. 5  Proposed authentication protocol
eter $Y^*_5$ being computed is compared to $Y_5$ stored in the mobile device. If both are equal, then we can trust that the mobile device is possessed by legal user. Subsequently, the user generates a random number $N_5.P$ and calculates the point $n_5 = N_5.P$ on the elliptic curve. Using the public key of the server PU's, the patient computes another point on the elliptic curve as an supplement key $PK = n_5.PU_s = n1.Y_1.P = Yi.N_5$

Now he calculates $Y_4 = h(N_1 || N_4 || N_5).P$. The P encrypts $(Y_4 || SPID_i^* || N_2)$ with the supplement key $K^*$. Then computes a verifier $V1 = Enc_{K}(Enc_{PK}(Y_4 || SPID_i^* || N_2)) || N_5)$ an encrypted value using $Y^*_4$. Next the user captures the current time stamp $T_p$ and computes a second verifier using the patient password $V_2 = h(Y^*_4 || SPID_i) || Y_4)$. At the end, he/she sends { $V_1 || V_2 || N_3 || K^*$} through an unsecured channel to the medical server.

- **Step 2:** At the reception of the message from patient, the server first checks the freshness of the timestamp $T_1$. If it holds, using its owner identity SID, its private key $K_s$, and the random $N_3$ received in the previous step, the server computes its version $Y^*_1 = h(SID, || N_3) || K_s$ and uses it to decrypt the received message i.e $Dec_{K_s}(V1) = (Enc_{K_s}(Y_1 || SPID_i^* || N_2)) || N_5)$. Now, in the possession of $n_6^*$ the server is able to get the value of the supplement key, such as $K^* = N_6.n_6^*$, which can be then used to decrypt $Dec_{K_s}^*(V1)(Enc_{K_s}^*(Y_1 || SPID_i^* || N_2)) = (Y^*_4 || SPID_i^* || N_2)$ and get the estimated values $Y^*_4$ and $N^*_2$. Subsequently, the server computes $X^*_7$ and compares the obtained value with $V_3$. If not identical, the server rejects the session and terminate the communication. Otherwise, if both equal, then the server can trust the authenticity of the patient and the received message. Thereafter, the server generates a random number ‘m’ and uses it to calculate $K^* = N_6.n_6^*$. Next, to create the second challenge $Y_6$ the server computes $N_2)$, and encrypts it using $K^*$ i.e $Y_5 = Enc_K^*(N^*_2)$. At the third challenge is also computed as the encrypted value of the secret commitment key ‘$K_s$’ using $(N^*_2)$ calculated in the registration phases, i.e $Y_6 = Enc_{N_2}(K^*)_3$. At this stage, a session key is computed as $SK$ along with an authentication verifier $Y^*_8$. Finally, the server sends the message { $Y_5, Y_6, SK, Au_1$} to the patient.

- **Step 3:** After receiving the message from the server, the user first decrypt $Y_5$ using key and get $(N^*_2)$. It checks freshness of message. Then, he/she computes $(N^*_2)$ uses it to decrypt $Dec(N^*_2) || N_5) = K^*_B$. Obtain the secret commitment key $K^*_B$. With the possession of secret key, the patient is now able to decrypt the first challenge sent in the registration phase $Y_6$, and Obtain $(N_2)$. At this moment, the patient verifies $N_2$. If they match then the server is legitimate and can be trusted.

Thereafter, the user sends the login request to the server and it proceeds to the computation of the session key as $SK = h(PU_s) || Y^*_1 || N_5 || N_2 || m_6 || T_5)$, and authentication verifier $Au = h(V^*_1 || V_1 || SK)$, using its own parameters and the received $Y_5$. Then, he/she compares the received $Au_1$ with its own $Au_2$ previously calculated. If equal, then the server is authenticated and both parties are now agreed on a common session key. All messages transferred in this phase is shown in Table 4.

### 4 Performance analysis

The proposed LWC technique is implemented in Arduino Uno (8-bit microcontroller) with 32 kb flash and 2 kb SRAM. The encryption and decryption time with clock cycles are shown in Table 5. Now, the performance measurement of the proposed scheme is done by measuring operational cost, Operational cost is the total of communicational cost and computational cost. Here the communication cost is calculated in two-part. During the registration process, the communication cost is 2520 bits and in the login process is 4260 bits. Computational cost depends on the number of hashing. The performance comparison is given in Table 6.

#### Table 5 Speed and memory usage comparison of LWC

| Algorithm | Speed (clock-cycle/ bytes) | Memory usage (bytes) | Encryption time (ms) | Decryption time (ms) | Rounds (bytes) |
|-----------|-----------------------------|----------------------|----------------------|----------------------|----------------|
| LEA [31]  | 24,621                      | 1601                 | 550                  | 106                  | 24/28/32       |
| HEIGHT [4] | 26,401                      | 1506                 | 569                  | 208                  | 32             |
| SIMON [3] | 38,026                      | 681                  | 625                  | 280                  | 32/36, 44/52, 54/68, 69, 72 |
| LWC(This Scheme) | 23,595                      | 1194.3               | 636                  | 130                  | 32             |
which shows that the number of hashing in the authentication process is less so that the proposed authentication protocol will be lightweight. Also, Table 7 shows that most network attacks are resisted by this authentication protocol.

5 Detail security analysis

In this section the formal security analysis is explained.

The formal proof of the proposed protocol is done by using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. AVISPA shows simulation results after verification process. AVISPA is widely accepted verification tool which uses on-the-fly-model (OFMC), CL-based Attack searcher (CL-At), SAT based model checker (SATMC), and Tree-Automata-based protocol Analyser (TA4SP). The first back end is on-the-fly-model (OFMC) checker. CL-based Attack searcher (CL-ATSE) is the second section. It provides transmission if any security threats occurred. SAT based model checker (SATMC) makes the proposed formula and solves SAT (state-of-the-art formula). Tree-Automata-based protocol Analyser (TA4SP) is the last backend. It performs tree automation include intruder. Avispa tool analyzes protocol using high-level protocol specification language (HLPSL language). There are basic role, composite role. The fundamental role represents each participant’s role. The roles for the session, and the goal and environment of the proposed scheme are specified the simulation result in proposed OFMC. Then after it gives the simulation result in proposed ATSE trace of attack. The output of OFMC’s proposed authentication is shown in Fig. 8. OFMC is a market-based methodology. It is a symbolic way for expressing state-space. OFMC is limited in the number of session protocols it can use. There is also a performance speed, as the execution time is really short. The Dolev-Yao Model is used to check for replay attacks. In regular sessions with man-in-the-middle assaults, this model is used.

![Fig. 6 Avispa code in Hlpsl user role](image_url)
The word SUMMARY is used in the next section. Its simulation procedures are available. It was determined to be safe, dangerous, and inconclusive. Avispa code is shown in Figs. 6 and 7. The DETAILS section ensures the safety of the proposed work. Result is utilized in the next section. Attacks were discovered. It creates SAFETY. Simulation result in proposed ATSE is shown in Fig. 8.

6 Conclusion and futurescope

One of the challenges in the IoT systems is data confidentiality which is focused in this paper. In this paper a lightweight block cipher technique is proposed which has a flexible structure. This helps to design a flexible cryptosystem for a wide range of hardware implementation on IoT devices. This framework is mainly designed for a health monitoring system.
systems which are a part of electronic healthcare. In this monitoring system the captured data is encrypted using LWC and the data user can access it after proper authentication. The performance of the system is also measured and the formal proof is done for high-level security. The LWC ciphering technique used mainly 128-bit to 256-bit keys. The computational cost of the proposed framework is low(12 Th) in comparison with another existing scheme. Thus it is suitable for IoT devices that have low power and memory. The major limitation of our work is the comparatively high encryption time of the proposed LWC. Thus the speed enhancement for software implementation of proposed LWC is one of the future work. Also to give optimized performance by balancing between memory usage and speed, in future an enhanced model can be produced.

References

1. Ali A, Khan FA (2010) An improved ek-g-based key agreement scheme for body area networks. In: International conference on information security and assurance, Springer, New York, pp 298–308
2. Alassaf N, Gutub A, Parah SA, Al Ghamdi M (2019) Enhancing speed of simon: a light-weight-cryptographic algorithm for iot applications. Multimed Tool Appl 78(23):32 633–32 657
3. Beaulieu R, Shors D, Smith J, Treatman-Clark S, Weeks B, Wing- ers L (2015) The simon and speck lightweight block ciphers. In: Proceedings of the 52nd Annual Design Automation Conference, pp 1–6
4. Hong D, Sung J, Hong S, Lim J, Lee S, Koo B-S, Lee C, Chang D, Lee J, Jeong K, et al (2006) Hight: a new block cipher suitable for low-resource device. In: International Workshop on Cryptographic Hardware and Embedded Systems. Springer, New York, pp 46–59
5. Mullai A, Mani K (2021) Enhancing the security in rsa and elliptic curve cryptography based on addition chain using simplified swarm optimization and particle swarm optimization for mobile devices. Int J Inf Technol 13(2):551–564
6. Shariq M, Singh K (2021) A vector-space-based lightweight rfid authentication protocol. In: International Journal of Information Technology, pp 1–10
7. Yamin M (2020) Counting the cost of covid-19. Int J Inf Technol 12(2):311–317
8. Kebande VR, Karie NM, Ikuesan RA (2021) Real-time monitoring as a supplementary security component of vigilantism in modern network environments. Int J Inf Technol 13(1):5–17
9. Hurbungs V, Bassou V, Fowdur T (2021) Fog and edge computing: concepts, tools and focus areas. Int J Inf Technol 13(2):511–522
10. Jiang C, Li B, Xu H (2007) An efficient scheme for user authentication in wireless sensor networks. In: 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW’07), vol 1. IEEE, pp 438–442
11. Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Workshop on the theory and application of cryptographic techniques. Springer, New York, pp 47–53
12. Kumari S, Renuka K (2021) Design of a password authentication and key agreement scheme to access e-healthcare services. Wireless Pers Commun 117(1):27–45
13. Jahan S, Chowdhury M, Islam R (2019) Robust user authentication model for securing electronic healthcare system using fingerprint biometrics. Int J Comput Appl 41(3):233–242
14. Alaba FA, Othman M, Hashem IAT, Aloataibi F (2017) Internet of things security: A survey. J Netw Comput Appl 88:10–28
15. El Zouka HA, Hosni MM (2019) Secure iot communications for smart healthcare monitoring system. Internet of Things, p 100036
16. Dhanvijay MM, Patil SC (2019) Internet of things: a survey of enabling technologies in healthcare and its applications. Comput Netw 153:113–131
17. Pasha M, Shah SMW (2018) Framework for e-health systems in iot-based environments. Wireless Communications and Mobile Computing, vol 2018
18. Islam MM, Rahaman A, Islam MR (2020) Development of smart healthcare monitoring system in iot environment. SN Comput Sci 1:1–11
19. Tamilselvi V, Sribalaji S, Vigneshwaran P, Vinu P, GeethaRamani J (2020) Iot based health monitoring system. In: 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, pp 386–389
20. Acharya AD, Patil SN (2020) Iot based health care monitoring kit. In: 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), IEEE, pp 363–368
21. Li M, Yu S, Lou W, Ren K (2010) Group device pairing based secure sensor association and key management for body area networks. In: Proceedings IEEE INFOCOM, IEEE 2010:1–9
22. Zhang Z, Wang H, Vasilakos AV, Fang H (2012) Ecg-cryptogr- phy and authentication in body area networks. IEEE Trans Inf Technol Biomed 16(6):1070–1078
23. Xue K, Hong P, Ma C (2014) A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. J Comput Syst Sci 80(1):195–206
24. Turkanović M, Brumen B, Höbl M (2014) A novel user authenti- cation and key agreement scheme for heterogeneous ad hoc wire- less sensor networks, based on the internet of things notion. Ad Hoc Netw 20:96–112
25. Das AK, Goswami A (2015) A robust anonymous biometric-based remote user authentication scheme using smart cards. J King Saud Univ Comput Inf Sci 27(2):193 – 210. Available: http://www. sciencedirect. com/science/article/pii/S1319 157815000178
26. He D, Zeadally S (2015) An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE Internet Things J 2(1):72–83
27. Yeh K (2016) A secure iot-based healthcare system with body sensor networks. IEEE Access 4:10 288–10 299
28. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, AN, Farouk A (2018) Secure medical data transmission model for iot-based healthcare systems. IEEE Access 6:20 596–20 608
29. Moosavi SR, Nigusse E, Levorato M, Virtanen S, Isoaho J (2018) Performance analysis of end-to-end security schemes in health- care iot. Procedia Computer Science, vol. 130, pp 432 – 439, the 9th International Conference on Ambient Systems, Networks and Technologies (ANT 2018)/The 8th International Conference on Sustainable Energy Information Technology (SEIT-2018)/Affili- ated Workshops. [Online]. Available: http://www. sciencedirect. com/science/article/pii/S1877 050918304228
30. Banerjee S, Dutta MP, Bhunia CT (2015) A perfect dynamic- id and biometric based remote user authentication scheme under multi-server environments using smart cards. In: Proceedings of the 8th International Conference on Security of Information and Networks, ser. SIN ’15, New York, NY, USA: ACM, pp. 58–64. [Online]. Available: https://doi.org/10.1145/2799079.2799084
31. Hong D, Lee J-K, Kim D-C, Kwon D, Ryu KH, Lee D-G (2013) Lea: A 128-bit block cipher for fast encryption on common processors. In: International Workshop on Information Security Applications. Springer, pp 3–27

32. Dhillon PK, Kalra S (2017) A lightweight biometrics based remote user authentication scheme for iot services. J Inf Secur Appl 34:255–270