Lightweight authentication scheme based on modified EAP security for CoAP protocol-based IoMT applications

Pritam S. Salankar* and Vinay Avasthi

School of Computer Science,
University of Petroleum and Energy Studies,
Energy Acres, BIDHOLI, via, Prem Nagar,
Dehradun, Uttarakhand 248007, India
Email: p.salankar@gmail.com
Email: VAVASTHI@ddn.upes.ac.in
*Corresponding author

Ashutosh Pasricha

Schlumberger, South Delhi, India
Email: apasricha@slb.com

Abstract: The medical data generated from the patients that are communicated and stored on servers are highly sensitive, and also the IoMT network creates open spaces for an adversary. The proposed work designs a lightweight authentication scheme to support the extensible authentication protocol (EAP) called lightweight EAP (L-EAP). The proposed L-EAP modifies the EAP model and dynamically changes the security service as per healthcare application requirements. The L-EAP selectively applies the data encryption and integrity without frequent re-handshaking with the server using one-bit epoch field in the EAP message header. The L-EAP performs such a key generation process as a part of the authentication phase and enlarges the lifetime of the IoMT network. The advanced encryption standard (AES) is improved for providing data confidentiality in L-EAP. The L-EAP improves the confusion property of cipher text in AES and applies shift row and XOR operations to all the words.

Keywords: internet of medical things; IoMT; lightweight mutual authentication; improved AES-based encryption; modified EAP; dynamic service change.

Reference to this paper should be made as follows: Salankar, P.S., Avasthi, V. and Pasricha, A. (2023) 'Lightweight authentication scheme based on modified EAP security for CoAP protocol-based IoMT applications', *Int. J. Information and Computer Security*, Vol. 20, Nos. 1/2, pp.176–198.

Biographical notes: Pritam S. Salankar is a PhD scholar at School of Computer Science, UPES, Dehradun, Uttarakhand. He has an ME in Electronics (specialisation in Computer Technology) from SGGS Nanded Maharashtra, BE in Electronics from BDCOE, Sewagram Dist Wardha, Maharashtra. His research area is light weight encryption algorithm for internet of things.

Vinay Avasthi has a BSc (PCM) from HPU Shimla – HP, MCA from MDU Rohtak – Haryana, Phil in Computer Science from MKU, Madurai – TN and PhD in Computer Science from UPES Dehradun Uttarakhand. He is an Associate Professor at School of Computer Science UPES Dehardun. He has around 40 publications in a reported journals/conference proceedings. His research interest includes are software engineering, cloud security, IOT, software reusability, machine learning, and smart computing. He is a member of CSI, ACM and IEEE.

Ashutosh Pasricha is the Oil Field Services and Equipment Sales Director at Schlumberger, South Delhi, India. He received his PhD from IIT, Delhi in 1999, MTech in Water Resources Engineering from REC, Kurukshetra in 1991 and BTech in Civil from REC, Kurukshetra in 1989. His dissertation topic is Watershed Modelling using Geographical Information. He has Certificate Course on Miller Heimen Strategic Selling Training from Certified Instructor. His professional affiliation are Indian Association of Hydrologists LM 940, Indian Water Resources Society LM 944508, Institution of Engineers (India) AM 71466/9 and Indian Society for Technical Education LM 14749. He has specialties in geographical information system and remote sensing technologies, infrastructure solution architecting, high end virtual reality and collaboration technologies/solutions, communication solutions and design expertise, application of various technologies in water resources sector, real time solutions and its implementation and project management.

1 Introduction

The internet of medical things (IoMT) consists of internet-enabled devices and upgrades the healthcare applications by utilising these internet-enabled sensors collectively. These devices can sense the environment, communicate with each other, and react to changes in their environment (Kabalci et al., 2019; Asghari et al., 2019). These IoMT devices are supposed to apply the constrained application protocol (CoAP) to communicate at the application layer (Shelby et al., 2014). With the increased adoption of IoMT, the security and confidentiality of data in CoAP remain the main problem, especially for healthcare applications (Hassan, 2019; Abdulghani et al., 2019; Obaidat et al., 2020; Yu et al., 2020; Radovici et al., 2018). The healthcare application provides various services, and the security requirement and priority of each service differ significantly. For instance, the healthcare IoT network monitors each patient's health securely by applying end-to-end communication. The primary services in the healthcare sector need strong authentication and encryption schemes (Panchatcharam and Vivekanandan, 2019). However, the low-priority services need authentication and integrity alone. Thus, it is concluded that the IoMT application needs a method that can apply security service optionally and dynamically on the IoMT application layer protocol according to the priority of messages. The proposed work selects the extensible authentication protocol (EAP) model to apply a security scheme dynamically over IoMT networks, based on the following observation (Pawlowski et al., 2015a). The EAP is the most commonly used authentication scheme in wireless networks, and it provides different authentication mechanisms. It offers flexibility to choose an authentication mechanism that fits best in each case without changing the protocol. However, the proposed work has to design a lightweight EAP for IoT healthcare applications since most EAP methods use six and

more than six flight handshake messages for authentication. The EAP is flexible, and there is a possibility to use EAP in IoMT communication via secret key generation using a pre-shared EAP key. These two points make the EAP the best choice for a secure IoMT application.

1.1 Contributions of the proposed work

The proposed work designs a lightweight EAP scheme (L-EAP) for authenticating the users in healthcare IoMT applications.

1 The proposed work aims to implement a lightweight authentication mechanism by modifying the EAP model and dynamically changing the security service from supporting both the authentication and data confidentiality to just integrity as per healthcare application requirements.

2 By utilising one-bit epoch field in the EAP message header, the L-EAP selectively applies the data encryption and integrity technique without frequently re-handshaking with the server. It ensures a lightweight, customised authentication scheme on the application layer.

3 The proposed lightweight authentication scheme performs the process of key generation as a part of the authentication phase and effectively utilises the constrained resources in IoMT devices.

4 The proposed work introduces nonce for reducing the round trip time from three to two without compromising the security to avoid the possibility of a denial of service (DoS) attack due to the complexity of basic EAP.

5 To ensure that a small change in the data makes huge modification in the encrypted format and improve the confusion property of cipher text in AES, the L-EAP scheme splits each word in plain text and applies shift row along with XOR operation to all the words instead of applying to the first word.

6 The L-EAP scheme introduces a restricted sequential round concept in AES without increasing the complexity of the encryption process to avoid the possibility of tracing the differences between the words in cipher text using the biased inputs in the key space.

2 Related work

Due to the limitations of IoMT devices, authentication in IoMT application scenarios is challenging. Many works have been proposed for lightweight solutions to address these limitations and support authentication in resource-constrained environments. Most conventional authentication schemes consider only the knowledge factor, representing information that the IoMT device possesses. However, it is not always secure. Most of the conventional schemes involve symmetric and asymmetric encryption schemes, but they are heavyweight for resource-constrained devices. The existing approaches exploit two-factor or three-factor, lightweight authentication schemes (Li et al., 2017, 2018; Wu et al., 2017, 2018; Jiang et al., 2017). Moreover, the local differential privacy can be applied for IoMT security. For instance, four different protocols have been developed

under local differential privacy using universal hash functions (Wu et al., 2020). The Lyapunov exponent analysis and echo state network (LEAESN) in Salemi et al. (2021) is designed using machine learning algorithms. However, the computational complexity of those protocols is high, and it is not feasible for resource-constrained medical sensors. A lightweight three-factor authentication protocol has been proposed for a constrained application protocol (COAP)-based network architecture (Dhillon and Kalra, 2017). Mostly, the suggested schemes consider identity, password, and secret key for authentication. However, they are suitable for a specific IoMT application. The IoMT smart objects in real-time applications belong to different services, but they need to be deployed and bootstrapped in the same security protocol over resource-constrained devices.

2.1 EAP-based authentication schemes for IoT

As the EAP supports multiple authentication schemes, it is suitable for many IoMT applications. A novel bootstrapping service with EAP and authentication, authorisation, and accounting (AAA) infrastructures attempts to offer a flexible, scalable, secure and constrained solution for resource-constrained IoMT devices. After bootstrapping, a new CoAP option (AUTH Option) is introduced for integrity protection and key hierarchy. The AAA-based infrastructures (Housley and Aboba, 2016) provide a flexible, scalable, and federation-aware bootstrapping service in IoMT. They are robust infrastructures for ensuring the authentication, authorisation, and accounting of IoT devices. In conjunction with the EAP (Aboba et al., 2016), a secure framework with authentication, authorisation, and key distribution has been proposed. Moreover, it can support large-scale deployments.

The extensible authentication protocol-pre-shared key (EAP-PSK) (Bersani and Tschofenig, 2007) exploits symmetric key cryptography and reduces computational costs. However, the EAP-PSK can offer a lower degree of scalability and security than a public key-based authentication mechanism. All of the above solutions share a common issue, and they enforce the nodes to frequently handshake with the gateway and sometimes introduce potential security threats due to lengthy cipher suits. The extensive authentication protocol (EAP) with slim extensive authentication protocol over low-rate wireless personal area networks (SEAPOL) (Pawlowski et al., 2015b), Trust extension protocol for authentication of new deployed objects and sensors through the manufacturer (TEPANOM) is presented in Pawlowski et al. (2015a), and low-overhead CoAP-EAP (LO-CoAP-EAP) in Garcia-Carrillo et al. (2017). The LO-CoAP-EAP has been consuming battery resources in an acceptable amount than most of the EAP-TLS methods. Moreover, the size of the EAP header has been reduced to achieve better resource consumption. The EAP supports multiple authentication methods, in which some of them are secure and some of them are high speed. However, it does not ensure consequent secure CoAP communication without consuming huge resources. Also, the DoS attack exploits the lengthy cipher suit and re-handshaking process in EAP protocols.

2.2 Lightweight encryption schemes for IoT

Several lightweight encryption algorithms using both symmetric and asymmetric techniques have been suggested for various IoT applications. A lightweight encryption algorithm is proposed in Usman et al. (2017) to provide enhanced security for data

transmission between IoT devices. It exploits the Feistel structure as well as network with a uniform substitution-permutation in a combinational form. Likewise, data encryption standard (DES) in Ren and Miao (2010) applies symmetric key block cipher with Feistel structure. The plaintext of 64-bit and a key size of 56 bits are used in the encryption process with 16 rounds. However, a main drawback in the DES algorithm that it lacks in allowing flexibility in Feistel structure and hence does not support any modification in it for various IoT application services (Ren and Miao, 2010). A symmetric encryption algorithm proposed in Gao et al. (2018) attempts to offer privacy in both forward and backward directions using multi-cloud computing. However, it is prone to information leakage. This algorithm is faster than DES, but it is vulnerable to several attacks. In addition, the involvement of several components in M-SSE makes it very complex.

An algorithm in Zhdanov and Sokolov (2016) is designed based on many-valued logic and variable block length. The encryption process is performed for five rounds iteratively. It varies the number of rounds, round1 includes the gamma and permutations procedures, and other rounds include substitution and gamma procedures. Super-encryption cryptography in Abdullah et al. (2018) is suggested with the international data encryption algorithm (IDEA) and word auto key encryption (WAKE) algorithm. The super encryption technique takes more than two symmetric cryptographic algorithms to ensure more security to IoT data. Even though they are designed specifically for resource-constrained IoT devices, some complex processes are performed with conventional symmetric and asymmetric algorithms for ensuring high-level security. The most attractive encryption algorithm for IoT is the tiny encryption algorithm (TEA) due to its lower memory utilisation and ease of implementation. The main problem associated with the TEA and its numerous developed versions is applying the same key for encryption rounds. However, it decreases the strength of the security algorithm. In addition, it takes a huge time for the encryption and decryption process (Rachmawati et al., 2018; Novelan et al., 2018). A novel tiny symmetric encryption algorithm (NTSA) is enhanced security for the IoT network, and it introduces additional key confusion dynamically for each round of encryption (Rajesh et al., 2019). However, it is limited to the specific IoT service, and it does not focus on reducing the unnecessary re-handshaking processes in IoMT applications.

3 The proposed method

3.1 Problem statement

The design of existing security models for IoMT is not always suitable for resource-constrained sensor devices due to the following reasons. The first reason is the expensive handshaking of EAP due to the lengthy cipher suite agreement process. Complex handshake processes are not protected from attacks always. Sending a handshake request message from the application layer frequently to low-memory and capacity devices can seem to be a DoS attack. An attacker could send several ClientHello messages to a server. This scenario would cause a DOS attack against the server. Applying the lightweight authentication scheme for healthcare data transmission to ensure confidentiality and integrity is not always necessary. To support various services

based on the priority of healthcare applications, the resource-constrained nodes should change the security services supporting both confidentiality and integrity to just confidentiality without handshaking with the server. Applying the existing cryptographic techniques for secure data communication is inadequate for resource-constrained sensor devices. The differential method or liner methods of cryptanalysis can deduce the overall key in AES since the generated words using the original key are related. Biased inputs in the keyspace of AES create a space to observe the differences between the words in the cipher text. Thus, the proposed work plans to improve IoMT security using EAP and implement lightweight and strong cryptography techniques, AES, and ECDSA, while minimising its complexity.

3.2 Overview of the proposed method

It is crucial to deploy the EAP with lightweight methods for IoMT security as per the application needs. The proposed security model implements the authentication service and changes the requirement of the security service based on the priority level. Figure 1 shows the block diagram of the L-EAP. To attain the aim without increasing the complexity, the proposed approach incorporates the following four ideas:

- *Lightweight EAP mutual authentication:* the proposed authentication scheme provides a lightweight mutual authentication along with the creation of a secret/private key. It results in reduced energy consumption without compromising communication security. The proposed mutual authentication provides two major functionality:
  1 lightweight mutual authentication, including secret/private key generation
  2 enabling application-specific cryptography technique, either lightweight advanced encryption standard (AES) or elliptic curve digital signature algorithm (ECDSA) with data integrity algorithm.

  It performs the process of key generation as a part of the authentication phase. The generated secret key in mutual authentication is used as the symmetric key for AES and the private key for ECDSA. The proposed mutual authentication scheme reduces the round trip time of EAP request/response messages without compromising communication security.
- *Application-specific customised security model in CoAP:* the proposed L-EAP scheme consists of only two cryptography and integrity methods, such as lightweight AES-128, ECDSA (Al-Zubaidie et al., 2019), and SHA 1 for data integrity. Enabling the re-handshaking with an IoMT node to select the security service is inefficient for resource-constrained IoMT devices. The proposed scheme introduces the one-bit epoch to selectively apply data encryption and integrity without re-handshaking with the server. It ensures a lightweight, customised authentication scheme concerning the application requirements. It decreases the resource usage and increases the network lifetime. A sender node sets the flag bits value in the epoch field to denote whether the data confidentiality needs to be applied during data transmission, which depends on the priority level of messages. It applies the data encryption method according to the flag bits value.

- *Reducing the lengthy cipher suite:* nonce is used for reducing the round trip time to two without compromising the security. It avoids the possibility of a DoS attack in L-EAP due to the complexity of basic EAP. Moreover, the risk of losing confidentiality and implemented security service due to the lengthy cipher suite process is minimised using nonce.
- *Improving AES-128 security:* the key expansion unit is suggested to deliver the expanded keys to the internal rounds of the AES. The expanded keys have to improve the property of confusion and diffusion. Those properties ensure that if any part of the key at either round 1 or round 'n' is known, there is no possibility to derive other keys of that round and the subsequent rounds. In the operation of shift row transformation, the proposed work divides each state into two parts in the matrix and introduces the restricted sequential round constantly to improve the state diffusion and security. It ensures that small changes in data make a huge modification in the encrypted format.

3.3 Application specific customised security model in L-EAP

Data security over healthcare communication is crucial. To solve the security issues, the proposed CoAP standard specifies the use of symmetric/asymmetric optionally along with a hashing algorithm that provides data confidentiality and integrity as a default cipher suite for EAP. However, the existing EAP designs are not fit for resource-constrained IoMT devices. There are several requirements in designing the novel lightweight authentication scheme, including bootstrapping and secure communication for IoMT applications.

3.3.1 System and network model

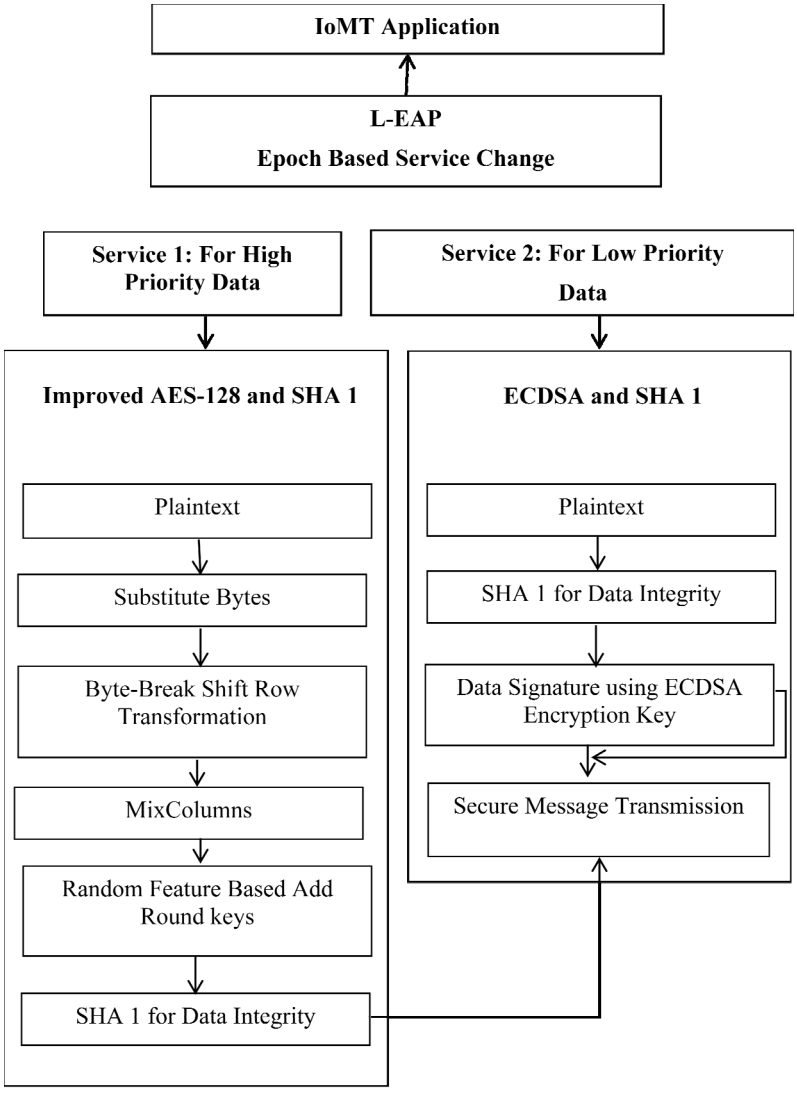
The system model of IoMT considers a network with N wireless devices. The gateway node δ is situated in the corner of the IoMT network and sensor objects denoted as S are located in different positions in the network. The most significant processes involved in the system of L-EAP are given in below.

- *Definition 1 (Registration phase):* In the registration phase, each IoMT node S is registered with a unique and fixed bit-length identity ID, at the δ and generates the pre-shared EAP key (ψ) for each node S. Both the entities δ and S require the maintenance of ψ and an entity δ is responsible for maintaining ψ for each registered communication entity. Thus, the gateway δ shares ψ_i with the corresponding S_i securely.
- *Definition 2 (Mutual authentication phase):* After receiving the EAP ID response message, the δ compares the ψ_i value of corresponding node S_i. If both the values are not equal, the proposed scheme terminates the EAP connection. Otherwise, the gateway δ believes that S_i is an authorised device, and it sends the AUTH request message with the nonce values, and both the entities such as S_i and δ derives SK = ψ || nonce 1 || nonce 2 for mutual authentication.
- *Definition 3 (Key generation phase):* In the L-EAP scheme, two nonce values authenticate the entities on both sides. The values of nonce 1, nonce 2, and ψ) are used to determine the same secret key, SK, on both sides individually.

- *Definition 4 (Service change phase):* A node S_i forwards the EAP_ID response by assigning the F_Bit value to one and continues the secure data communication. Without executing the process of mutual authentication processes again, the S_i changes the service from one to another by sending the EAP_ID response with zero value in the flag bit.

The phases above are the most prominent processes involved in the L-EAP.

Figure 1 Block diagram of the proposed work



3.3.2 Bootstrapping in IoMT

The bootstrapping includes the transfer of security parameters and keying material to enable trustworthy operation in L-EAP. It is performed before the process of authentication and communication between the smart object and the gateway node. The bootstrapping phase is executed as a prerequisite offline phase, where the IoMT nodes have to share a 128-bit Pre-shared EAP Key ψ for performing further operations in L-EAP. As each IoMT device relies on different operations (AES-128, ECDSA, and SHA 1) to secure its data communications over various application services, it is essential to provide key material and generate secret keys for subsequent communications. Moreover, the L-EAP only includes the bootstrapping operations between gateway δ and IoMT device S_i. It is assumed that a secure protocol (like RADIUS) is running between the gateway and server.

3.3.3 Secure communication in IoMT

The six flight messages used in the EAP handshake process lead to communication delay and energy inefficiency. Also, the lengthy cipher suit tends to the risk of losing node confidentiality and data privacy information. Thus, the proposed work has to present a novel EAP-based mutual authentication scheme, L-EAP, in lightweight processing and faster response. Healthcare applications do not require both data integrity and confidentiality for transferring all the messages over different services. The communication requires only data integrity for low priority messages, but not data confidentiality, because such information might not be useful to attackers. During the transmission of reports to a patient, the communication needs to apply data integrity and confidentiality. Whenever a communication entity requires to change a cipher suite for supporting another service in a healthcare application, the overburden handshake process needs to be repeated. It is important to avoid the frequent re-handshaking process. Moreover, in the aspect of effective resource use of IoMT devices, reducing the computation load to perform authentication and data encryption every time is crucial.

3.4 Selectively applying data encryption or integrity

The proposed scheme can apply security service optionally according to the need of the application. An IoMT node can change its security service from data encryption using lightweight AES and data integrity, and the next is data integrity with digital signature alone. The first service is suitable for sharing private information between patient and doctor, whereas the latter is applied for less-important communication. The EAP cipher suite should be negotiated during the handshake process between the IoMT node and gateway. However, the communication messages provide confidentiality using AES or data integrity with a signature using ECDSA optionally after completing the EAP handshake process. Even after the EAP session is created, the communication messages with or without encryption can be exchanged during the effective time. There is a need to frequently change the service and re-handshaking due to the unpredictable IoMT service scenarios. However, the main cause of resource waste is the negotiation of cipher suite change for a particular service. To avoid this problem, the proposed L-EAP sets the flag bits value in the epoch field to represent whether encryption is applied during data transmission. Encryption is applied to data based on flag bits value in the header. A

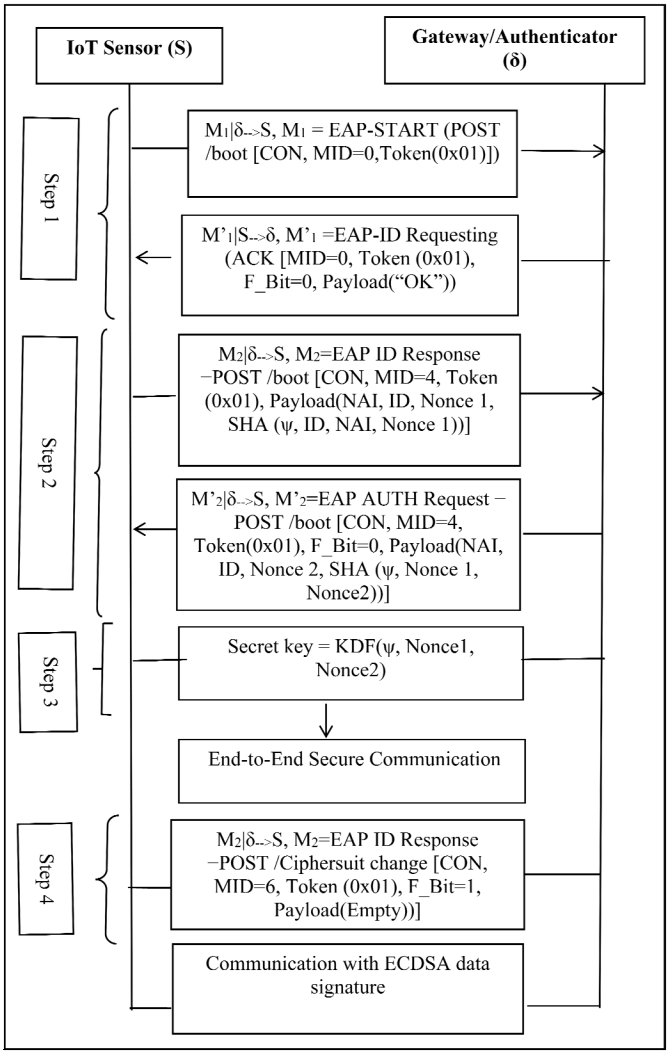
receiver checks whether message encryption is applied or not according to the flag bit (F_Bit) value and thereby verifies the message value.

Table 1 Flag bit in epoch field

F_Bit	*Service*
0	Lightweight AES-128 with SHA128
1	SHA128 with ECDSA digital signature

If the encryption-required messages are transferred, the EAP sets the epoch field bit value as zero and cipher suite to 'lightweight AES-128 with SHA128'. Moreover, if encryption is not required, the EAP session to transfer the messages is set to 'SHA128 with ECDSA digital signature' without initiating the re handshaking process.

Figure 2 L-EAP mutual authentication



3.5 Lightweight EAP mutual authentication

The proposed L-EAP is the mutual authentication scheme implemented between IoMT sensors and gateway, and also it provides an initial secure secret/private key generation for end-to-end communication. The proper utilisation of cryptography and hashing algorithms facilitate the proposed mutual authentication mechanism to use only two round trips to the IoMT server for the complete authentication procedure. To reduce the communication delay after authentication, the L-EAP performs a secure key generation process as a part of its mutual authentication. The L-EAP includes the sensor's network access identifier (NAI) and randomly generated nonce with the first message sent to the authentication server. The message is secured with a hashing technique SHA 1. A secure key generation for end-to-end encryption in the mutual authentication process provides a significant reduction in message exchange without compromising L-EAP security. Figure 2 demonstrates the process of L-EAP mutual authentication.

The proposed authentication scheme provides mutual authentication by carrying out the request-response authentication procedure in both directions. As per the CoAP, a message can be of a type of confirmable (CON), non-confirmable (NON), an acknowledgement (ACK), or a reset (RST). The messages CON or NON are used for sending a request or response depending on the Code field value in the header (Shelby et al., 2014).

Step 1 The first step is M1, EAP-Start-ID. Request handshake, and it is performed between the sensor S and the gateway δ. By using the L-EAP, the sensor nodes connect to the δ. When the IoMT device wants to start the bootstrapping service for EAP, it sends a con POST/boot request to the gateway.

Step 1.1 If a gateway δ accepts the first message, it replies with the M_1' = EAP-ID request message, which requests the sensor identity, NAI. Each message includes a message ID (MID) for avoiding duplicate transmissions. *Every message explores a unique MID for the message, and so it avoids the replay attack later.* An IoMT device is sending a confirmable message wait for an ACK message from the gateway. A token value (Token) is chosen randomly for relaying the request message with the corresponding response. It is maintained for the whole authentication process. *It is because it assists in correlating the request with a matching response.*

Step 2 In the second step, the sensor S sends an M_2 = EAP ID response message, containing the EAP session ID (ID), NAI, and randomly generated nonce 1. The sensor node takes the hash value for ψ, ID, NAI, nonce 1, where the ψ is the pre-shared EAP key between sensor and gateway. This message from the IoMT device indicates creating a resource for the bootstrapping service to the gateway. The message contains a nonce 1, and it is used for the generation of fresh cryptographic material for consequent communication. *Moreover, the randomly generated nonce 1 value assists in preventing the attacker from tracing the secret key value*. The gateway authenticates the sensor node using the preshared EAP key, ψ. The hashing mechanism ensures the integrity of the EAP request/response authentication procedure.

Step 2.1 The gateway δ generates a 128 bit nonce 2 and shares it along with the hash created from the ψ, nonce 1 and nonce 2, which is also used for the same purpose as nonce 1. This message assists the sensor node S in authenticating the gateway δ properly. If the authentication fails at either sensor S or gateway δ, an EAP Fail message is sent to inform the failed authentication and return to an initial state.

Step 3 The mutual authentication process ends with a secure key generation process. To generate the secure secret/private key, a key derivation function (KDF) is utilised, and it is a simplified version of the KDF, GKDF (Clancy and Tschofenig, 2009). Secure communication is started using the proposed scheme.

Step 4 While changing the service, the sender node forwards the EAP_ID response by setting the F_Bit to one. *Notably, zero value in F_Bit denotes the high priority data communication*. The gateway changes the service and communicates with the IoMT node without re-initiating the handshaking process. Thus, L-EAP supports various IoMT healthcare applications without consuming huge resources.

3.6 Private data communication in IoMT using lightweight AES-128

The encryption algorithms need to be unbreakable without having the secret key. However, the attackers employ the cryptanalysis technique and identify either the secret key or plaintext through differential and linear operations. The success rate of cryptanalysis is high if the computational complexity of the algorithm is limited. There are two methods used in encryption techniques, such as diffusion and confusion to thwart cryptanalysis. Diffusion denotes the distributed nature of the encryption algorithm. Encryption with a higher degree of diffusion denotes that a single bit change in the plaintext tends to change many cipher text digits. The confusion defines the complexity of the relationship between the cipher text and the encryption key. The confusion mostly exploits the substitution blocks to replace the plaintext values with other values, and the repeated substitution operation guarantees a high degree of confusion. To improve the robustness of AES, the shift rows of the cipher block hides the perceptual information. Even though, in the original algorithm, shift row transformation achieves diffusion. A main drawback of the model is its simple structure.

The proposed lightweight AES-128 is a symmetric block cipher with an iterative structure. The lightweight AES-128 structure consists of two main blocks, such as cipher block and key expansion block. It specifies the iterative blocks as rounds, and each round has different sub-functions. The AES sub-functions are

1 substitute bytes

2 shift rows

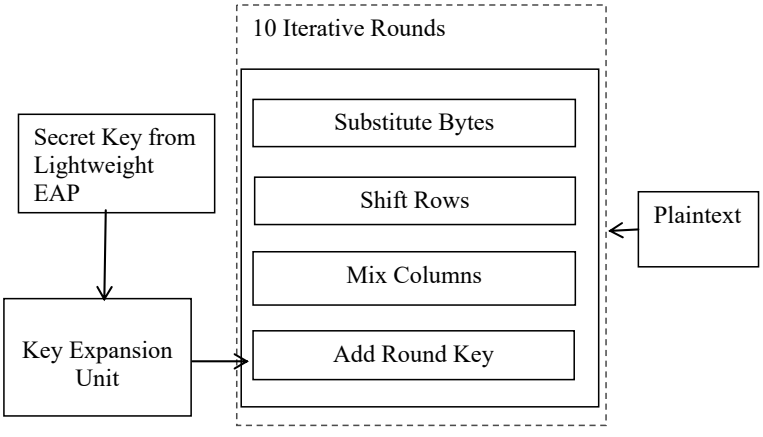
3 mix columns

4 add round key.

It improves the security of IoMT communication against linear and differential cryptanalysis. The basic structure of AES is shown in Figure 3. The AES-128 works on a plaintext of size 128 bits, which is named a block. It partitions the 128 bits into 16 8-bit

values, and it is considered as elements of a four × four matrix. The AES packs the elements of the matrix in column order. This kind of matrix representation is named the state matrix s(x). The sub-functions transform the plaintext into a highly uncorrelated cipher text. Even though those functions are responsible for providing keys to each of the rounds and ensuring data confidentiality, the generated cipher text words using the original key are related. It paves the way for data confidentiality attacks. To avoid this problem, the second and fourth sub-functions are modified in the lightweight AES-128.

Figure 3 Basic structure of AES-128



Other sub-functions in L-EAP are similar to the AES-128.

3.6.1 Byte-break shift row transformation

The AES applies the shift row operation and XOR operation only to the first word of the key expansion unit. Even though it achieves confusion property, the one-to-one mapping property of the XOR function creates open spaces for an adversary. Thus the proposed approach introduces Byte-break shift row transformation instead of considering the state of the matrix. The byte in each state of the matrix is split into nibbles, which denotes that each state element into two-state elements. $S_{i,j}(k)$ represents a state of i^{th} row and j^{th} column. Moreover, the value of k is four since the proposed approach splits the byte on each state element. A data in the rows of state, a nibble is XORed with the shift count sequence of the rows and right-shifted by one bit. The shift count sequence of the rows in one column is shown in Table 2. The same process is repeated for all the columns. It increases the confusion rate in generating the cipher text with the algorithm, and it improves the strength of AES-128 in L-EAP against cryptanalysis.

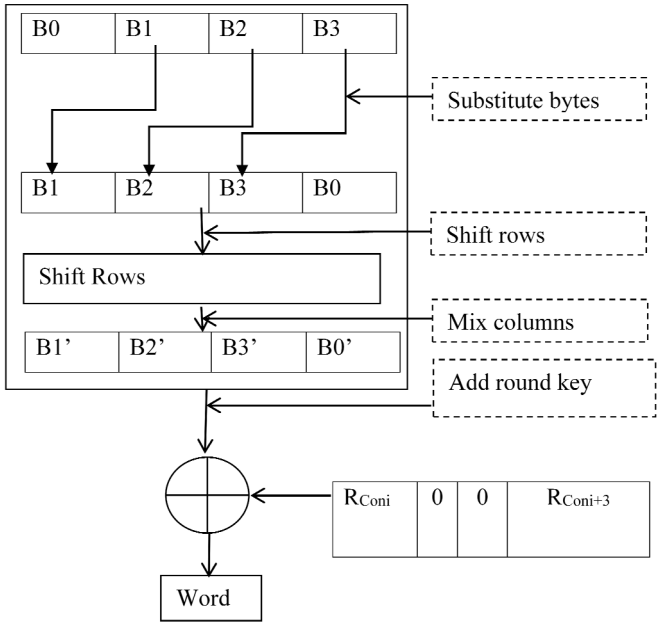
Table 2 Shift count sequence

State ($S_{i,j}(k)$)	*Operation*	*Shift count sequence*
$S_{0,04}$	XOR	0000
$S_{1,04}$	XOR	0001
$S_{2,04}$	XOR	0010
$S_{3,04}$	XOR	0011

3.6.2 Restricted sequential round constant-based add round keys

After the byte-break shift row operation, each column of the resultant state matrix is transformed to a new value to improve the diffusion characteristics of the proposed algorithm. Depending upon the size of the bits in keys, the number of rounds is allowed for AES. The key size of the 128-bit concept allows ten rounds. The key scheduling algorithm in AES is responsible for providing keys to each of the rounds. However, the generated words using the original key are related to each other. The differential method or liner methods of cryptanalysis can deduce the overall key if any word is traceable. Even though the byte-break shift row transformation increases the confusion to the algorithm, there is a possibility to obtain back the original keyspace using the reverse engineering process. Moreover, the differences between the words can be observed using biased inputs in the key space. The sub-function of Add round keys produces the N round keys using the XOR operation with Rcon, derived using GF(2^8) (Benvenuto, 2012) and the state matrix elements. The main drawback in the function of adding round keys is the usage of zero bytes in Rcon. The XOR operation with zero produces the same result. It creates a space for an attacker to trace the secret key. Thus, the proposed methodology attempts to use the idea of sequential round constant. However, if all the bytes are non-zero, it increases the complexity of the AES process. So, the proposed L-EAP plans to introduce restricted sequential round constantly; only the first and fourth byte contains non-zero values.

Figure 4 The proposed add round function in L-EA-CoAP



In AES, the Rcon values are taken only once from the round constants generated using the Rijndael proposal in GF(2^8). In the proposed work, it is performed twice to generate (R_{Coni}, 0, 0, R_{Coni+3}). The structure of the enhanced key expansion unit with the restricted

sequential Rcon is shown in Figure 4. The concept of non-zero round constants in the key expansion unit improves the confusion property of the L-EAP-AES.

3.7 Low priority communication in healthcare application using ECDSA

There is no need to apply the data encryption for some IoMT messages, but they have to prove their authenticity and data integrity at the gateway node δ. Instead of AES-128, the proposed work exploits the ECDSA algorithm for providing a data signature. The symmetric algorithm AES-128 does not ensure non-repudiation, representing the proof of the origin of data because a couple of nodes share a secret key for secure data communication as per the AES-128. Thus, the proposed work exploits the SHA 1 with ECDSA data signature algorithms. The ECDSA algorithm is appropriate for resource-constrained environments due to its small size keys, and it provides integrity, authentication, and non-repudiation. The ECDSA algorithm exploits the key length of 160 bits. Moreover, the operations used in the ECDSA algorithm are as follows: public key generation, signature generation and signature verification.

- *Public key generation at sensor node*
  1 Instead of randomly selecting an integer value d in the interval [1, n − 1], the proposed L-EAP considers a secret key generated during the authentication process as d. If authentication is not performed earlier, an integer value is randomly generated.
  2 Computing the public key value, Q = dG, where G is the base point.
- *Signature generation at sensor node*
  1 Selecting a pseudorandom integer k.
  2 Computing the kG = (x1, y1)
  3 Computing r = x1 mod n. If it returns a zero value, then go to step 1.
  4 Computing the value of k^{-1} mod n.
  5 Applying the SHA-1 algorithm on the plaintext and converting those bit strings to an integer e.
  6 Computing the value of $s = k^{-1}(e + dr) \bmod n$. If it returns a zero value, then go to step 1.
  7 The signature for the plaintext is (r, s).
- *Signature verification at gateway*
  1 Verifying that the values of r and s are integers in the interval [1, n – 1].
  2 Computing SHA-1 (plain text) and converting those bit strings to an integer e.
  3 Computing the value of $w = s^{-1} \bmod n$.
  4 Computing the value of u1 = ew mod n and u2 = rw mod n.
  5 Computing the X value by applying u1G + u2Q.
  6 If X = θ, then reject the signature. Otherwise, the signature is valid.

The ECDSA and SHA-1 are important to ensure strong security against different attacks in low priority messages. The ECDSA algorithm provides strong data integrity and authentication using a data signature and prevents attack tampering with the data.

4 Attack and cost analysis

The security provision of the proposed L-EAP authentication scheme while implementing on CoAP healthcare applications and various services depends on the capability of the proposed authentication scheme in handling different attacker models and offering a secure mutual authentication between the server and IoMT devices. The secure communication of L-EAP against different attackers in Healthcare IoMT applications is as discussed below:

- *Security against replay attack:* if an attacker node A_i attempts to get a registration/AUTH request for a legitimate IoMT device, S_i sends it later and thus gains network access later. The replay attack case is infeasible in the proposed L-EAP = CoAP because all entities (S_i and δ) use a randomly chosen token and nonce values that prevent the attacker from sending the authentication request at a later time. Thus, the proposed L-EAP successfully resists replay attack.
- *Security against guessing attack:* Assume that an attacker A_i attempts to penetrate the hash message between S_i and δ. This attacker attempts to guess the ψ from the EAP ID response or AUTH request to use it to access the network as a legitimate device. An attacker cannot detect the EAP preshared key ψ for any authorised IoMT device because it does not break the configured process of SHA-128 used in the L-EAP. Moreover, the lightweight AES-128 exploits the byte-break shift transformation, and so it is infeasible to guess the secret key by observing the relationship between the words generated during the encryption. As a result, it is safe against guessing attacks in IoMT applications.
- *Security against DoS Attack:* to execute a DoS attack against L-EAP, an attacker needs to eavesdrop on the EAP or AUTH request and send the same request multiple times to destroy IoMT. However, as per the proposed work, legitimate IoMT devices reject login requests containing the same token value, and an attacker A_i cannot use the same nonce values again.
- *Security against traceability attack:* a traceability attacker collects as several EAP authentication requests as possible and analyses these requests to trace an IoMT device identity and secret data about their health. All exchanged requests among entities include the user's identity, and the IoMT devices apply a secure and lightweight AES algorithm to prevent attackers from tracing the data and maintaining the forward secrecy. It reduces the complexity of the basic AES algorithm without making any possibility for attackers to trace the secret key.
- *Security against data confidentiality and integrity attacks:* the proposed L-EAP mechanism achieves better data confidentiality, even in the worst case if the preshared key is compromised since the restricted sequential round constant-based add round keys in the proposed lightweight AES algorithm cannot be easily compromised. It is because, for every intermittent session, a unique round of constant value is generated. If an attacker attempts to modify the packet to either server or IoMT device, the corresponding entity can easily identify the modified packet since SHA 1 is performed. Thus, the proposed authentication scheme L-EAP also ensures message integrity.

4.1 Time, computation, and storage complexity

In addition to the security of the proposed scheme, the L-EAP efficiency is evaluated in terms of Time complexity, storage, and computational complexity.

4.1.1 Time complexity

The bootstrapping time B(T) and communication time C(T) are the important parameters in time complexity estimation. In general, the number of messages exchanged between IoMT entities also the main reason for high time complexity. In the EAP authentication process, the existing LO-Co AP-EAP usually spends more than one EAP request message to select the authentication method. The EAP request message introduces F-bit to select or change the EAP type in a single request message to reduce the time complexity.

$$\text{Time Complexity} = \mathrm{B(T)} + \mathrm{C(T)} \tag{1}$$

$$\text{Time Complexity}_{\text{LO-CoAP-EAP}} = \mathrm{O((k * Re)n)} + \mathrm{O(nm)} \tag{2}$$

$$\text{Time Complexity}_{\text{L-EAP}} = \mathrm{O(kn)} + \mathrm{O(nm)} \tag{3}$$

The bootstrapping time complexity of the proposed work is O(kn), where the value of k represents the number of selected EAP methods. If a first EAP method type is selected, the value of k is one; otherwise, it is more than one. However, frequent re-handshaking in existing work Re is the main reason behind the high value of time complexity in LO-CoAP-EAP. *Re represents the number of handshaking processes. The proposed work attempts to change the security method without initiating the re-handshaking procesF_ using F_Bit*. Moreover, the communication time depends on the number of messages m communicated between IoMT entities.

4.1.2 Computational and storage complexity

The number of encryption/decryption operations, number of signature/verification operations, and the number of random number generation. The proposed scheme focuses on reducing the computational cost of the resource-constrained IoMT devices by computing the secret key on both the IoMT entities individually. It shows a significant reduction in the computational cost of the proposed work. However, the existing work LO-CoAP-EAP separately computes the secret key for secure IoMT communication. Thus, the computational complexity of the proposed work is significantly reduced more than the existing work. A notation of α in equation (5) shows a slight reduction in the computational complexity of the existing work since it uses a session identifier and token empty in the security scheme. Decreasing the number of bytes in the message does not show a huge impact on secure CoAP communication, compared to the number of messages exchanged during mutual authentication.

$$\text{Comp Complexity}_{\text{L-EAP}} = \mathrm{O(n \log n)} \tag{4}$$

$$\text{Comp Complexity}_{\text{LO-CoAP-EAP}} = \mathrm{O(\alpha n)} \tag{5}$$

Table 3 Storage cost of the proposed L-EAP and existing LO-CoAP-EAP

L-EAP			*LO-CoAP-EAP*		
Parameter	*IoMT device*	*Gateway*	*Parameter*	*IoMT device*	*Gateway*
NAI	√	√	NAI	√	√
Nonce 1	√	-	Nonce S	√	-
Nonce 2	-	√	MID	√	-
Token	√	√	Master session key	√	√
Ψ	√	√	The extended master session key	-	√
MID	√	-	Transient session key	√	√
-	-	-	App key	√	√
-	-	-	Network session key	√	√
Total storage cost (bits)	640	512	Total storage cost (bits)	896	768

The storage cost is mainly depending on the number of parameters used for mutual authentication and secure communication process. The storage cost of the proposed scheme is smaller than the existing work due to the lengthy cipher suite with EAP-method type. Avoiding a sending message to IoMT for service change, the proposed work can save a $(k - 1) * 128$ bits using an F-bit field. Thus, the complexity of L-EAP is significantly reduced in IoMT healthcare applications. Table 3 shows that the storage cost of the IoMT device-side is 640 bits, while the storage cost of the server is 896 bits. Similarly, compared to the proposed scheme, the existing scheme has considerable storage costs in terms of 1,024 bits on the client side.

5 Performance evaluation

The proposed L-EAP is implemented by extending the CoAP protocol to demonstrate its performance using the Contiki Cooja network simulator. The IoMT communication process is generally initiated between the client and the server. However, an attacker can disturb the IoMT sensitive health data communication. The mutual authentication scheme is applied to the CoAP to initiate the secure connection between the client and server to overcome this issue. This section illustrates the experimental results of the L-EAP on CoAP (L-EAP-CoAP) and LO-CoAP-EAP (Garcia-Carrillo et al., 2017). The testing is carried out on 30 compatible devices working under the control of the Contiki OS for 180 seconds. This work simulates the proposed and existing works in a 100×100 m^2 area, where 28 client nodes, one server, and one border router are deployed. The communication range of each node is set to 50m. The message transmission interval is 10 sec, and the packet size is 127 bytes.

5.1 Simulation results

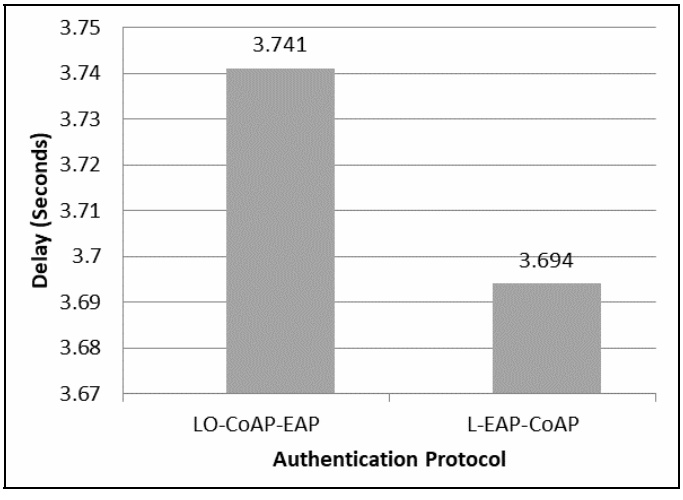
The performance analysis is executed in terms of performance metrics such as delay, energy consumption, and message size overhead.

- *Delay:* the delay is defined as the time taken by a client node for mutual authentication and secure IoMT communication with the server.
- *Energy consumption:* it is the amount of joules consumed to deliver the data from source to destination.
- *Message size overhead:* it is defined as the total length of the header in the packets transmitted, and it is measured in bytes.

5.1.1 Delay

The number of IoMT sensor nodes is taken as 30 to analyse the performance of L-EAP-CoAP. Figure 5 illustrates the performance of L-EAP-CoAP and LO-CoAP-EAP in terms of delay. From Figure 5, the delay of L-EAP-CoAP decreases than LO-CoAP-EAP over the same network area. For 30-node topology, the L-EAP-CoAP reduces the delay of 0.047 seconds, compared to the LO-CoAP-EAP. In most of the existing works, the CoAP messages that need no encryption can be exchanged only after performing the mutual authentication between the IoMT client node and server, even immediate to the communication of CoAP messages with encryption between the same pair of nodes. To avoid this unnecessary authentication and encryption, the proposed L-EAP-CoAP introduces epoch-based service change and reduces the entire communication delay. As the proposed work performs the key generation as a part of the authentication phase, the L-EAP-CoAP effectively utilises the constrained resources in IoMT devices. For instance, the L-EAP-CoAP communicates with the server in 3.694 seconds, whereas LO-CoAP-EAP takes 3.741 seconds.

Figure 5 Delay under 30-node topology

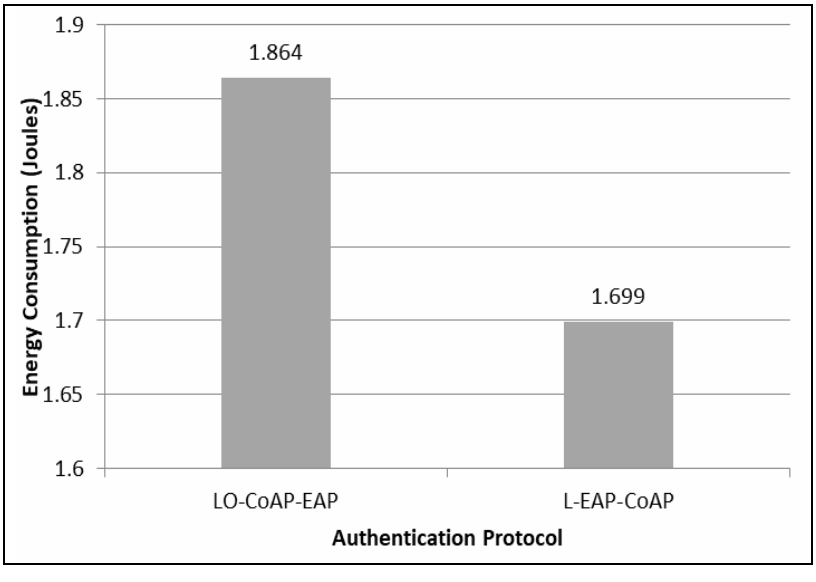


5.1.2 Energy consumption

Figure 6 demonstrates the energy consumption for both L-EAP-CoAP and LO-CoAP-EAP. In the network with 30 IoMT sensors, the L-EAP-CoAP results in low energy consumption, whereas the LO-CoAP-EAP corresponds to high energy

consumption. In such scenarios, the main reason behind the energy consumption difference is malicious activity detection. Both the works exploit AES for encryption, and the generated words using the original AES key are related to each other. The attacker can deduce the overall key if any word is traceable. It tends to unnecessary energy loss at IoMT devices. Besides, the XOR operation with zero produces the same result, and it opens a space for an attacker to trace the secret key. As the proposed methodology implements the idea of Sequential Round Constant and reduces the malicious interruption in IoMT communication and energy consumption. For instance, the L-EAP-CoAP consumes 1.699 joules in 30-node topology, and in the same scenario, the LO-CoAP-EAP consumes 1.864 joules.

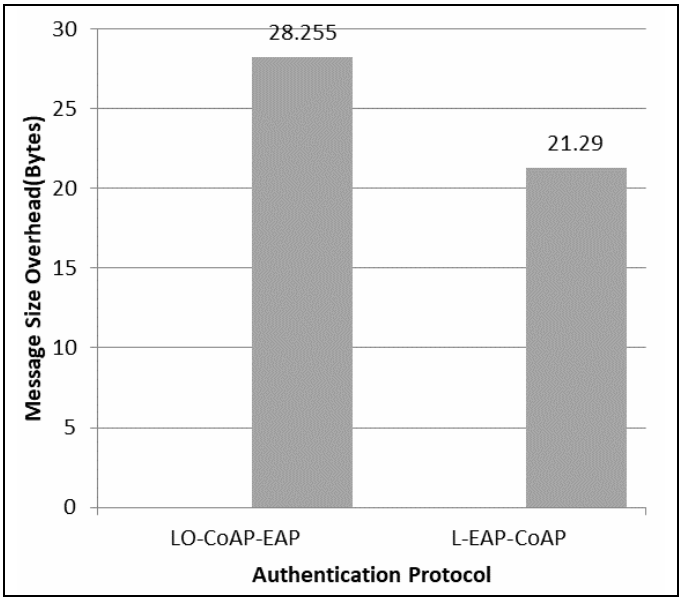
Figure 6 Energy consumption of communication under 30-node topology



5.1.3 Message size overhead

From the simulation results, the message size overhead is observed and plotted in Figure 7 for L-EAP-CoAP and LO-CoAP-EAP under 30-node topology. The message size overhead is measured as the size of messages in bytes. Compared to the L-EAP-CoAP, the message size overhead of LO-CoAP-EAP work is increased. In existing work, the number of messages exchanged for confirming EAP is high, and the size of the EAP PSK field increases the message size overhead than the proposed work. However, the LO-CoAP-EAP increases the number of messages to confirm the communication service and message size overhead in contrast with the proposed L-EAP-CoAP, when the network nodes are 30. For instance, the LO-CoAP-EAP utilises 28.255 bytes for communication, whereas the L-EAP-CoAP utilises 21.29 bytes in the same scenario of 30-node topology.

Figure 7 Message size overhead of communication under 30-node topology



6 Conclusions

The proposed work attempts to design a mutual authentication scheme in IoMT for various communication services in healthcare. Most of the existing works lack in dealing with the dynamically changing security services based on the priority. A lightweight authentication mechanism is implemented to support the modified EAP model and dynamically change the security service to overcome this issue. The proposed L-EAP scheme exploits a one-bit epoch field in the EAP message header to change the security service from supporting both the authentication and data confidentiality to just integrity as per the application requirements. It avoids frequent re-handshaking of a particular IoMT client connecting to the server and makes the proposed mutual authentication scheme a lightweight, customised security scheme on the application layer. The key generation process is performed as a part of the authentication phase, and the proposed authentication scheme can effectively utilise the constrained resources in IoMT devices. The proposed L-EAP performance on CoAP is evaluated using the Cooja simulator and compared with the LO-CoAP-EAP in 30 node topology. The proposed L-EAP-CoAP delivers the CoAP messages by consuming only 1.699 joules without compromising the network security, whereas the LO-CoAP-EAP spends 1.864 joules.

References

Abdulghani, H.A., Nijdam, N.A., Collen, A. and Konstantas, D. (2019) 'A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective', *Symmetry*, Vol. 11, No. 6, p.774.

Abdullah, D., Rahim, R., Siahaan, A.P.U., Ulva, AF, Fitri, Z., Malahayati, M. and Harun, H. (2018) 'Super-encryption cryptography with IDEA and WAKE algorithm', *J. Phys. Conf. Ser.*, Vol. 1019, No. 1, pp.1–7.

Aboba, B., Simon, D. and Eronen, P. (2016) *Extensible Authentication Protocol (EAP) Key Management Framework* [online] https://tools.ietf.org/html/rfc5247 (accessed July 2020).

Al-Zubaidie, M., Zhang, Z. and Zhang, J. (2019) *Efficient and Secure ECDSA Algorithm and Its Applications: A Survey*, arXiv preprint arXiv:1902.10313.

Asghari, P., Rahmani, A.M. and Javadi. H.H.S. (2019) 'Internet of things applications: a systematic review', *Computer Networks*, Vol. 148, pp.241–261.

Benvenuto, C.J. (2012) 'Galois field in cryptography', *University of Washington*, Vol. 1, No. 1, pp.1–11.

Bersani, F. and Tschofenig, H. (2007) *RFC 4764 – The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method*, Tech. rep., IETF Network Working Group, 2007.

Clancy, T. and Tschofenig, H. (2009) *Extensible Authentication Protocol-Generalized Pre-Shared Key (EAP-GPSK) Method*, RFC 5433.

Dhillon, P.K. and Kalra, S. (2017) 'A lightweight biometrics based remote user authentication scheme for IoT services', *Journal of Information Security and Applications*, Vol. 34, pp.255–270.

Gao, C., Lv, S., Wei, Y., Wang, Z., Liu, Z. and Cheng, X. (2018) 'M-SSE: an effective searchable symmetric encryption with enhanced security for mobile devices', *IEEE Access*, Vol. 6, pp.38860–38869.

Garcia-Carrillo, D., Marin-Lopez, R., Kandasamy, A. and Pelov, A. (2017) 'A CoAP-based network access authentication service for low-power wide area networks: LO-CoAP-EAP', *Sensors*, Vol. 17, No. 11, p.2646.

Hassan, W.H. (2019) 'Current research on internet of things (IoT) security: a survey', *Computer Networks*, Vol. 148, pp.283–294.

Housley, R. and Aboba, B. (2016) *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management* [online] http://www.rfc-editor.org/info/rfc4962 (accessed July 2020).

Jiang, Q., Zeadally, S., Ma, J. and He, D. (2017) 'Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks', *IEEE Access*, Vol. 5, No. C, pp.3376–3392.

Kabalci, Y., Kabalci, E., Padmanaban S., Holm-Nielsen, J.B. and Blaabjerg. F. (2019) 'Internet of things applications as energy internet in smart grids and smart environments', *Electronics*, Vol. 8, No. 9, pp.1–16.

Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A.K. and Choo, K.K.R. (2018) 'A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments', *J. Netw. Comput. Appl.*, Vol. 103, pp.194–204.

Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M. and Choo, K.K.R. (2017) 'An enhanced 1-round authentication protocol for wireless body area networks with user anonymity'. *Comput. Electr. Eng.*, Vol. 61, pp.238–249.

Novelan, M.S., Husein, A.M., Harahap, M. and Aisyah, S. (2018) 'SMS security system on mobile devices using tiny encryption algorithm', *IOP Conf. Ser. J. Phys. Conf. Ser.*, Vol. 1007, No. 1, p.012037.

Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A. and Brown, J. (2020) 'A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures', *Computers*, Vol. 9, No. 2, p.44.

Panchatcharam, P. and Vivekanandan, S. (2019) 'Internet of things (IoT) in healthcare – smart health and surveillance, architectures, security analysis and data transfer: a review', *International Journal of Software Innovation (IJSI)*, Vol. 7, No. 2, pp.21–40.

Pawlowski, M.P., Jara, A.J. and J. Ogorzalek, M.J. (2015a) 'Compact extensible authentication protocol for the internet of things: enabling scalable and efficient security commissioning', *Mobile Information Systems*, Vol. 2015, pp.1–11.

Pawlowski, M.P., Jara, A.J. and Ogorzalek, M.J. (2015b) 'EAP for IoT: more efficient transport of authentication data – TEPANOM case study', *Proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications Workshops (AINA '15)*, pp.694–699.

Rachmawati, D., Sharif, A. and Budiman, M.A. (2018) 'Hybrid cryptosystem using tiny encryption algorithm and LUC algorithm', *MS&E*, Vol. 300, No. 1, p.012042.

Radovici, A., Rusu, C. and Şerban, R. (2018) 'A survey of IoT security threats and solutions', *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, p.1–5.

Rajesh, S., Paul, V., Menon, V.G. and Khosravi, M.R. (2019) 'A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices', *Symmetry*, Vol. 11, No. 2, p.293.

Ren, W. and Miao, Z. (2010) 'A hybrid encryption algorithm based on DES and RSA in Bluetooth communication', *Proceedings of the 2010 Second International Conference on Modeling, Simulation and Visualization Methods*, pp.221–225.

Salemi, H., Rostami, H., Talatian-Azad, S. and Khosravi, M.R. (2021) 'LEAESN: predicting DDoS attack in healthcare systems based on Lyapunov exponent analysis and echo state neural networks', *Multimedia Tools and Applications*, pp.1–22.

Shelby, Z., Hartke, K. and Bormann, C. (2014) *The Constrained Application Protocol (CoAP)*, Rfc 7252, p.112.

Usman, M., Ahmed, I., Aslam, M.I., Khan, S. and Shah, U.A. (2017) 'SIT: a lightweight encryption algorithm for secure internet of things', *Int. J. Adv. Comput. Sci. Appl.*, Vol. 11, No. 2, pp.1–21.

Wu, F., Li, X., Sangaiah, A.K., Xu, L., Kumari, S., Wu, L. and Shen, J. (2018) 'A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks'. *Futur. Gener. Comput. Syst.*, Vol. 82, pp.727–737.

Wu, F., Xu, L., Kumari, S. and Li, X. (2017) 'An improved and anonymous two-factor authentication protocol for healthcare applications with wireless medical sensor networks', *Multimed. Systems*, Vol. 23, No. 2, pp.195–205.

Wu, X., Khosravi, M.R., Qi, L., Ji, G., Dou, W. and Xu, X. (2020) 'Locally private frequency estimation of physical symptoms for infectious disease analysis in internet of medical things', *Computer Communications*, January, Vol. 162, pp.139–151.

Yu, M., Zhuge, J., Cao, M., Shi, Z. and Jiang, L. (2020) 'A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices', *Future Internet*, Vol. 12, No. 2, p.27.

Zhdanov, O.N. and Sokolov, A.V. (2016) 'Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic', *Far East J. Electron. Commun.*, Vol. 16, pp.573–589.