

JLSAIoMT : Justifiable lightweight and secure mutual authentication scheme for Internet of Medical Things

Shivangi Batra *

Bhawna Narwal †

Amar Kumar Mohapatra §

Department of Information Technology

Indira Gandhi Delhi Technical University for Women (IGDTUW)

Kashmere Gate

Delhi 110006

India

Abstract

With the demographic expansion, healthcare exigencies are increasing invariably, owing to which it is pertinent to provide healthcare services around the corner. The Internet of Medical Things (IoMT) has expedited this concept of rendering expeditious healthcare facilities to medically and geographically isolated patients. These systems empower patients and clinicians to maintain and monitor health records cost-effectively and effortlessly. This IoMT environment involves transmitting, processing, and storing sensitive patient data among the communicating entities. Evaluating and strengthening the security of such integrated and diverse healthcare networks is crucial. This research work elucidates the two most frequent and notable scenarios the first one being clinical isolation where the patient is medically advised to confine himself to healthy individuals and the second scenario is geographic isolation, where the patient is present at a remote location, spatially bound and unable to visit the doctor physically. In both scenarios, the patients are equipped with body sensors, using which the patient data is collected and further exchanged with the medical practitioner to remotely keep track of patient health. The network model for both scenarios is discussed in the upcoming section in detail. Edge and cloud servers have been used to solve latency and storage concerns. The objective of this work is to design a lightweight, mutual authentication scheme for secure data transmission and remote communication. The security strengths of the proposed JLSAIoMT: Justifiable Lightweight and Secure Mutual

* ORCID-ID: 0009-0002-2738-3673

† ORCID-ID: 0000-0003-3849-5566

§ ORCID-ID: 0000-0002-8025-6879

* E-mail: shivangi011phd23@igdtuw.ac.in (Corresponding Author)

† E-mail: bhawnanarwal@igdtuw.ac.in

§ E-mail: akmoahpatra@igdtuw.ac.in

Authentication Scheme for Internet of Medical Things, scheme have been tested using AVISPA simulation and the RoR model. Withal, the environment of Raspbery PI has been used to analyze the execution time of the scheme. Performance parameters have also been provided using the NS2 network simulator. Moreover, the use of biometrics has also been incorporated to enhance the security of JLSAioMT and is found to be more secure against security attacks and cost-effective compared to PSLA2P of Abdussami et al. and other counterpart schemes.

Subject Classification: 68M12, 68M18, 68M25.

Keywords: *Internet of Medical Things (IoMT), Lightweight, Mutual authentication, Security.*

1. Introduction

Technology has made humans rethink and reformulate the tenets of efficacy, efficiency, and effectiveness in every realm of life. From academics to healthcare, technology has transformed and vitalized society profoundly. The healthcare domain is a cardinal integrant of human life, and researchers are unabatingly working in this sector to reinforce medical services using technological advancements. Expanding the horizon of the Internet of Things (IoT) [1] to the healthcare industry enables academicians to recontextualize and subsume the attributes of IoT in the medical environment. These characteristics primarily include connectivity and integrity among the communicating devices, and, in the healthcare ecosystem, sensors, smart gadgets, and wearables are a substantial part of such connecting devices [2]. This connectivity bridges the geographic boundaries of patients and doctors and actualizes remote patient monitoring, extraction, handling, and management of patient data in a sound and secure manner [3].

This digital and technological elevation to the medical sector brings forth the idea of the IoMT. Determinatively, IoMT promulgates the revolutionary and visionary facet of the conventional medical industry and related services. IoMT facilitates medicare amenities in a more accessible, affordable, and manner to the patients with 24x7 availability [4]. Foreby, using wireless devices a customized, comprehensive, adaptive, and engaging environment is created for the patient and his/her family to regularly keep track of their health vitals and check for health updates. Moreover, IoMT effectuates accurate and continuous exchange of patient statistics, exclusive wellness services, and immediate clinical intervention [1-4]. However, healthcare devices have limited resources in terms of memory, processing power, and computational capabilities, making it

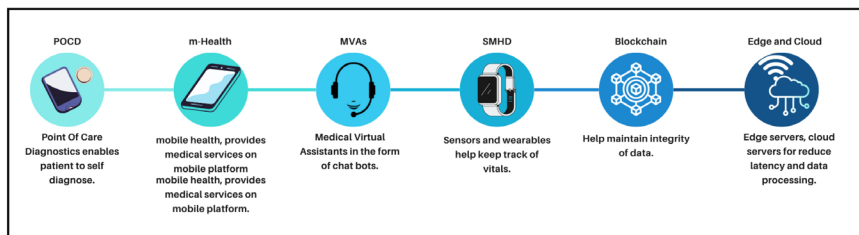


Figure 1

Fundamental components of the IoMT framework

infeasible for the operationally heavy, standard cryptographic protocols to be administered on these devices. Thereby, it is imperative to design a secure and lightweight mutual authentication scheme for such resource-constrained entities, predominantly in the healthcare sector [5]. Taking note of the high-security requirements, statistical analysis, and storage of humongous patient data, utilizing bio-hashing, fog, and edge computing [4], along with cloud technology, is a promising solution. Incorporating patient biometrics through bio-hashing can enhance security and strengthen the process of patient verification and mutual authentication [6]. Cloud provides interoperability, storage, and desired computational capacity for the healthcare network. While, edge computing and fog nodes minimize transmission, processing, and propagation latency [4,7-8]. Fig.1 shows the fundamental components that strengthened and transformed the healthcare industry.

In this paper, two most familiar and allied everyday healthcare cases have been considered, wherein, in the first scenario, the patient is medically isolated, whereas, in the second scenario, the patient is geographically isolated. The patient is quarantined and has no physical contact with the clinician but is monitored concomitantly by the wearables and sensors. Nonetheless, doctors have access to patient data through medical servers. In the second scenario, it is not feasible for the patient to reach the doctor, where the patient needs an emergency intervention but resides remotely. In such a case, local healthcare staff can attach sensors to the patient, and specialized medical practitioners can access the vital readings of the patient through the edge servers. After accessing this real-time patient data, specialized doctors can send the immediate course of action through cloud servers. These scenarios have been methodically discussed in detail in the upcoming sections [4]. The entire concept of being able to exchange, analyze and process sensitive patient data amongst all the healthcare entities and patients' families without physically being in contact with the

medical practitioners and without compromising on the security aspect is the motivation behind this work. Therefore, we propose a secure and lightweight mutual authentication scheme JLSA IoMT, corroborating the IoMT framework. Thereupon it is indispensable to exercise caution over the following security demands of the IoMT network:

- *Mutual Authentication*: All the participating entities must authenticate one another before the commencement of actual communication.
- *Integrity*: Safeguard critical patient data from any illegitimate handling and modification
- *Anonymity*: True identity of the patient must not be revealed, if not there will be a high probability of an adversary taking advantage of the real patient's identity, leading to data inconsistencies and unavoidable data mutations.
- *Forward/Backward Secrecy*: Despite the adversary knowing the session key at a particular instant, it is crucial to protect and preserve the older and upcoming sessions.

1.1 Problem formulation

With the growing digital and contactless era, remote health monitoring and virtual consultation systems have developed leaps and bounds. The IoMT framework has actualized and sustained this far-off communication. It is essential to safeguard vulnerable patient data from active and passive attacks. Thence, it is of prime importance to

- secure the medical servers and cloud servers from the adversary,
- safeguard the patient's privacy and anonymity and achieve untraceability [4],
- be cautious of the resource-constrained working environment.

On account of the aforesaid issues, it is required to design a secure, privacy-preserving, and lightweight mutual authentication scheme for the smart healthcare industry.

1.2 Author's contribution

- A lightweight, mutual authentication scheme JLSA IoMT has been suggested for the IoMT environment.
- The scheme is claimed to counter more security attacks than [4].

- Biohashing has been utilized to perpetuate the security and privacy of the patient.
- Two medical scenarios have been considered namely clinically isolated scenario and geographically isolated scenario.
- AVISPA simulation, RoR model, and informal analysis have been presented to support the strength of the proposed JLSAIoMT scheme.

1.3 *Blueprint of the paper*

Following the introduction, motivation, and contribution of the paper, the subsequent sections comprise of literature review, and a detailed description of network architecture, after which the proposed JLSAIoMT scheme is laid out. The results of the AVISPA simulation along with the RoR model and informal security analysis have been furnished. Comparisons based on cost and security features have also been tabulated along with NS2 simulation in the later sections. Finally, a summary of the work has been put up.

2. Literature review

In 2020, Ghubaish et al. [9] discussed various threats encountered and security requirements in the IoMT domain. They also proposed a security architecture for different stages of data, including data in transit, process, and at rest. While, Garg et al. [10] advocated using blockchain in the IoMT environment and proposed a secure key agreement protocol to support communication between embedded devices, local servers, and cloud servers. Authors of [11], designed a Deep Neural Network (DNN) training model for the IoMT domain and integrated the concept of edge computing for secure and speedy data transmission. RM et al. [12] took notice of the security attacks in the IoMT network and developed an intrusion detection system for the IoMT space using the technology of DNNs. Indumathi et al. [13] drafted a secure and stable, blockchain-based medicare environment for patients. They worked on varied subdomains of the IoMT network and examined the associated security concerns. Then, Almogren et al. [14] suggested the use of fuzzy logic in IoMT space to enhance the efficiency, reliability, and computational power of the network.

In 2021, Sowjanya et al. [15] discovered security vulnerabilities and ameliorated the work of He et al. [16]. Exploiting the properties of ECC, [15] devised a secure and lightweight authentication protocol for the IoMT

framework. In the same year, Shamshad et al. [17] remediated the authentication scheme of Qiu et al. [18] and extended the idea of ECC used by [18], and introduced the concept of encipherment to enhance the security and efficiency of the former protocol. Together in time, Khan et al. [19] proposed a potent and coherent model for detecting the attacks in the IoMT ecosystem utilizing explainable artificial intelligence. In late 2021, Sun et al. [20] suggested a lightweight, mutual authentication scheme for a smart health monitoring model which also supported device mobility. They also suggested a dependable and authentic routing mechanism for device-to-server communication.

In 2022, Singh et al. [21] studied the lesser-explored area of medical imaging security and recommended a scheme for the security and authenticity of medical images. Their scheme was anchored around the concept of region-based medical image watermarking. Further, the authors of [3] stressed the pivotality of artificial intelligence in boosting the industry of Point Of Care Devices (POCD). Then, Chen et al. [1] in the same year harnessed the attributes of an asymmetric cryptosystem and drafted a biometric-based privacy-preserving protocol for authentication of the Internet of Health Things. In 2022, Zhu et al. [22] brought together the features of deep learning and edge computing and delineated the design of an IoMT enabled wearable gadget. Then, researchers [23] integrated the concept of blockchain with edge and fog computing to intensify the area of IoMT and designed a deep-learning model for cancer detection. Lakhan et al. [24] fundamentally focused on latency issues in the health sector. They explored the network optimality and scheduling parameter in IoMT applications. In the same period, Jia et al. [25] proffered two authentication schemes based on ECC and physically unclonable functions. However, their security proof was purely based on informal analysis. Alam et al. [26] analyzed the utility of blockchain in the IoMT environment, over fog computing and presented a comparative study of the two technologies. Then, the artificial intelligence-empowered secure and lightweight scheme was presented by authors of [27] for the IoMT setting. In late 2022, seminal contributions were made by [4] who propounded a cloud and edge-based secure and lightweight mutual authentication scheme for the modern medical system. They used Scyther to test and prove the security of their scheme.

The most recent works of Khan et al. [28] in 2023 posited a fog-cloud framework adopting ensemble learning to analyze the network traffic and associated vulnerabilities in the IoMT network. They used various performance metrics to evaluate their model. Secure and swift processing

of healthcare data was the major concern for the authors of [29]. They aimed to design a model to promptly identify threats and attacks. Then, Vela et al. [30] came up with the idea of home diagnosis through virtual reality. Nonetheless, their suggested framework was computationally heavy. In the same year, Panja et al. [31] enforced fuzzy logic in the IoMT domain, utilizing which they designed a real-time patient monitoring system along with a mobile application. Authors of [32] administered the concept of Support Vector Machines (SVMs) in IoMT in conjunction with deep transfer learning to develop a model to accurately examine the medical scans of the patients. While Gupta et al. [33] worked with heterogeneous IoMT devices using federated learning algorithms.

3. Network model

Biohashing: Biohashing has been used to strengthen the security of the proposed JLSA-IoMT scheme. Any key value known only to the patient is accepted and fed in a randomized algorithm. The patient's fingerprint is used to extract the biometric feature. The authentication code is computed after unifying the obtained seed value with the biometric feature of the patient by hashing [6,34].

Clinically Isolated Environment: Fig. 2 depicts the clinically isolated scenario where the patient is kept in isolation and their vitals are captured through the sensors placed on their body. Sensitive patient data will be sent to the medical servers, from where the data can be accessed by the medical practitioners. Clinicians can thereafter provide necessary medical assistance. The medical server can issue health updates to the patient's family. Patient's family members can use the mobile number and unique pseudo-identity of the patient as a request parameter with the medical server and thereby receive periodic updates through an installed application [4]. Asymmetric encryption can be used for communication between the patient's family and the medical server.

Geographically Isolated Scenario: Fig. 3 portrays the geographically isolated scenario where a patient residing remotely, may at some time need emergency medical guidance and at other times may need specialized health advice from a doctor residing far away from reach of the patient. In such a scenario, a team of locally available healthcare providers may attach the sensors on the patient from where the data can be transmitted to the edge servers for processing, following which cloud servers can be placed to store the patient records. Medical practitioners will be able to access

patient data through cloud servers[4]. To minimize the time lag, edge servers are located in an area close to the data source.

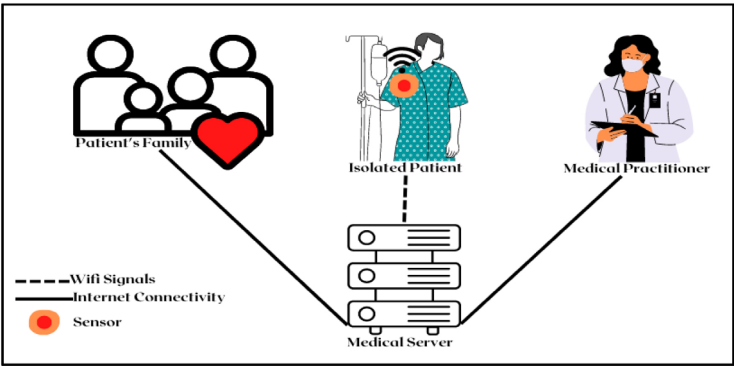


Figure 2
Clinically Isolated Environment [4]

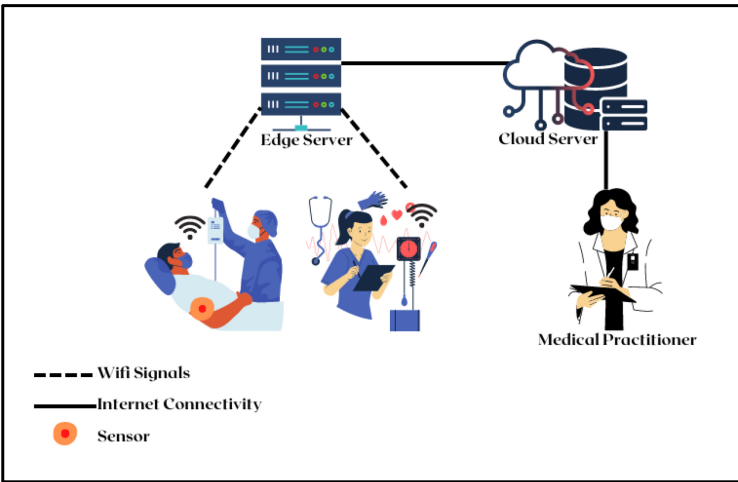


Figure 3
Geographically Isolated Environment [4]

3.1 Threat model

It is worth noting that although medical servers, edge servers, and cloud servers are considered trusted entities the exchange of patient data happens over a public channel. Such transmission increases the chance of the adversary attempting various security attacks over the insecure

channel. A Dolev-Yao (D-Y) threat model [4,35] is adopted in this paper conforming that, the adversary “ Q ”, has control over the entire transmission path and is capable of performing various active and passive attacks. As per the D-Y adversary model, Q can also strive to speculate the identity of the patient or that of the medical practitioner.

4. Clinically isolated environment

Table 1 denotes the symbols used throughout the sections. This scenario consists of four phases: sensor registration with the medical

Table 1
Description Table

Symbols	Description
S	Sensor
MS	Medical Server
MP	Medical Practitioner
EdS	Edge Server
ClS	Cloud Server
S_{ID}	Sensor Identity
MS_{ID}	Masked identity of the Sensor
K_{MS}	Secret key of Medical Server
SK_{SM}	Session key for Sensor and Medical Server
MP_{ID}	Identity of Medical Practitioner
MP_{PWD}	Password of Medical Practitioner
MP_{BIO}	Biometric of Medical Practitioner
MMP_{ID}	Masked Identity of Medical Practitioner
SK_{PS}	Session Key between Medical Practitioner and Medical Server
EdS_{ID}	Identity of the Edge Server
$MEdS$	Masked Identity of Edge Server
SK_{ESCS}	Session key for Edge Server and Cloud Server
K_{ClS}	Secret key of Cloud Server
$r1, r2, r3, r4, r5, R1, R2, R4, R5$	Random nonce
$T1, T2, \dots, T6$	Timestamps
$Hs(), Hb()$	Hash function, Bio-Hash
$\oplus$	XOR operation
$\parallel$	concatenation operation

server, mutual authentication between the sensor and medical server, registration of the medical practitioner with the medical server, and mutual authentication between the medical practitioner and the medical server. Fig. 4 describes the algorithm for the same.

4.1 Sensor registration with the Medical Server

An identity, S_{ID} is assigned to the sensor during its fabrication.

1. $r1$ and MS_{ID} are generated by S. Where, $MS_{ID} = H(S_{ID}||r1)$.
2. MS_{ID} is sent as a registration request parameter to MS.
3. On receiving the request from S, MS generates $r2$ and computes
 - a. $A1 = Hs(MS_{ID}||K_{MS}) \oplus r2$
 - b. $A2 = A1 \oplus Hs(MS_{ID}||K_{MS}||r2)$
4. MS stores $\langle r2, MS_{ID}, A1 \text{ and } A2 \rangle$ and sends $\langle A1, A2 \rangle$ to S
5. S stores $\langle A1, A2, MS_{ID} \rangle$ in its memory.

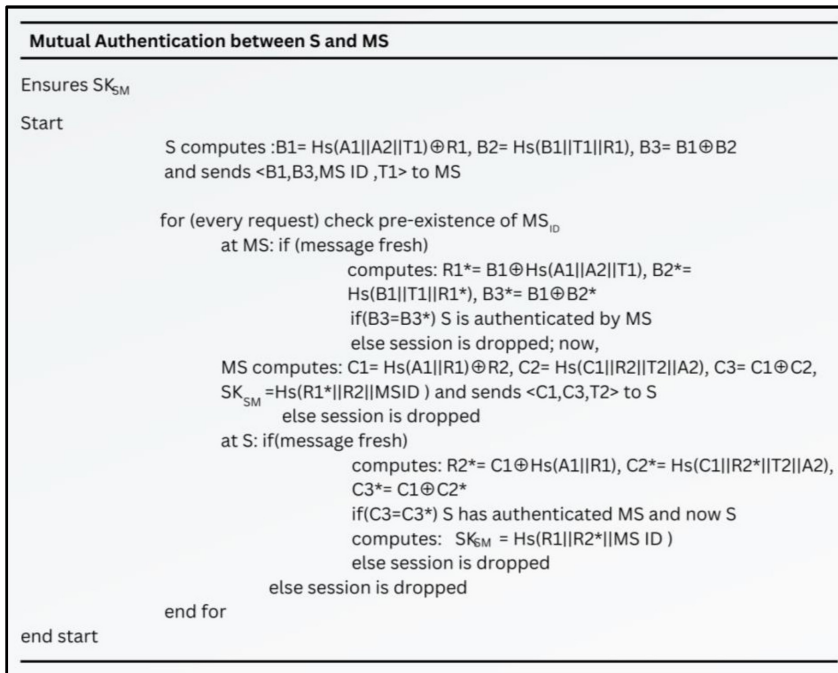


Figure 4

Mutual Authentication between Sensor and Medical Server

4.2 Mutual Authentication between the sensor and Medical Server

1. S generates $R1$, and $T1$ and evaluates
 - a. $B1 = Hs(A1||A2||T1) \oplus R1$
 - b. $B2 = Hs(B1||T1||R1)$
 - c. $B3 = B1 \oplus B2$
2. S sends $\langle B1, B3, MS_{ID}, T1 \rangle$ to MS
3. MS checks the freshness of the received message by calculating the difference between the current timestamp and the received timestamp being less than equal to a fixed threshold. If the message is found fresh then MS evaluates the following:
 - a. $R1^* = B1 \oplus Hs(A1||A2||T1)$
 - b. $B2^* = Hs(B1||T1||R1^*)$
 - c. $B3^* = B1 \oplus B2^*$
4. MS checks if the computed value of $B3$ is same as the received $B3$. If $B3$ does not equal $B3^*$, then the session is aborted. If valid then S is authenticated by MS and now MS generates $R2$, and $T2$ and computes the following:
 - a. $C1 = Hs(A1||r1) \oplus R2$
 - b. $C2 = Hs(C1||R2||T2||A2)$
 - c. $C3 = C1 \oplus C2$
 - d. $SK_{SM} = Hs(R1^*||R2||MS_{ID})$
5. MS sends $\langle C1, C3, T2 \rangle$ to S
6. S checks the freshness of the received message by calculating the difference between the current timestamp and the received timestamp being less than equal to a fixed threshold. If the message is found fresh then S evaluates the following:
 - a. $R2^* = C1 \oplus Hs(A1||R1)$
 - b. $C2^* = Hs(C1||R2^*||T2||A2)$
 - c. $C3^* = C1 \oplus C2^*$
7. S checks if the computed value of $B3$ is same as the received $B3$. If $C3$ does not equal $C3^*$, then the session is aborted. If valid then S has authenticated MS and now S computes $SK_{SM} = Hs(R1||R2^*||MS_{ID})$. This SK_{SM} will be used further for communication.

4.3 Medical Practitioner registration with the Medical Server

1. MP computes $MMP_{ID} = Hs(MP_{ID} || MP_{PWD} || Hb(MP_{BIO}))$ and sends it to MS.
2. On receiving the registration request, MS computes the following:
 - a. $D1 = Hs(MMP_{ID} || K_{MS}) \oplus r2$
 - b. $D2 = D1 \oplus Hs(MMP_{ID} || K_{MS} || r2)$
3. MS saves $\langle D1, D2, MMP_{ID} \rangle$ and sends $\langle D1, D2 \rangle$ to MP
4. MP stores $\langle D1, D2, MMP_{ID} \rangle$ in smart device.

4.4 Mutual Authentication between the Medical Practitioner and Medical Server

MP enters its credentials (MP_{ID} , MP_{PWD} , and MP_{BIO}) and then the value of MMP_{ID} is matched with the stored value. If the MP is verified then the process continues else the session drops due to non-verified practitioner.

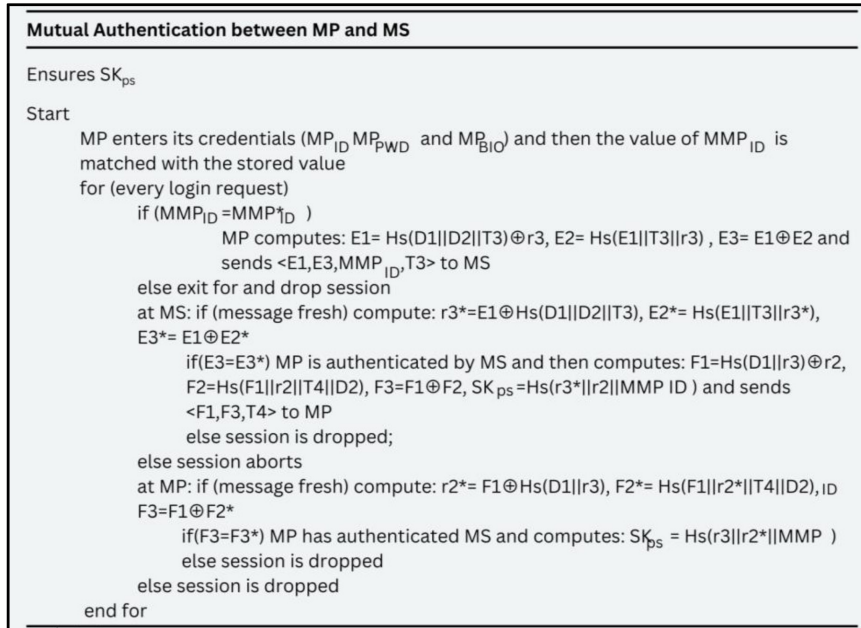


Figure 5

Mutual Authentication between Medical Practitioner and Medical Server

Now, MP generates r_3 , and T_3 and computes

1. $E1 = Hs(D1 || D2 || T3) \oplus r_3$
2. $E2 = Hs(E1 || T3 || r_3)$
3. $E3 = E1 \oplus E2$ and sends $\langle E1, E3, MMP_{ID}, T3 \rangle$ to MS
4. MS checks the freshness of the received message by calculating the difference between the current timestamp and the received timestamp being less than equal to a fixed threshold. If the message is found fresh then MS evaluates the following:
 - a. $r3^* = E1 \oplus Hs(D1 || D2 || T3)$
 - b. $E2^* = Hs(E1 || T3 || r3^*)$
 - c. $E3^* = E1 \oplus E2^*$
5. MS checks if the computed value of $E3$ is same as the received $E3$. If $E3$ does not equal $E3^*$, then the session is aborted. If valid then MP is authenticated by MS and now MS generates $T4$ and computes the following:
 - a. $F1 = Hs(D1 || r3) \oplus r_2$
 - b. $F2 = Hs(F1 || r2 || T4 || D2)$
 - c. $F3 = F1 \oplus F2$
 - d. $SK_{ps} = Hs(r3^* || r2 || MMP_{ID})$ and sends $\langle F1, F3, T4 \rangle$ to MP
6. MP checks the freshness of the received message by calculating the difference between the current timestamp and the received timestamp being less than equal to a fixed threshold. If the message is found fresh then MP evaluates the following:
 - a. $r2^* = F1 \oplus Hs(D1 || r3)$
 - b. $F2^* = Hs(F1 || r2^* || T4 || D2)$
 - c. $F3 = F1 \oplus F2^*$
7. MP checks if the computed value of $F3$ is the same as the received $F3$. If $F3$ does not equal $F3^*$, then the session is aborted. If valid then MP has authenticated MS and now MP computes $SK_{ps} = Hs(r3 || r2^* || MMP_{ID})$.

This SK_{ps} will be used further for communication.

5. Geographically isolated environment

The communication between the sensor and edge server is analogous to that between the sensor and medical server during the clinically isolated scenario. Similarly, the transaction between the medical practitioner and the cloud server is analogous to that between the medical practitioner and the medical server. Registration and mutual authentication between cloud and edge servers are described further. Fig. 5 draws down the algorithm for the same.

5.1 Edge Server registration with Cloud Server

1. EdS generates r_4 and $MEdS = Hs(EdS || r_4)$ and sends MEdS to CIS.
2. CIS on receiving MEdS, generates r_5 and computes $G = Hs(MEdS || K_{CIS}) \oplus r_5$ and saves MEdS and G in its memory and sends G to EdS.
3. EdS saves $\langle MEdS, G \rangle$ in its memory.

5.2 Mutual Authentication between Edge Server and Cloud Server

1. EdS generates R_4 , and T_5 and computes:
 - a. $I1 = Hs(G || T5 || MEdS) \oplus R_4$
 - b. $I2 = Hs(I1 || R4 || T5)$
 - c. $I3 = I1 \oplus I2$ and sends $\langle MEdS, I1, I3, T5 \rangle$ to CIS.
2. CIS checks the freshness of the received message by calculating the difference between the current timestamp and the received timestamp being less than equal to a fixed threshold. If the message is found fresh then CIS evaluates the following:
 - a. $R4^* = I1 \oplus Hs(G || T5 || MEdS)$
 - b. $I2^* = Hs(I1 || R4^* || T5)$
 - c. $I3^* = I1 \oplus I2^*$
3. CIS checks if the computed value of $I3$ is the same as the received $I3$. If $I3$ does not equal $I3^*$, then the session is aborted. If valid then EdS is authenticated by CIS and now CIS generates R_5 , and T_6 and computes the following:
 - a. $J1 = Hs(G || R4) \oplus R_5$
 - b. $J2 = Hs(R_5 || T6 || J1)$
 - c. $J3 = J1 \oplus J2$

- d. $SK_{escs} = Hs(R4^* || R5 || MEdS)$ and sends $\langle J1, J3, T6 \rangle$
4. EdS checks the freshness of the received message by calculating the difference between the current timestamp and the received timestamp being less than equal to a fixed threshold. If the message is found fresh then EdS evaluates the following:
 - a. $R5^* = J1 \oplus Hs(G || R4)$
 - b. $J2^* = Hs(R5^* || T6 || J1)$
 - c. $J3 = J1 \oplus J2^*$
 - d. $SK_{escs} = Hs(R4 || R5^* || MEdS)$ and this SK_{escs} will be used for future communications.

6. RoR MODEL

In this section, RoR model for geographically isolated scenarios is explained. The primary components of RoR model are as follows [4,35]:

1. **Participants:** The two participating entities in communication between Edge Server and Cloud Server are EdS_a and ClS_b . π^{eds} and π^{cls} represent the instances EdS and ClS of Edge and Cloud Server respectively.
2. **Partnering:** For EdS and ClS to be partners, the instances must share a common session key.
3. **Adversary:** Q has absolute control over the transmission channel. Q has the full potential to be a passive listener and is also capable to perform active attacks.
4. **Freshness:** This property holds only if the shared session key has not been revealed to Q .

It is noteworthy that cryptographic primitives such as hash functions are available to all the stakeholders (entities, Q). Next, we list down the most frequently fired queries.

1. **Execute** (π^{eds}, π^{cls}) **Query:** The messages exchanged between EdS and ClS are obtained by Q . Thereby this query increases the chance of an eavesdropping attack.
2. **Send** ($\pi^{eds} / \pi^{cls}, message$) **Query:** Send query is fired to obtain the message sent by the communicating entities and the likelihood of an active attack rises using Send ($\pi^{eds} / \pi^{cls}, message$).

3. **ConstructSK_{PS}** (π^{eds}, π^{cls}) **Query:** This can be used for the construction of the session key between the two participants.
4. **Test** (π^{eds}, π^{cls}) **Query:** Prior to this query a fair coin, FCon is tossed. The outcome of which is stored with **Q**. For the value of FCon = 1, true session key, SK_{ESCS} is returned, whereas, for the value of FCon = 0, **Q** will receive a random string of length same as that of SK_{ESCS}.

Now we describe the **Semantic Security** of the session key: It deals with **Q**'s ability to differentiate between the original SK_{ESCS} and the random string of similar length. **Q** predicts the value of FCon using Test query and if the predicted value is the same as FCon then **Q** wins.

Also, let WINN be the possibility of **Q** to succeed in the game and the advantage, adv of **Q** in successfully breaking the semantic security in polynomial time Pnt be:

$$\text{adv}_Q^{\text{SK}_{\text{ESCS}}}(Pnt) = |2\text{Pr}[\text{WINN}] - 1|$$

Theorem: Considering the advantage of **Q** to obtain SK_{ESCS}, averse to the proposed JLSAIoMT scheme. Send query can be used to intrude the proposed JLSAIoMT scheme, will be denoted as $\text{adv}_Q^{\text{SK}_{\text{ESCS}}}(Pnt) \leq \frac{H_{\text{num}}^2}{|H_{\text{dom}}|} + 2\text{adv}_Q^{\text{SK}_{\text{ESCS}}}(Pnt) \cdot \left(\frac{\text{SndQ}}{|H_{\text{dom}}| \cdot 2^{rb}}\right)$, where SndQ denotes Send queries, H_{num} the number of hash queries, $|H_{\text{dom}}|$ the domain of the hash function, $\text{adv}_Q^{\text{SK}_{\text{ESCS}}}$ the advantage of reconstructing SK_{ESCS} and rb be random bits.

Proof: Games G0, G1, G2, G3, G4, elucidate the security proof of the proposed JLSAIoMT scheme.

1. **Game 0[G0]:** Tracing the real attack model, **Q** might guess the FCon bit before the game which is denoted as:

$$\text{adv}_Q^{\text{JLSAIoMT}}(Pnt) = |2 \cdot \text{Pr}[\text{WINN}] - 1| \quad (1)$$

2. **Game 1[G1]:** It provides the possibility of an eavesdropping attack. A number of Execute queries can be put up by **Q** and then Test queries can be fired to know if the SK_{PS} is true or not. $\text{SK}_{\text{ESCS}} = \text{Hs}(\text{R4} || \text{R5} || \text{MEdS})$, where random nonce are used and MEdS being the masked identity along with the value of SK_{ESCS} is closed under one wayness of the hash function. So,

$$Pr[WINN]G0 = Pr[WINN]G1 \text{ and } Pr[WINN]G1 - Pr[WINN]G0 = 0 \quad (2)$$

3. **Game 2[G2]:** It deals with various active attacks. An attempt is made by $\mathbf{Q}$ to detect the collision in the hash function. Repeated Send queries are fired to learn hash collisions. For $\mathbf{Q}$ to be able to check these collisions in Pnt is nearly impossible as timestamps, private parameters, and random nonces have been incorporated in communicated messages. Also, by the square of approximation of the birthday paradox let us infer the following:

$$|Pr[WINN]G2 - Pr[WINN]G1| \leq \frac{H_{num}^2}{2 \cdot |H_{dom}|} \quad (3)$$

4. **Game 3[G3]:** Here, the delineation of G3 and G2 depends on the sound values being discarded by EdS and ClS, this is symbolized as:

$$|Pr[WINN]G3 - Pr[WINN]G2| \leq \frac{SndQ}{2^{rb}} \quad (4)$$

5. **Game 4[G4]:** $\mathbf{Q}$ tries to construct SKPS, utilizing the Construct query. For $\mathbf{Q}$ to construct SK_{ps} is next to impossible because of the use of random nonces and irreversible property of the hash function. This is indicated by:

$$adv_Q^{JLSAIoMT}(\text{Pnt}) \leq \frac{H_{num}^2}{|H_{dom}|} + 2 \cdot adv_Q^{SK_{ESCS}} \cdot \left(\frac{SndQ}{|H_{dom}| \cdot 2^{rb}} \right) \quad (5)$$

$adv_Q^{JLSAIoMT}(\text{Pnt})$ has minimal probability. The proposed JLSAIoMT scheme is secure under a large hash space and there is an inappreciable chance of breaking the semantic security of the scheme.

7. Informal security analysis

1. **Incorrect Credential Detection:** Whenever the medical practitioner attempts a device login the value of the computed MMP_{ID} is checked with the stored MMP_{ID}. Moreover, biometrics by means of biohashing has been incorporated to provide an additional layer of security. Biometrics is unique to the individual and is closed under one wayness of hash. MMP_{ID} is also closed under the irreversible nature of the hash function.
2. **User Device Lost Attack:** Parameters stored on the smart device are $\langle D1, D2, \text{MMP}_{ID} \rangle$. To compute D1 and D2, it is a prerequisite to know the value of MMP_{ID}. Nevertheless, computing MMP_{ID} in

polynomial time is unfeasible. Further, to determine MMP_{ID} , Q needs to know MP_{ID} , MP_{PWD} , and MP_{BIO} . All these parameters cannot be guessed, replicated, and reproduced due to them being unique to an individual.

3. **Mutual Authentication:** It is achieved by checking the equality of the parameter computed with that received from the communicating entity. $B3$, $C3$, $E3$, $F3$, $I3$, and $J3$ are used to mutually authenticate S and MS , MS and S , MP and MS , MS and MP , EdS and ClS , and ClS and EdS .
4. **Anonymity and Untraceability:** Sensors are placed on the patient and the health data is captured by the sensors and transmitted over the channel. All the sensor communications are done using its masked identity. The masked identity of the sensor has a random nonce appended and is closed under the unidirectional hash function. Moreover, when the family of the patient requests the medical server for the health update of the patient, they also use the pseudo-identity of the patient which will be closed under the property of the hash function. Only masked identities of the participating entities are transmitted over the open network which is hashed and additionally uses random nonce to achieve untraceability.
5. **Man in the Middle Attack:** As parameters required to compute the authenticating parameters are unknown to Q so it will be non-viable for Q to compute the authenticating parameters. Furthermore, the scheme was proven SAFE over AVISPA which also supports that the scheme is resistant to MitM attack.
6. **Impersonation Attack:** Biometrics of the medical practitioner firsthand prevents impersonation attack. Whereas in the case of edge server and cloud server, it is impractical to compute the helping parameter G which is required to compute other transmitted parameters. Similarly for the sensor, it is impossible to compute the helping parameters such as $A1$ and $A2$. Moreover, random nonces and timestamps are used throughout the scheme to maintain uniqueness. Furthermore, the scheme was proven SAFE over AVISPA which also supports that the scheme is resistant to impersonation attacks.
7. **Replay Attack:** The use of secret parameters, random nonces, and timestamps are used throughout the scheme to withstand the replay

attacks. Furthermore, the scheme was proven SAFE over AVISPA which also supports that the scheme is resistant to replay attacks.

8. **Insider Attack:** The one wayness property of hashing, and biohashing helps prevent insider attacks. In the first place, the credentials of the entities are unique to the particular entity but are also computed with the help of random nonces and moreover are masked and are nearly impossible to be computed in polynomial time.
9. **Eavesdropping Attack:** It is well known from the D-Y model that Q has access to the transmitted messages but it is essential to note that it is computationally hard for Q to compute the values of authenticating parameters which are additionally closed under the unidirectional nature of the hash function.
10. **Offline Guessing Attack:** The use of biometrics and biohashing along with hashed (masked) identity and hashed (masked) passwords makes the scheme stand against offline guessing attacks.
11. **Birthday Collision Attack:** The use of hashing and biohashing help prevent collision attack in the proposed JLSAioMT scheme.
12. **Session Verification:** The session Key is used for exchanging data between the communicating parties. The use of random nonce and the prior verification of session keys along with it being closed under the hash function makes session secure.
13. **Forward/Backward Secrecy:** Every entity in clinically isolated and geographically isolated scenarios exchanges dedicated session keys. Random nonces make an integral part of these session keys, making the current session unaffected even if the session key of the previous and upcoming sessions are known to Q.
14. **Parallel Session Attack:** Q might attempt to execute a parallel session attack by replaying the messages. The use of random nonces, timestamps, and secret parameters makes it hard for Q to guess the authenticating parameters which are required to launch a parallel session. Thence the scheme is safe against parallel session attacks.
15. **Session Key Disclosure:** Session keys communicated between participating entities in clinically isolated and geographically isolated scenarios are furnished using random nonces that are fresh at every instant.

8. AVISPA simulation

The proposed JLSAIoMT scheme has been proven SAFE under AVISPA which confirms its security against Man in the Middle attack, replay attacks, and impersonation attacks. Fig. 6, and 7 displays the simulation result for the clinically isolated scenarios and Fig. 8, and 9 presents the same for geographically isolated scenarios. The security is tested over OFMC, CL-AtSe AVISPA backends [36].

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/IoMT.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
```

Figure 6
SAFE over OFMC backend on
AVISPA

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/IoMT.if
GOAL
As Specified
```

Figure 7
SAFE over CLA-AtSe backend on
AVISPA

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/Emergency.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
```

Figure 8
SAFE over OFMC backend on
AVISPA

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/Emergency.if
GOAL
As Specified
```

Figure 9
SAFE over CLA-AtSe backend on
AVISPA

9. Performance analysis

In this section we breakdown and evaluate the storage, communication, and computation costs of the proposed JLSAIoMT scheme and present a comparative analysis based on the security strengths and the involved cost of our scheme with counterpart schemes. All the costs have been presented for the clinically isolated scenario and the cost for the geographically isolated scenario are computed in a similar fashion.

9.1 Storage costs

The stored parameters and associated costs for the entities are presented in Table 2. From [6] it is evaluated that hash function, random nonces, identities, timestamps, ECC multiplication, and encryption/decryption require 160 bits, 128 bits, 160 bits, 32 bits, 320 bits, and 128 bits respectively.

Table 2
Storage Cost

Entities	Stored Parameters	Storage Cost (in bits)
S	$\langle A1, A2, MS_{ID} \rangle$	480
MP	$\langle D1, D2, MMP_{ID} \rangle$	480
MS	$\langle A1, A2, MS_{ID}, D1, D2, MMP_{ID}, r2 \rangle$	1088
MEdS	$\langle MEdS, G \rangle$	320
CIS	$\langle MEdS, G \rangle$	320

9.2 Communication overhead

The communication cost is calculated using the messages transmitted between the entities during the authentication phase and has been tabulated in Table 3.

Table 3
Communication Cost

Communicating Entities	Communication Cost (in bits)
$S \rightarrow MS$	512
$MS \rightarrow S$	352
$MP \rightarrow MS$	512
$MS \rightarrow MP$	352
$EdS \rightarrow CIS$	512
$CIS \rightarrow EdS$	352

9.3 Computation cost

The computation cost for clinically isolated scenarios and geographically isolated scenarios are presented in table 4.

Table 4
Computation Cost

Scenario	Computation Cost
Clinically Isolated Scenario	20 Hs() + 16 XOR operations
Geographically Isolated Scenario	30 Hs() + 24 XOR operations

9.4 Execution time

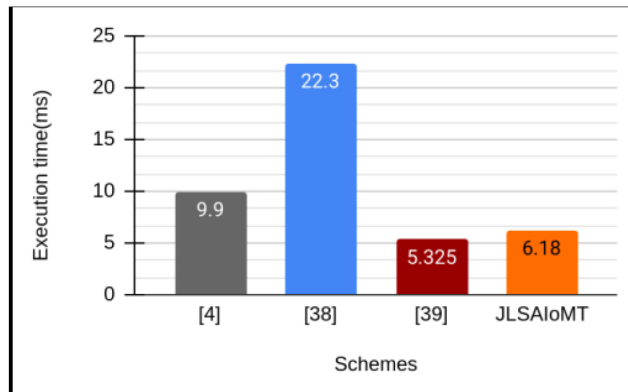
To evaluate the execution time of the proposed JLSAIoMT scheme, Raspberry Pi environment has been replicated from [37]. An environment consisting of Raspberry Pi 4B (2019) model, 64 bit- Ubuntu 20.04.2 LTS operating system with 8GB memory and 1.5 GHz quad-core processor was provided by [37]. Over this environment, the estimated time needed for a hash operation, ECC multiplication, and encryption/decryption was found to be 0.309ms, 2.848ms, and 0.012ms respectively. The time for the XOR operation was found to be negligible. The same has been tabulated in Table 5.

Table 5
Execution Time

Scenario	Execution Time
Clinically Isolated Scenario	$20 \text{ Hs} * 0.309 = 6.18\text{ms}$
Geographically Isolated Scenario	$30 \text{ Hs} * 0.309 = 9.27\text{ms}$

9.5 Comparative analysis

A comparative study of the proposed JLSAIoMT scheme with other counterpart schemes has been provided in Table 6. Additionally, Fig.10 represents a graph of execution time against related schemes. Moreover, Table 7 provides a comparison based on achieved security features.

**Figure 10**

Graph of execution time vs schemes

Table 6

Cost Comparative of proposed JLSAIoMT schemes with equivalent schemes

Schemes	Messages Exchanged	Communication Cost	Computations Performed	Execution Time
[4]	4	2048 bits	32 Hash (Localized Scenario)	9.9ms
[38]	2	1184 bits	17 Hash, 6 ECC Multiplications	22.3ms
[39]	5	2752 bits	17 Hash, 6 Encryption/Decryption	5.325ms
JLSAIoMT	4	1728 bits	20 Hash (Clinically Isolated Scenario)	6.18ms

It is very well inferred that although the communication cost of [38] is lesser than the proposed JLSAIoMT scheme, its execution time is remarkably high when compared to JLSAIoMT. Further, it is clear that [39] has a reduced execution time compared to JLSAIoMT but has an exceeding communication cost. JLSAIoMT has better communication cost, and execution time than that of [4] and is also fulfills a good number of the security requirements than [4,38,39].

Table 7
Comparison based on security features

Security Features Achieved	[4]	[38]	[39]	JLSAIoMT
Incorrect Credential Detection	UnD	UnD	UnD	Y
User Device Lost Attack	Y	UnD	UnD	Y
Mutual Authentication	Y	UnD	Y	Y
Anonymity and Untraceability	Y	UnD	Y	Y
Man in the Middle Attack	Y	Y	Y	Y
Impersonation Attack	Y	UnD	Y	Y
Replay Attack	Y	UnD	Y	Y
Insider Attack	UnD	Y	UnD	Y
Eavesdropping Attack	UnD	UnD	UnD	Y
Offline Guessing Attack	UnD	UnD	UnD	Y
Birthday Collision Attack	UnD	UnD	UnD	Y
Session Verification	Y	UnD	UnD	Y
Forward/Backward Secrecy	Y	UnD	Y	Y
Parallel Session Attack	UnD	UnD	UnD	Y
Session Key Disclosure	Y	Y	Y	Y

* Here, Y, and UnD represents the security features achieved and those undefined respectively.

10. NS2 simulation

Performance parameters have been analyzed using a network simulator. Throughput, end-to-end delay, packet delivery ratio, and jitter are among the parameters considered. An environment similar to [40] has been replicated to run the simulation. A comparative graph against the throughput of compared schemes has been presented in Fig.11. Table 8 defines the ns2 configuration used for the simulation, whereas, Table 9 compares the performance parameters of counterpart schemes. Although [38] has higher Packet Delivery Ratio but has substantial execution time and is resistant to lesser security attacks.

Table 8
NS2 Configuration

Configurations	Description
Operating System	Ubuntu 18.04.2 LTS
Routing Protocol	AODV
Wireless Standard	IEEE 802.15.4
Mobility	Static

Table 9
Comparative Analysis of Performance Parameters

Schemes	Throughput (Kbps)	Delay	Packet delivery ratio	Jitter
[4]	122	0.001	0.928	-0.006
[38]	113.56	0.0034	1	-0.0056
[39]	0.118	-128.28	0.355	-0.0039
JLSAIoMT	122	0.001	0.928	-0.006

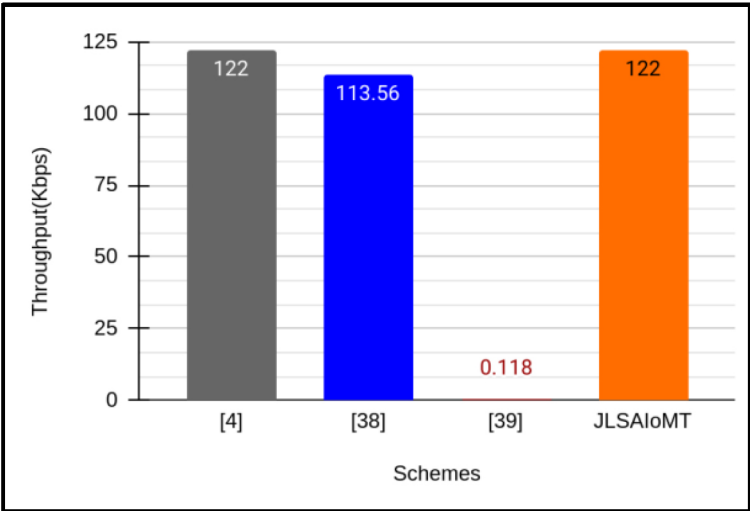


Figure 11
Graph comparing throughput of counterpart schemes

11. Conclusion

This paper provides a secure and lightweight mutual authentication scheme for IoMT environment. In view of the security concerns, biohashing was introduced to preclude any unauthorized access. On analyzing the computation and communication cost it was inferred that our scheme was more cost-effective compared to other counterpart schemes. Forbye, the scheme was found to be better-timed, and robust against a number of active and passive attacks. The security of the session key was tested using the RoR model. The scheme had been tested SAFE over AVISPA tool. The overall performance cost calculated was also improved to comparative schemes. Additionally, the scheme had appreciable values of throughput and other performance parameters. An informal security analysis was also presented to support the security claims.

Acknowledgments

The authors extend their gratitude to ISEA for supporting this work.

Data availability

Not applicable

Author's contribution

All authors have contributed equally in this paper.

Conflicts of interest

The authors declare that there are no conflicts of interest in this paper.

Ethical standard

This article does not contain any studies with human participants performed by any of the authors.

Funding

This research received no specific grant from any funding agency, in the public, commercial or non-profit sectors.

References

- [1] C.-M. Chen, Z. Chen, S. Kumari, and M.-C. Lin, "Lap-ioht: A lightweight authentication protocol for the internet of health things," *Sensors*, vol. 22, no. 14, p. 5401 (2022).
- [2] F. Pelekoudas-Oikonomou, G. Zachos, M. Papaioannou, M. de Ree, J. C. Ribeiro, G. Mantas, and J. Rodriguez, "Blockchain-based security mechanisms for iomt edge networks in iomt-based healthcare monitoring systems," *Sensors*, vol. 22, no. 7, p. 2449 (2022).
- [3] P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. Thipperudraswamy, "Artificial intelligence (ai) and internet of Medical Things (iomt) assisted biomedical systems for intelligent healthcare," *Biosensors*, vol. 12, no. 8, p. 562 (2022).
- [4] M. Abdussami, R. Amin, and S. Vollala, "Provably secured lightweight authenticated key agreement protocol for modern health industry," *AdHoc Networks*, vol. 141, p. 103094 (2023).
- [5] A. Joshi and A. K. Mohapatra, "A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography," *Journal of Information and Optimization Sciences*, vol. 41, no. 7, pp. 1645–1672 (2020).
- [6] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain," *Ieee Access*, vol. 10, pp. 98944–98958 (2022).
- [7] M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog," *IEEE access*, vol. 7, pp. 150936–150948 (2019).
- [8] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "A puf-based mutual authentication scheme for cloud-edges iot systems," *Future Generation Computer Systems*, vol. 101, pp. 246–261 (2019).
- [9] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718 (2020).
- [10] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of Medical Things deployment," *IEEE access*, vol. 8, pp. 95956–95977 (2020).

- [11] I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, and G. N. Nguyen, "An effective training scheme for deep neural network in edge computing enabled internet of Medical Things (iomt) systems," *IEEE Access*, vol. 8, pp. 107112–107123 (2020).
- [12] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekalu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for dnn using hybrid pca-gwo for intrusion detection in iomt architecture," *Computer Communications*, vol. 160, pp. 139–149 (2020).
- [13] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, Z. Wen, and X. Qi, "Block chain based internet of Medical Things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (bc iomt u 6 hcs)," *IEEE Access*, vol. 8, pp. 216856–216872 (2020).
- [14] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of Medical Things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4485–4497 (2020).
- [15] K. Sowjanya, M. Dasgupta, and S. Ray, "Elliptic curve cryptography based authentication scheme for internet of Medical Things," *Journal of Information Security and Applications*, vol. 58, p. 102761 (2021).
- [16] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601 (2016).
- [17] S. Shamshad, M. F. Ayub, K. Mahmood, S. Kumari, S. A. Chaudhry, and C.-M. Chen, "An enhanced scheme for mutual authentication for healthcare services," *Digital Communications and Networks*, vol. 8, no. 2, pp. 150–161 (2022).
- [18] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems," *IEEE access*, vol. 6, pp. 7452–7463 (2017).
- [19] I. A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, and B. S. Ali, "Xsru-iomt: Explainable simple recurrent units for threat detection in internet of Medical Things networks," *Future generation computer systems*, vol. 127, pp. 181–193 (2022).
- [20] J. Sun, F. Khan, J. Li, M. D. Alshehri, R. Alturki, and M. Wedyan, "Mutual authentication scheme for the device-to-server communication in the internet of Medical Things," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15663–15671 (2021).

- [21] P. Singh, K. J. Devi, H. K. Thakkar, and K. Kotecha, "Region-based hybrid medical image watermarking scheme for robust and secured transmission in iomt," *IEEE Access*, vol. 10, pp. 8974–8993 (2022).
- [22] T. Zhu, L. Kuang, J. Daniels, P. Herrero, K. Li, and P. Georgiou, "Iomt-enabled real-time blood glucose prediction with deep learning and edge computing," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 3706–3719 (2022).
- [23] M. U. Nasir, S. Khan, S. Mehmood, M. A. Khan, A.-u. Rahman, and S. O. Hwang, "Iomt-based osteosarcoma cancer detection in histopathology images using transfer learning empowered with blockchain, fog computing, and edge computing," *Sensors*, vol. 22, no. 14, p. 5444 (2022).
- [24] A. Lakhan, A. H. Sodhro, A. Majumdar, P. Khuwuthyakorn, and O. Thinnukool, "A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks," *Sensors*, vol. 22, no. 6, p. 2379 (2022).
- [25] X. Jia, M. Luo, H. Wang, J. Shen, and D. He, "A blockchain-assisted privacy-aware authentication scheme for internet of Medical Things," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21838–21850 (2022).
- [26] S. Alam, M. Shuaib, S. Ahmad, D. N. K. Jayakody, A. Muthanna, S. Bharany, and I. A. Elgendy, "Blockchain-based solutions supporting reliable healthcare for fog computing and internet of Medical Things (iomt) integration," *Sustainability*, vol. 14, no. 22, p. 15312 (2022).
- [27] M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, and J. J. Rodrigues, "Ascp-iomt: Ai-enabled lightweight secure communication protocol for internet of Medical Things," *IEEE Access*, vol. 10, pp. 57990–58004 (2022).
- [28] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. ur Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in iomt," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 10, pp. 10125–10132 (2023).
- [29] S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A fuzzy-based duo-secure multi-modal framework for iomt anomaly detection," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 131–144 (2023).
- [30] L. M. Vela, H. Crandall, T. Lim, F. Zhang, A. Gibbs, A. R. Mitchell, A. Condon, L. M. Diamond, H. Zhang, and B. Sanchez, "Iomt-enabled stress monitoring in a virtual reality environment and at home," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10649–10661 (2023).

- [31] S. Panja, A. K. Chattopadhyay, A. Nag, and J. P. Singh, "Fuzzy-logic-based iomt framework for covid19 patient monitoring," *Computers & Industrial Engineering*, vol. 176, p. 108941 (2023).
- [32] R. O. Ogundokun, S. Misra, A. O. Akinrotimi, and H. Ogul, "Mobilenet-svm: A lightweight deep transfer learning model to diagnose bch scans for iomt-based imaging sensors," *Sensors*, vol. 23, no. 2, p. 656 (2023).
- [33] A. Gupta, S. Misra, N. Pathak, and D. Das, "Fedcare: Federated learning for resource-constrained healthcare devices in iomt system," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1587–1596 (2023).
- [34] H. Abubakar, "Bio-Hash: A fusion of Biometric Security and Hashing" [online document], May 9 (2020). Available: <https://medium.com/dataseries/bio-hash-a-fusion-of-biometric-security-and-hashing-470708876098> [Accessed: February, 2023].
- [35] B. Narwal and A. K. Mohapatra, "Samaka: secure and anonymous mutual authentication and key agreement scheme for wireless body area networks," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 9197–9219 (2021).
- [36] B. Narwal and A. K. Mohapatra, "Seemaka: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks," *Wireless Personal Communications*, vol. 113, no. 4, pp. 1985–2008 (2020).
- [37] S. Yu and K. Park, "Isg-slas: Secure and lightweight authentication and key agreement scheme for industrial smart grid using fuzzy extractor," *Journal of Systems Architecture*, vol. 131, p. 102698 (2022).
- [38] C. M. Kumar, R. Amin, and M. Brindha, "Cyber security and applications,"
- [39] A. P. G. Lopes and P. R. Gondim, "Mutual authentication protocol for d2d communications in a cloud-based e-health system," *Sensors*, vol. 20, no. 7, p. 2072 (2020).
- [40] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Computer methods and programs in biomedicine*, vol. 135, pp. 37–50 (2016).

Received January, 2024