Jan, Mian Ahmad, Wenjing Zhang, Aamir Akbar, Houbing Song, Rahim Khan, and Samia Allaoua Chelloug. "A Hybrid Mutual Authentication Approach for Artificial Intelligence of Medical Things." IEEE Internet of Things Journal, 2023, 1–1. https://doi.org/10.1109/JIOT.2023.3317292.

https://doi.org/10.1109/JIOT.2023.3317292

A Hybrid Mutual Authentication Approach for Artificial Intelligence of Medical Things

Mian Ahmad Jan, Wenjing Zhang, Aamir Akbar, Houbing Song, Rahim Khan, Samia Allaoua Chelloug

***Abstract*—Artificial Intelligence of Medical Things (AIoMT) is a hybrid of the Internet of Medical Things (IoMT) and artificial intelligence to materialize the acquisition of real-time data via the smart wearable devices. Due to a diverse geographical environment of IoMT, secure and reliable communication among these devices is a challenging task that needs to be resolved on priority basis. For this purpose, numerous device-focused authentication approaches have been proposed in the literature, however, the problem still persists. This paper introduces an advanced, secured, and efficient solution for the IoMT by leveraging a lightweight mutual authentication scheme as well as facilitating AI-enabled Big Data analytics and predictive modeling. The proposed approach is specifically designed to establish secured communication between wearable sensing devices and servers within IoMT by exploiting the desirable features of cloud-edge paradigm. In this approach, every device needs to verify whether the requesting wearable device is legitimate or not and this process needs to be carried out prior to the actual communication. Our proposed approach employs a hybrid of Advanced Encryption Standard, i.e., AES 128-bit and Medium Access Control (MAC) for the establishment of secured communication sessions. In addition, the proposed approach utilizes real-time data collection from wearable devices, enabling predictive modeling for the early detection of health anomalies, thereby, enhancing the patient outcomes of a specific disease. This continuously adaptive approach excels in real-time decision-making, promptly alerting healthcare professionals of potential risks. Simulation results have verified that the proposed approach serves an ideal solution for the resource-constrained devices by achieving the expected level of authenticity through minimum possible communication and processing overhead. Additionally, this scheme is prune against well-known security attacks in the AIoMT infrastructures.**

***Index Terms*—AIoMTs, IoMTs, Authentication, Privacy, Wearable Devices, Healthcare, Cloud-Edge paradigm.**

I. Introduction

The Internet of Things (IoT) is improving human lives by enabling regular monitoring and control of diverse activities, particularly in healthcare for critical patient monitoring. The effective use of IoT and artificial intelligence in healthcare ensures timely and appropriate treatment for all patients [1], [2]. As a result, a specialized branch of IoT, the Internet of Medical Things (IoMT), has emerged recently, which is crucial in emergency scenarios, such as intensive care units, to ensure the constant availability of necessary medical services. In IoMT-equipped healthcare facilities, small yet intelligent sensing devices capture and transmit patients data to cloud data centers for assisting healthcare professionals in identifying symptoms for various diseases [3]. IoMTs with AI-enabled sensing and Big Data analytics for cardiovascular activities, ECG, skin resistance and EEG are crucial for early disease detection. They are crucial in emergencies like Intensive Care Units (ICUs) by identifying the symptomatic patients and tracing disease origins using data from wearable devices.

In these networks, each wearable sensing device utilizes a wireless medium to transmit the gathered data to its respective server. Wireless communication is highly susceptible to numerous security and privacy breaches. Therefore, authenticity of the sensing devices and the servers is necessary to ensure the secured transmission of data [4]. Hence, designing a secured and privacy-preserved communication mechanism, specifically in line with the needs of machine-to-machine or device-to-server communication, is required for the applications of IoMT. In the literature, numerous machine-to-machine authentication schemes have been reported to overcome security and privacy issues associated with the IoMT networks. A global assertion and hashing-based authentication mechanism was reported to ensure an ongoing transmission activity among the active devices, i.e., wearables and their associated servers [5]. A lightweight mutual authentication approach that has the ability to establish secured communication sessions with minimal communication and processing overhead was proposed in [6]. A 3-factor authentication scheme using a bi-linear pairing was proposed for a multiserver infrastructure in [7]. However, the proposed scheme is vulnerable to key impersonation and offline guessing attacks. A lightweight mutual authentication approach for healthcare informatics was proposed in [8]. This approach involves three phases to ensure seamingless transmission of data from wearables to remote servers via the intermediate gateways. A MAC-AODV-enabled authentication scheme was presented in [9] to resolve the blackhole attack. Similarly, a remote user-enabled device authentication scheme with embedded biometric identifications was introduced to preserve the security and privacy [10]. However, this approach is highly susceptible to invalid password attacks. A lightweight authentication scheme was developed to secure the transmission of packets among various devices in a Telecare Medical Information System [11]. An anonymous authentication mechanism to prohibit an unauthorized device from accessing data is reported

Mian Ahmad Jan is with the Department of Computer Science, College of Computing and Informatics, University of Sharjah, Sharjah, 27272, United Arab Emirates (e-mail: mjan@sharjah.ac.ae)
Aamir Akbar and Rahim Khan are with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. E-mail: (amirakbar, rahimkhan)@awkum.edu.pk
Wenjing Zhang is with the College of Information Science and Technology, Hebei Agricultural University, China. E-mail: zwjndjs@163.com
Houbing Song is with the College of Engineering and Information Technology, University of Maryland, United States. E-mail: songh@umbc.edu
Samia Allaoua Chelloug is with the Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia Email: Sachelloug@pnu.edu.sa

[12], [13]. A lightweight and anonymous authentication scheme was presented to minimize the possibility of machine learning-enabled attacks in IoMT [14]. Ad hoc on-demand distance vector (AODV)-enabled authentication schemes were reported to safeguard communication sessions [15], [16]. An authentication mechanism using a trust model was reported to address a specific attack i.e., device compromised or device seized, where an adversary acts as an authentic device [17]. Likewise, a forge-enabled authentication mechanism was presented to address various problems associated with the traditional AODV scheme [18], [19]. Fake route request messages (RREQ) were utilized to recognize intruder or adversary devices in the closed proximity. Additionally, a device behavior-enabled routing scheme was presented, where unusual responses are the key to highlight the intruder [20]. Likewise, comprehensive guidelines were devised to ensure the design of machine learning-based cybersecurity for IoT [21]. A deep learning-enabled approach was presented in [22] for the encryption and decryption of images in IoMT. The authors in [28] proposed a secured framework for a communication network using edge computing and machine learning. This framework aims to minimize the detection rate of false attacks within the traffic flows in presence of known and unknown attacks. However, it suffers from network congestion with excessive overhead and QoS degradation.

The aforementioned studies are ideal solutions to address numerous problems, however, the complexity and specificity of applications are the main challenges that need to be addressed. In this paper, a lightweight, secured, and privacy-preserving approach for IoMT is proposed to ensure the establishment of proper communication sessions between various authentic servers and their associated wearable sensing devices. Each message undergoes encryption to protect its contents from potential intruders, providing an extra layer of security to the communication process. Furthermore, our proposed approach facilitates an AI-based real-time data collection and analysis from diverse wearable devices, ensuring data integrity and relevance. Our proposed method effectively manages 'Big Data' and utilizes predictive modeling. By training models on historic data, our proposed approach enables the future health anomaly detection, based on current data, leading to early intervention by significantly improving the patient outcomes. The proposed approach features continuous learning and adaptability. With each new data point, the predictive models are updated and refined, improving accuracy over time and efficiently adapting to evolving health trends. Therefore, our lightweight mutual authentication scheme, combined with secured data collection and predictive modeling, presents a secured, efficient, and advanced solution for IoMTs by enabling a responsive and reliable healthcare solution. The main contributions of this work are as follows:

1) A lightweight, secured, and privacy-preserving technique for the Internet of Medical Things (IoMT) is proposed to mimic the actual environment of smart hospitals.
2) Advanced Encryption Standard (AES-128 bit) and MAC addresses are used to form a hybrid authentication and communication approach for IoMT.
3) Our proposed approach integrates AI with IoMT, i.e., AIoMT, to allow Big Data analytics and predictive modeling for the prediction of health anomalies and improve patients' health outcomes. Therefore, this novel approach excels in real-time analysis and decision-making while continually learning and adapting to new data, ensuring a responsive, efficient, and reliable healthcare.

The remaining paper is organized as follow. In Section II, we have provided a comprehensive description and analysis of our proposed hybrid mutual authentication approach for AIoMT. In Section III, the algorithms of our proposed approach are discussed in detail. In Section IV, the secured data collection and predictive modeling of our proposed approach is discussed. In Section V, experimental setup and simulation results, which were obtained using plausible assumptions, are presented. Finally, concluding remarks of the paper, especially with possible extension measures, have been reported in Section VI.

II. Hybrid Mutual Authentication for Artificial Intelligence of Medical Things

Our proposed mutual authentication approach uses the MAC addresses of active wearable devices C_i and the prospective server devices S_j to guarantee secured transmission of packets between legitimate devices. If an active C_i is eager to initiate a secured transmission session with another device C_{i+1} or S_j, then the authenticity of all these devices needs to be verified. Authenticity is verfied by utilizing the registration mechanism of MAC addresses, preferably in an offline phase. Each C_i is bound to store MAC addresses of every S_j in our IoMT network. Likewise, every S_j is bound to collect and store MAC addresses of numerous C_i, preferably those residing in direct communication range of the member-devices class. An additional class, i.e., non-member-devices, is created to store addresses of those legitimate devices C_i, which are deployed in vicinity of other server devices S_{j+1}. Initialization of every communication session is subject to confirmation of MAC address registration. In other words, intruder devices A_k that are not registered with any S_j are not allowed to initiate a transmission activity either with a server S_j or another active C_i, as soon as our IoMT network becomes operational. The proposed device-to-server mutual authentication approach is divided into three phases, i.e., (i) Offline registration (ii) Authentication and (iii) communication. The generalized structure of the proposed AI and cloud-based authentication for wearable device in IoMT is presented in Fig.1.

A. Offline Registration Phase

In this phase, C_i sends an encrypted request message to the nearest S_j or its own neighbouring device C_{i+1}**iff** it is unable to transmit the message directly to S_j. The MAC address of requesting C_i is one of the components present within the payload of transmitted message, which is encrypted using AES-128. The receiving device, either an S_j or C_{i+1}, decipher this message to retrieve the MAC address of C_i and stores in its memory, i.e., member-devices class, which contains the MAC addresses of other legitimate devices as well. Next, C_{i+1} or S_j generates and transmits an encrypted response message by appending its MAC address within the payload. Additionally, the payload of this message contains successful

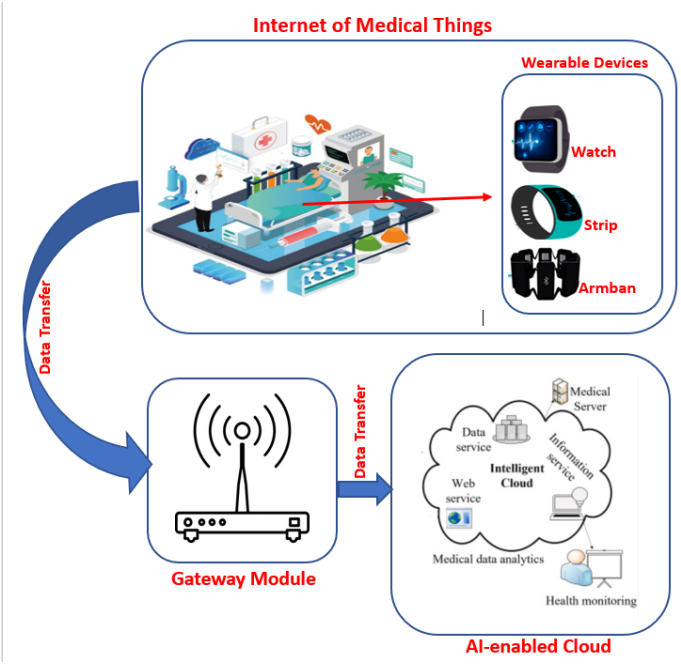

Fig. 1: Generalized structure of the proposed AI and Cloud-based authentication for wearable devices in IoMT

registration information of the device, preferably the requesting C_i present within the class member-device. C_i deciphers the received message and retrieves the MAC address of S_j and stores it in the class of trusted servers. Additionally, every server S_j requires to share its list of member devices C_i with other servers S_{j+1}, which are stored by these non-member yet authentic servers of IoMT. Please note that the entry of intruder devices A_k is not possible in this phase as the underlying IoMT is not yet operational.

To determine a suitable class for a particular requesting device i.e., member-device or non-member-device, localization function is used. The distance between C_i and S_j is computed using Eq. 1.

$$d_{i,j} = \frac{\sqrt{(C_{x_i} - S_{x_j})^2 + (C_{y_i} - S_{y_j})^2}}{(x_i + y_j)} \quad (1)$$

If the distance $d_{i,j}$ is less than the defined threshold value δ, where δ = 0.1, then C_i belongs to the member-device class. Based on Eq. 1, connectivity $M(i,j)$ and distance metric $\Delta(i,j)$ are defined as:

$$M(i,j) = \begin{cases} 1, & i \neq j \\ 0, & otherwise \end{cases} \quad (2)$$

$$\Delta(i,j) = \begin{cases} d_{i,j}, & i \neq j \\ 0, & otherwise \end{cases} \quad (3)$$

The movement model of a device (if applicable) is represented by Eq. 4.

$$V_{i(t)} = \frac{1}{3}\omega v_{i(t-1)} + a(rand) \quad (4)$$

where, ω, a and $rand$ are used to represent inertial weight, acceleration and random function, respectively. The relative localization of a particular C_i along with radial error is represented using

$$Error_{avg} = \frac{\sum_{i=1}^{n} \sqrt{(C_{x_i} - S_{x_j})^2 + (C_{y_i} - S_{y_j})^2}}{n \times R} \times 100\% \quad (5)$$

$$Error_x = \frac{\sum_{i=1}^{n} abs(C_{x_i} - S_{x_j})}{n \times R} \times 100\% \quad (6)$$

Here, n represents the number of devices within the coverage region of a particular S_j and R represents the wireless communication range, respectively. The graphical representation of the underlying registration phase is shown in Fig. 2.

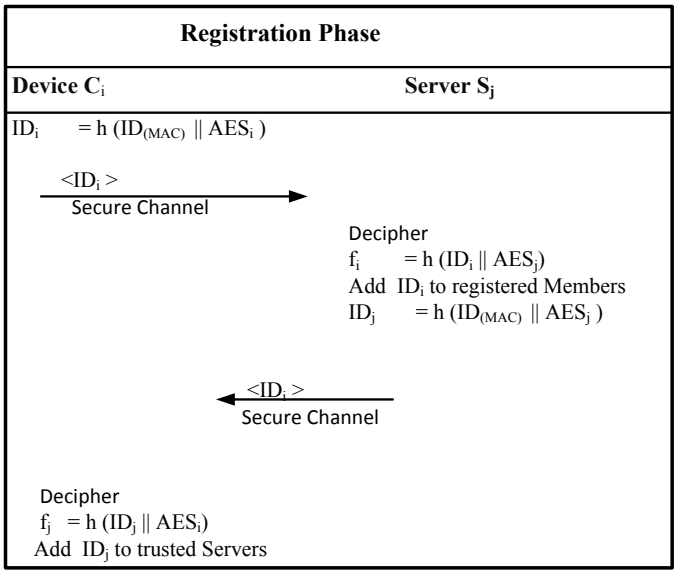

Fig. 2: Offline Registration Phase

B. Authentication Phase

In this phase, if an active device, either an adversary A_k or an authentic wearable C_i, is eager to initiate the data transmission session with the nearest S_j, it generates an encrypted request message. It sends this message to the nearest S_j and waits for the response. S_j confirms legitimacy of C_i by searching the MAC address of the sender in its authentic MAC class, i.e., member-devices class in this case, using Eq. 7.

$$Authentic(C_i) = \begin{cases} \textbf{iff } (\exists_{i=0\ldots m} \mid MAC(C_i) \in MAC_{reg} \\ \textbf{OR} \\ \textbf{iff } (\exists_{i=0\ldots m} \mid MAC(C_i) \in MAC_{NonReg} \end{cases} \quad (7)$$

Here, MAC_{reg} represents the class of MAC addresses that was registered with S_j in the offline registration phase. If a match is found, then it confirms the legitimacy of C_i. The intended S_j allows C_i to start the transmission of data by informing it via an encrypted message that contains the MAC address of S_j in the embedded payload. A detailed description of the entire procedure is reflected in Fig. 3.

Alternatively, if the MAC address of C_i does not match, then S_j assumes that the requesting device is an intruder A_k or an active device of another server that resides in its vicinity. For this purpose, S_j looks for the MAC address entries in

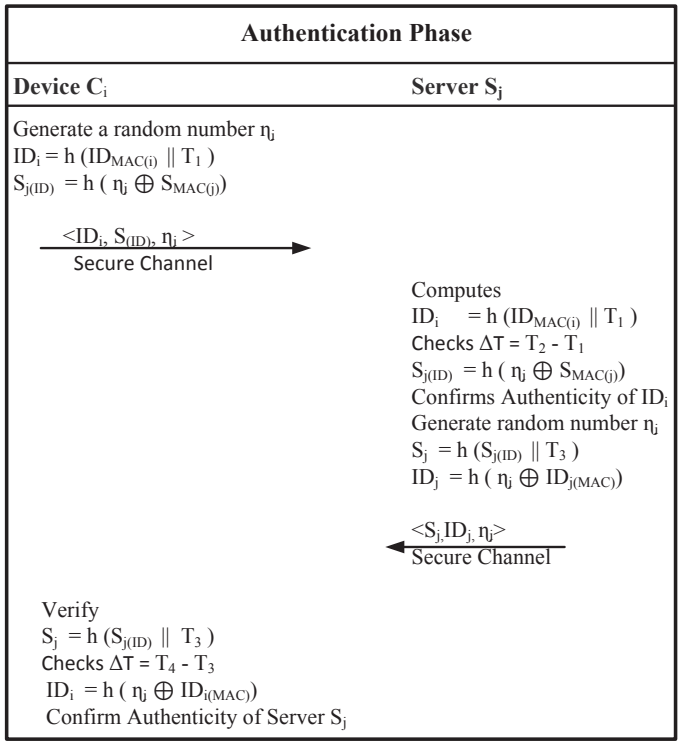

Fig. 3: Successful authentication of a requesting device

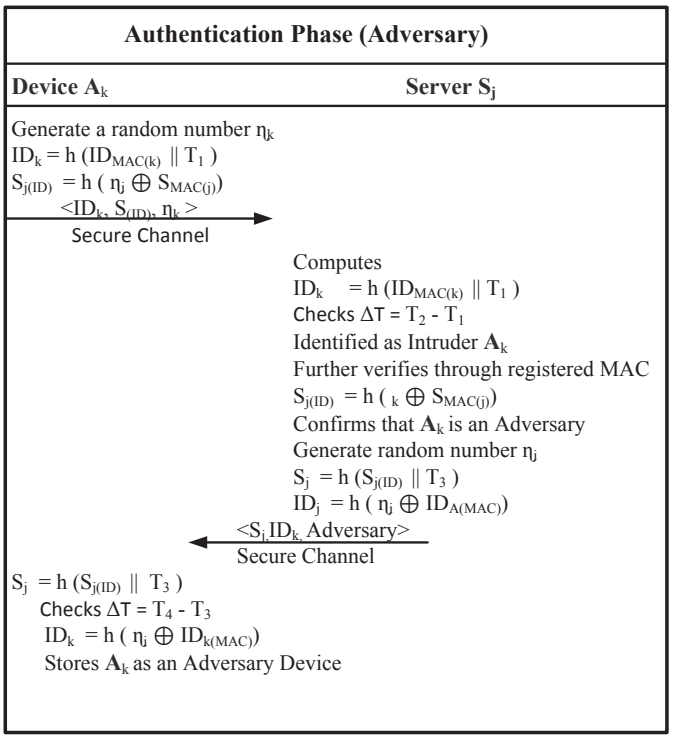

Fig. 4: Successful detection and blacklisting of an Adversary

the non-member-class. If a matching MAC address is found then it confirms authenticity of the requesting C_i, however, the latter is not allowed to initiate data transmission session as it does not belong to the member-class. If the MAC address of the requesting C_i does not have an associated entry in the non-member class, then S_j confirms that this device A_k is an adversary and need to be blacklisted as shown in Eq. 8. This whole process is depicted in Fig. 4.

$$Authentic(C_i) = \begin{cases} \textbf{iff } (\forall_{i=0\ldots m} \mid (MAC(C_i) \notin MAC_{reg}) \\ \textbf{AND} \\ \textbf{iff } (\forall_{i=0\ldots m} \mid (MAC(C_i) \notin MAC_{NonReg}) \end{cases} \tag{8}$$

In addition, S_j transmits an encrypted alarming message to every active C_i. Assume a device *X* sends an encrypted message to the nearest server *Y*, which decrypts this message, retrieves the MAC address from the payload and checks the authenticity of *X* by searching the address in the member-class. If *X* has previously joined and registered its MAC address in the offline registration phase, then its address will be stored in the database of *Y*. In this case, a match will be found and *X* will be permitted to transmit data. Before initiating the communication session, *X* checks the authenticity of *Y* by verifying its MAC address. When the authenticity of both the requesting and receiving devices are confirmed, then a proper communication session is established. Alternatively, if the MAC address was not previously stored or registered with *Y* and vice versa, then the communication sessions are aborted in both the cases and the devices are added to the blacklisted class. *Y* has the capacity to ensure whether the requesting *X* is authentic or not before allowing it to start any transmission activity. To realize this, *Y* verifies the authenticity of *X* by comparing its MAC address with the stored MAC addresses. There are two possible scenarios: (i) *X* is an authentic active device **iff** MAC of *X* is stored in member-devices class, and (ii) *X* is an adversary A_k **iff** a matching value is not found within the stored addresses, i.e., in both member and non-member classes. In the former case, *X* is permitted to start transmission of data, whereas in the latter case, the MAC address of the request initiating device is added to the blacklisted class. Moreover, Y notifies its decision to every neighbouring device using an encrypted message.

Theorem 1: Establishing transmission sessions between active C_i and S_j **iff** both C_i and S_j are trusted and authentic.

Proof: Assume that a formal request for data transmission is initiated by an adversary A_k towards S_j. The latter needs to verify the authenticity of A_k using Eq. 9.

$$Authentic = \textbf{iff } (\exists_{i=0\ldots m`} \mid (MAC(A_k) \in Reg - MAC_{S_j})) \tag{9}$$

Because the requesting device is an adversary, it is not possible that the MAC address of A_k will be found at S_j. Moreover, S_j verifies the authenticity of requesting A_k via searching its MAC address in the non-member-devices class, using Eq. 10.

$$Intruder = \textbf{iff } (\exists_{i`=0\ldots m`} \mid (MAC(A_k) \in NonReg - MAC_{S_j}) \tag{10}$$

Likewise, MAC address of A_k is not stored with S_j, neither in member class nor in non-member class. Therefore, the MAC address of A_k is blacklisted and permission to establish a

communication session is denied using Eq. 11.

$$Intruder = \begin{cases} \textbf{iff } (\forall_{i=0\ldots m} \mid (MAC(A_k) \notin Reg - MAC_{S_j}) \\ \textbf{iff } (\forall_{i`=0\ldots m`} \mid (MAC(A_k) \notin NonReg - MAC_{S_j}) \end{cases} \tag{11}$$

Conversely, if a legitimate device C_i has sent this request to S_j, the latter must follow a similar procedure by matching the MAC address of C_i against the registered MAC addresses, using Eq. 12. A matching MAC address is found because C_i has taken part in the offline registration phase to register its MAC address. As soon as the authenticity of the requesting C_i is verified, then an encrypted 'permission granted' message is sent by S_j. However, a communication session is not initiated yet as C_i must confirm the authenticity of S_j as well, using Eq. 12.

$$Authentic = \textbf{iff } (\exists_{j=0\ldots n} \mid (MAC(S_j) \in Reg - MAC_{C_i})) \tag{12}$$

If a match is found, then the authenticity of S_j is confirmed, and C_i immediately initiates a communication session. Hence, the establishment of a proper data transmission session between an active C_i and S_j is feasible **iff** both C_i and S_j are trusted.

Theorem 2: A request is processed by S_j or C_i **iff** it is authentic or reliable.

Proof: Assume that a request is generated and transmitted by an authentic device C_i, which is intercepted by an adversary A_k located near the concerned S_j. Additionally, A_k may generate its own response message and sent it back to C_i. In this case, C_i verifies the authenticity of S_j by comparing its MAC address against the registered MAC addresses using Eq. 12 and Eq. 13, respectively.

$$Intruder = \textbf{iff } (\forall_{j=0\ldots n} \mid (MAC(S_j) \notin Reg - MAC_{C_i})) \tag{13}$$

The requesting C_i identifies A_k as an adversary and blacklists it. Initially, it is far more difficult for A_k to break the AES-128 encryption algorithm within the stipulated time interval as these devices have very limited processing capabilities. If somehow A_k deciphers the encrypted message and generates a response message similar to the received one, then it will not be processed by C_i. Additionally, the message generated by C_i can be intercepted by A_k and an updated copy of it may be forwarded to S_j. However, updation of this message requires time, which ultimately makes the authenticity of the message questionable. S_j not only verifies the authenticity of the requesting device using Eq. 12, but also utilizes the expected delivery time or propagation delay metrics to ensure the authenticity of the messages from C_i using Eq. 14.

$$P_{delay} = \frac{((C_{x_i} - S_{x_j})^2 + (C_{y_i} - S_{y_j})^2)^{1/2} / (x_i \ + \ y_j)}{T_{speed}} \tag{14}$$

P_{delay} of the updated message is greater than the expected delay of the concerned device C_i. Thus, the message is discarded and an altered encrypted message is sent. Conversely, if the concerned message is processed by S_j, then the response message will be received as expected and C_i can confirm the authenticity of S_j using MAC address and P_{delay} parameter, as shown in Eq. 14.

Hence, a request message is processed by S_j or an authentic C_i **iff** the message is legitimate.

C. Communication Phase

Upon the successful authentication of a requesting wearable C_i and the concerned server S_j, the two parties start data communication. In each communication session, an individual packet transmission time is represented by Eq. 15.

$$T_x = t \times \frac{m}{R_0} \tag{15}$$

Here, *t*, *m*, and R_0 represent the time, packet/block size, and modulation rate, respectively. Furthermore, the average propagation time interval for a particular block is represented by Eq. 16.

$$t_1 = T \times \sum_{i=0}^{v} p^i \tag{16}$$

where, p^i is a channel or medium failure probability function.

Apart from the conventional authentication process, an additional mechanism is needed for those wearables C_i that have the ability to move from the vicinity of one server S_j to another server, e.g. S_{j+1}. This mechanism is extremely important as the majority of IoMT infrastructures support mobile devices. For example, in smart hospitals, when a patient is admitted then he or she is assigned a dedicated bed in a particular ward. It is highly likely that a dedicated server S_j or a cluster head module may be operational in that area, where wearable devices attached to the patient's body are linked with it and communicate directly depending on the circumstances. However, if a patient needs an X-ray or an MRI scan, then he or she need to move to another section where such facilities are available. In this case, it may not be feasible for the wearable devices C_i, which are attached to the patient's body, to communicate or establish a proper communication session with its server S_j. Therefore, these devices C_i need to be registered with the nearest servers with whom C_i can easily establish the communication sessions. In this type of scenario, these wearable devices generate two different messages. The first message is sent to S_j, which is already connected. This message has a description that a particular C_i is moving from the vicinity of S_j and will no longer be a part of the member-devices. The concerned S_j removes all such devices C_i from the member-devices class, whereas these are kept in the registered devices list that contains the MAC addresses of all registered devices. It is important to note that this information is shared in cipher form to preserve the authenticity of messages transmitted from both sides. Furthermore, these devices send request messages, preferably in cipher text form, to the nearest server S_{j+1}, which resides in their communication range. S_{j+1} verifies the authenticity of the requesting devices C_i via the aforementioned approach, i.e., if the MAC addresses of these devices belong to the registered class then they are added, otherwise, the request is denied. This whole process is described in detail as shown in Fig. 5.

These sessions are established by the requesting C_i to transmit its captured data. For communication, these devices are permitted to use any reliable device-to-server communication approach, which are already available from the literature. Furthermore, the communication mechanism should be smart enough to resolve specific scenarios, such as when multiple devices C_i are eager to start the packets' transmission session

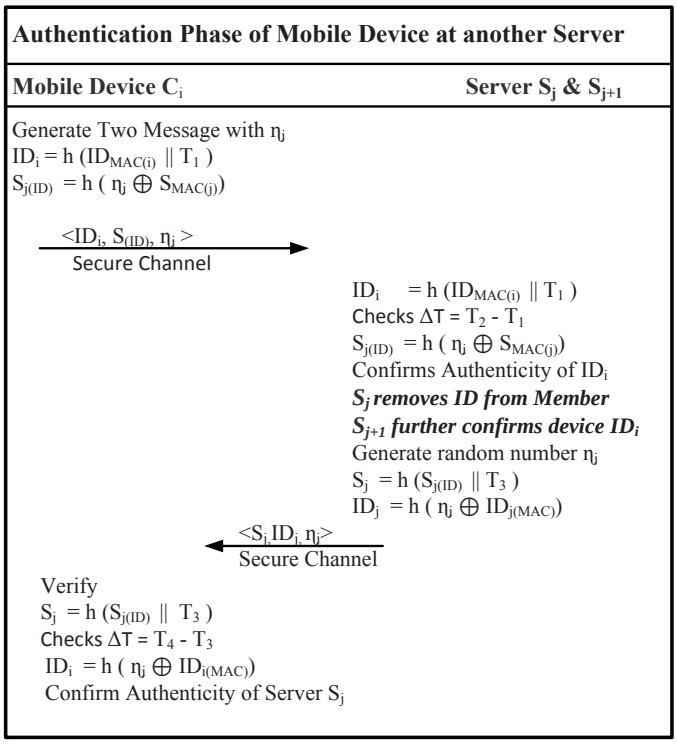

Fig. 5: Verification of the Movable Member-devices in an IoMT Network

with a common server simultaneously. A common problem with concurrent communication is packet collision, and the adopted communication mechanism should have the capacity to either avoid packet collision completely or should be at the minimal possible level.

III. Algorithms for Device-to-Server Mutual Authentication in the IoMT Networks

In this section, dedicated algorithms are presented for every wearable C_i and server devices S_j. These algorithms force C_i and S_j to verify the authenticity of each and every message along with its source, i.e., origin. These algorithms bound C_i and S_j to transmit messages in encrypted form to ensure the security and reliability of data as well as the communicating devices. For this purpose, AES-128 bit encryption algorithm is used to convert plain text into cipher text prior to its transmission in the IoMT networks.

Every C_i is forced to leave a message for the concerned S_j if the former is on the move. However, it is highly likely that an A_k may broadcast such a message for interrupting an ongoing communication session. Therefore, S_j needs to verify the authenticity of these messages prior to any action. As soon as the authenticity of the concerned C_i is verified then an appropriate action is carried out, i.e., this particular device C_i is removed from the member-devices class, however, it is retained in the registered devices class. In continuation of this process, when C_i enters the vicinity of another server S_{j+1}, it needs to send a request message, preferably in the cipher text form, as described above. When the concerned S_{j+1} verifies the authenticity of C_i, then the latter is added to the member-devices class.

Algorithm 1 Security and Privacy-preserved algorithm for Server S_j in the IoMT networks

Require: Member-device C_i sends a communication session establishment request
Ensure: Permitted or Denied
$NonMemberDevices \leftarrow$ Zero
$MemberDevices \leftarrow$ Zero
$Msg_{cp} \leftarrow$ "null"
$BlacklistedorAdversary \leftarrow 0$
$C_i \leftarrow$ Device $\in$ IoMT
$S_j \leftarrow$ Server $\in$ IoMT
for $\forall_{i=0...m}\ C_i \in IoMT$ **do**
  Transmit Msg_{cp} to S_j
  if MAC ($C_i \in MemberDevices$) **then**
    C_i is authentic
    Permission Granted
  elseif MAC address ($C_i \in NonMemberDevices$) **then**
    C_i is authentic
    Permission is denied
  elseif MAC address ($C_i \notin MemberDevices \& \notin NonMemberDevices$) **then**
    C_i is an Adversary
    C_i is blacklist
  end if
end for
return Legitimate and Adversary Devices

Algorithm 2 Security and Privacy-preserved algorithm for legitimate device in the IoMT Networks

Require: Server S_j sends a permission-granted message
Ensure: Authentic or Blacklisted
$RegServer \leftarrow$ Zero
$Msg_{cp} \leftarrow$ "null"
$Blacklist \leftarrow 0$
$C_i \leftarrow$ Device $\in$ IoMT
$S_j \leftarrow$ Server $\in$ IoMT
for $\forall_{j=0...m}\ S_j \in IoMT$ **do**
  Send Msg_{cp} to Device C_i
  if MAC ($S_j \in RegServer$) **then**
    S_j is authentic
    Communication session is initiated
  elseif MAC address ($S_j \notin RegServer$) **then**
    S_j is an Adversary
    S_j is blacklisted
    Communication session is aborted
  end if structure
end for loop
return Authentic and Blacklisted Server Modules

IV. Secure Data Collection and Predictive Modeling

Upon successful authentication and authorization of wearable devices from their concerned servers, our proposed scheme facilitates secure and real-time data collection. This helps with the continuous monitoring of patients' health status, facilitat-

Algorithm 3 Authentication algorithm for server S_j to verify authenticity of the mobile devices in the IoMT networks

Require: Member-device C_i sends a Leave Message to the Concerned Server

Ensure: Member Status Terminated or Identifies as Adversary

$NonMemberDevices \leftarrow$ Zero
$MemberDevices \leftarrow$ Zero
$Msg_{cp} \leftarrow$ "null"
$BlacklistedorAdversary \leftarrow 0$
$C_i \leftarrow$ Device $\in$ IoMT
$S_j \leftarrow$ Server $\in$ IoMT
for $\forall_{i=0...m}\ C_i \in IoMT$ **do**
    Decipher the Transmitted Msg_{cp} to Server S_j
    if MAC ($C_i \in MemberDevices$) **then**
        C_i is authentic
        Remove from Member-devices Class
    elseif MAC address ($C_i \in NonMemberDevices$) **then**
        C_i is authentic
        Action not Required
    elseif MAC address ($C_i \notin MemberDevices$) &&($C_i \notin NonMemberDevices$) **then**
        C_i is an Adversary
        C_i is blacklist
    end if
end for
return Legitimate and Adversary Devices

ing prompt intervention in case of any detected anomalies. Considering n wearable devices, where a device C_i sends its data securely to a server S_j in the IoMT, is mathematically represented as follows:

$$X_j = \bigcup i = 1^n x_{C_i} \tag{17}$$

The collected data X_j at the server S_j, obtained from various devices including C_i, is utilized to train a predictive model based on neural networks, enabling data analysis and pattern recognition. A dataset X_j consisting of input features set $F^{in} = \{F^1, F^2, F^3, \cdots, F^k\}$ and corresponding target variables F^T. Therefore, by training neural networks on several medical servers and on a large volume of historical data, the predictive model learns complex patterns and relationships within the data and helps to make accurate predictions regarding potential health anomalies based on the current data inputs.

Once the data has been securely collected, our proposed scheme facilitates the detection of anomalous patterns in the collected data. This is achieved through the utilization of deep learning algorithms, such as deep autoencoders and recurrent neural networks (RNNs). Deep autoencoders are trained to accurately reconstruct the input data, learning to encode the normal patterns in a compressed latent space representation. Anomalies, which deviate from these learned patterns, lead to higher reconstruction errors [25]. Similarly, by training an RNN on normal data sequences, it can capture the temporal dynamics and identify deviations from the learned patterns as anomalies [26].

Furthermore, variations in data quality, missing values, and imbalances are critical considerations that need to be taken into account. In addition to enabling secure, real-time, and diverse data collection from wearable devices, the proposed scheme incorporates data preprocessing techniques such as data cleaning, normalization, and imputation to address missing values. These challenges can arise due to differences in device accuracy, signal noise, data transmission issues, and variations in patient conditions. Moreover, techniques such as oversampling or undersampling can be used to address class imbalances, which ensures a balanced representation of different health conditions in the collected data [27]. Oversampling increases the number of instances in the minority class, either by duplicating instances or generating synthetic data points. This improves the predictive model's ability to classify instances from the minority class accurately. Conversely, undersampling reduces the number of instances in the majority class, creating a more balanced representation of different health conditions. By reducing the dominance of the majority class, the predictive model becomes less biased and can capture the patterns of the minority class more effectively.

V. Simulation Results and Discussion

In this section, a detailed comparison of the proposed mutual authentication with the existing approaches is made in terms of numerous performance metrics such as computational and communication overheads, end-to-end delay, average packet loss ratio, and residual energy etc. These algorithms were implemented using an open source platform, i.e., OMNET++. The power consumption models of transceivers along with on-board battery were similar for C_i and S_j. Likewise, similar topological structures such as random-top, graph-enabled topology, random-center and tree-based topologies are used, where maximum possibility of the adversary A_k are ensured. We have assumed that an active wearable C_i communicates directly with an S_j only if it is deployed in the coverage region of the Xbee module. Various parameters that are utilized in the proposed simulation setup are given in Table I.

A. Computational Overhead

In Table II, a comparison of computational overhead for our proposed device-to-server authentication and field-proven approaches is presented, which clearly shows that our approach has the lowest computational cost as compared to the existing approaches. The parameters T_h and T_{XOR} are used to depict the processing time of a hash function and XOR operation respectively, whereas, T_{ran} is used to represent random nonce. The computational cost of T_{ran} is almost negligible, however, it is is quite high in case of T_h. The analytical results presented in Table II show that the proposed authentication approach is an ideal solution for the IoMT networks.

B. Communication Overhead

To evaluate and compare the communication overhead of our proposed device-to-server authentication and existing approaches, we have considered only those messages from offline

TABLE I: Simulation Setup

Parameters	values
Deployed Region of IoMT	700m × 700m
Devices C_i	50, 100, 200, 300, 500, 1000
Servers S_j	five
Capacity of on-board Battery (E_s)	52000 mAh
Residual Energy (E_r)	E_s-E_{curr}
Power Consumption of the Transmitter (P_{T_x})	91.4 mW
Channel Delay (Ch_{delay})	12 milliseconds
Power Consumed by Receiving Module (P_{R_x})	59.1 mW
Power Consumption (Idle Mode)	1.27 mW
Power Consumption (Sleep Mode)	15.4 μW
Transceiver Energy (Idle) (T_i)	1 mW
Coverage Range (T_r)	250m
Receiving Power Threshold (RTS_n)	1024 bits
Packet Size	127 bytes
Hop Count (H_c) of S_j	0
Initial H_c of C_i	∞
Intruder devices A_k	5-10
Maximum distance between C_i and S_j	240m
Sampling Rate	15 seconds

TABLE II: Comparison of our device-to-server authentication and Field-proven approaches for computational overhead

Approaches	**Client/Wearable Messages**	**Device-Side Messages**	**Server-Side Messages**	**Total Messages & Overhead**
Proposed Authentication Approach	$2T_h$	-	$2T_h + 4T_{RAN}$	$4T_h + 4T_{RAN}$
Mian et al. [6]	$2T_h + 2T_{XOR}$	-	$2T_h + 2T_{XOR}$	$4T_h + 4T_{XOR}$
Abdelshafy et al. [15]	$5T_h + 5T_{XOR}$	$2T_h + 1T_{XOR}$	$2T_h + 6T_{XOR}$	$6t_h + 11T_{XOR}$
Gupta et al. [24]	$7T_h + 4T_{XOR}$	$4T_h + 4T_{XOR}$	$5T_h + 3T_{XOR}$	$16T_h + 11T_{XOR}$
Makhalouf et al. [16]	-	$2T_h + 6T_{XOR}$	$7T_h + 7T_{XOR}$	$9T_h + 13T_{XOR}$
Hasan et al. [23]	$2T_h + 6T_{XOR}$	$2T_h + 5T_{XOR}$	$3T_h + 3T_{XOR}$	$7T_h + 14T_{XOR}$
Liu et al. [17]	-	$2T_h + 2T_{XOR}$	$1T_h + 2T_{XOR}$	$3T_h + 4T_{XOR}$

registration (if required) and communication phases, which are mandatory for the establishment of a secured communication session between C_i and S_j. The computational cost analysis presented in Table III shows the exceptional performance of our proposed mutual authentication approach against its rival approaches. Our approach has the lowest possible communication overhead as compared to the field-proven approaches.

TABLE III: Comparison of our device-to-server authentication and Field-proven approaches for communication overhead

Approaches	Number of Messages	Bits
Proposed Scheme	4	4,096
Gupta et al. [24]	5	3,038
Makhalouf et al. [16]	5	6,144
Abdelshafy et al. [15]	5	24,546
Liu et al. [17]	60	30,620
Hasan et al. [23]	6	32,000

C. Security and Privacy Analysis

In this section, a comprehensive comparison of our device-to-server authentication is made against the field-proven approaches. Various IoMT scenarios, where C_i and S_j have used a similar authentication scheme, were tested against possible intruder attacks, and we concluded that our proposed approach is not susceptible to these attacks as shown in Table IV. The proposed model is tested by launching various types of intruder attacks against C_i and S_j, respectively. Furthermore, multiple intruder attacks were launch simultaneously and the proposed approach has shown convincing results.

D. End-to-End Delay

The proposed authentication approach has the ability to guarantee the minimal possible value for end-to-end delay while transmitting a packet from source to intended destination, i.e., from C_i to S_j and vice versa. Fig. 6 shows that the proposed approach has the least possible effects on the wireless communication between source and destination devices in the IoMT networks. While performing simulation, we have observed that end-to-end delay metric is highly effected if security measure is susceptible to numerous possible intruder attacks i.e., man-in-the-middle and black-hole attacks.

E. Average Packet Delivery Ratio

The packet delivery ratio is the ratio of generated and successfully delivered packets in the IoMT networks. An authentication scheme is considered reliable if it does not affect various network performance metrics such as packet delivery ratio, throughput, etc. Fig. 7 shows that the proposed mutual authentication scheme have the least possible effects on the average packet delivery ratio of the IoMT network. Furthermore, these results were computed in the IoMT networks where various possible intruder attacks were launch simultaneously.

F. Average Throughput

The average throughput is an important feature to consider while evaluating the performance of a routing or communi-

TABLE IV: Comparative analysis of various Security and Privacy-preserving approaches

Security Attacks	[6]	[23]	[16]	[5]	[15]	[8]	Proposed Scheme
Client Device Impersonation Attack	✓	✓	✓	✓	×	✓	✓
Eavesdropping Attack	✓	×	✓	✓	×	✓	✓
Server Module or Edge Impersonate Attack	×	✓	×	×	✓	✓	✓
Perfect Backward & Forward Attack	✓	×	✓	✓	✓	✓	✓
Member-device Impersonate Attack	✓	✓	✓	×	×	✓	✓
Man-in-the-Middle Attack (MITM)	✓	×	×	✓	×	×	✓

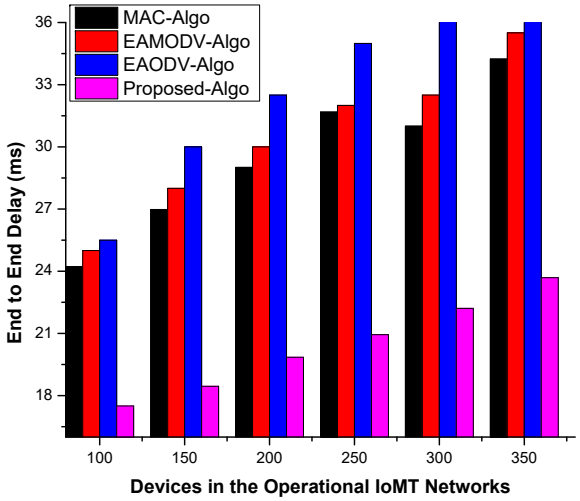

Fig. 6: End-to-End Delay

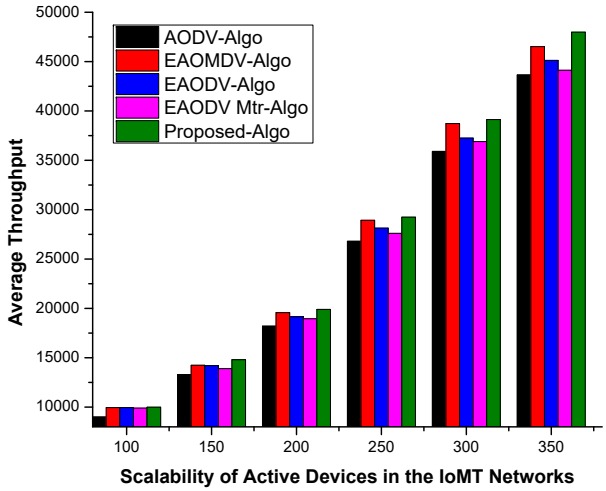

Fig. 8: Average Throughput

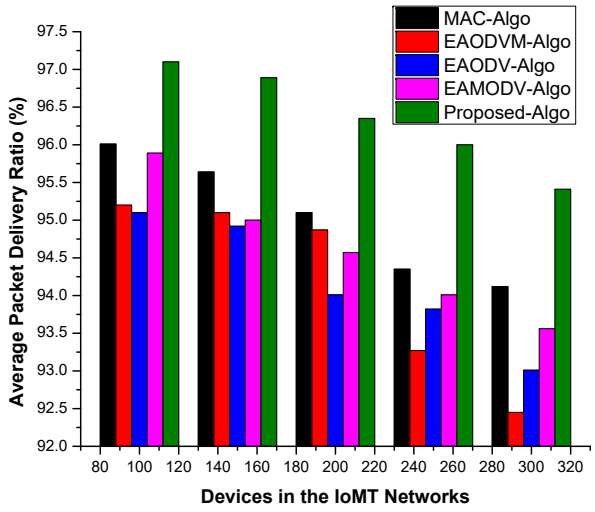

Fig. 7: Average Packet Delivery Ratio

cation approach, especially when the devices are distributed randomly. In addition, the average throughput of the system is proportional to the average retransmission ratio of the packets. Subsequently, this implies that the highest average throughput equatees to minimal loss during packet transmission over the internet. As a result, regardless of the IoMT deployment, the proposed privacy-preserving, secured mutual authentication and communication system is designed to obtain and achieve an average maximum throughput. The simulation results shown in Fig. 8 demonstrate that the suggested system outperforms the field-proven approaches in term of average throughput assessment measure. These approaches were also computed for the IoMTs, where a large number of malicious devices had been inserted and were attempting to interfere. In addition, the proposed approach is not susceptible to the scalability issue.

G. Ratio of the Generated to the Verified Messages

Usually in the IoMT networks, it is highly likely that both the server module S_j and wearable module C_i may be surrounded by adversary devices, which continuously try to intercept or interrupt an ongoing communication session between the two legitimate devices. Therefore, authentication schemes need to be smart enough not only to ensure that these devices are not permitted to start a communication session either with C_i or S_j, but at the same time report the existence of these adversaries to C_i and S_j, respectively. In the proposed authentication approach, we have carried out numerous simulations by deploying

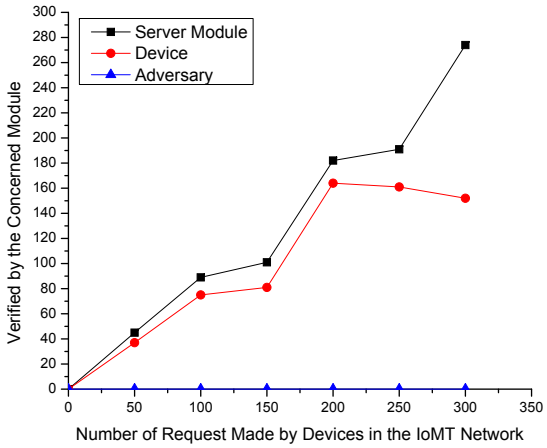

Fig. 9: Ratio of the Number of Request Generated to the Ratio of Verified Messages at the Respective Destination Module

adversaries at different positions in the closed proximity of C_i and S_j. We have observed that the proposed approach is not vulnerable to any attack launched by these adversaries. However, these adversaries somehow affect the overall ratio of the number of request generated to the ratio of verified messages, which is depicted for both C_i and S_j in Fig. 9. We have observed that if the ratio of the adversary devices within the proximity of these legitimate devices increased then a slight decrease may occur in the verified messages, which is an indication that these adversaries may not be able to be permitted, but these may still affect the performance of the underlying system.

VI. Conclusion and Future Work

In this paper, we proposed and designed a lightweight hybrid mutual authentication approach that allows real-time data collection, Big Data analytics, and predictive modeling to enhance patients' health outcomes. Our approach enables the secured communication between wearable devices and their concerned servers while also allowing for big data analytics and decision-making along with continuous learning and adapting to new data, thereby ensuring responsive, effective, and reliable healthcare facilitation. The legitimate devices are successfully authorized while malevolent entities are blacklisted prior to the initiation of data communication. We have demonstrated through extensive simulations that our proposed approach outperforms the existing field-proven approaches in terms of various performance metrics such as end-to-end delay, computational and communication overheads, average throughput, and packet delivery ratio. Future work will focus on enhancing the authentication process by designing more efficient security algorithms and implementing multi-factor authentication techniques. Additionally, we aim to explore the integration of advanced AI techniques, such as deep learning and Large Language Models (LLMs), to enhance the predictive accuracy and efficiency of health anomaly detection within the IoMT.

A. Acknowledgement

We are grateful to the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R239), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, for supporting this work.

B. Funding

This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R239), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

References

[1] F. Wei, P. Vijayakumar, N. Kumar, R. Zhang, and Q. Cheng, "Privacy-preserving implicit authentication protocol using cosine similarity for internet of things," *IEEE Internet of Things Journal*, 2020.

[2] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[3] R. K. Mahendran and P. Velusamy, "A secure fuzzy extractor based biometric key authentication scheme for body sensor network in internet of medical things," *Computer Communications*, vol. 153, pp. 545–552, 2020.

[4] A. Krall, D. Finke, and H. Yang, "Mosaic privacy-preserving mechanisms for healthcare analytics," *IEEE Journal of Biomedical and Health Informatics*, 2020.

[5] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[6] M. A. Jan, F. Khan, R. Khan, S. Mastorakis, V. G. Menon, M. Alazab, and P. Watters, "Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-cps," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5829–5839, 2020.

[7] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, pp. 58–80, 2016.

[8] M. A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar, and N. Stergiou, "LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics," *IEEE transactions on green communications and networking*, vol. 5(3), p. 1202-1211, 2021.

[9] M. Adil, R. Khan, M. A. Almaiah, M. Al-Zahrani, M. Zakarya, M. S. Amjad, and R. Ahmed, "Mac-aodv based mutual authentication scheme for constraint oriented networks," *IEEE Access*, vol. 8, pp. 44 459–44 469, 2020.

[10] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2014.

[11] R. Amin and G. Biswas, "Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment," *Wireless Personal Communications*, vol. 84, no. 1, pp. 439–462, 2015.

[12] 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.

[13] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Transactions on industrial electronics*, vol. 63, no. 11, pp. 7124–7132, 2016.

[14] Prosanta Gope, Owen Millwood, and Biplab Sikdar. A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things. *IEEE Transactions on Industrial Informatics*, 18(3):1971–1980, 2021.

[15] M. A. Abdelshafy and P. J. King, "Aodv and saodv under attack: Performance comparison," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2014, pp. 318–331.

[16] A. M. Makhlouf and M. Guizani, "Se-aomdv: secure and efficient aomdv routing protocol for vehicular communications," *International Journal of Information Security*, pp. 1–12, 2019.

[17] Y. Liu, M. Dong, K. Ota, and A. Liu, "Activetrust: Secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.

[18] B. Karthikeyan, S. H. Ganesh, and N. Kanimozhi, "Security improved ad-hoc on demand distance vector routing protocol (sim aodv)." *International Journal on Information Sciences & Computing*, vol. 10, no. 2, 2016.
[19] T. Delkesh and M. A. J. Jamali, "Eaodv: detection and removal of multiple black hole attacks through sending forged packets in manets," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 1897–1914, 2019.
[20] S. Shahabi, M. Ghazvini, and M. Bakhtiarian, "A modified algorithm to improve security and performance of aodv protocol against black hole attack," *Wireless Networks*, vol. 22, no. 5, pp. 1505–1511, 2016.
[21] Azzedine Boukerche and Rodolfo WL Coutinho. Design guidelines for machine learning-based cybersecurity in internet of things. *IEEE Network*, 35(1):393–399, 2020.
[22] Yi Ding, Guozheng Wu, Dajiang Chen, Ning Zhang, Linpeng Gong, Mingsheng Cao, and Zhiguang Qin. Deepedn: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet of Things Journal*, 8(3):1504–1518, 2020.
[23] M. R. Hasan, Y. Zhao, Y. Luo, G. Wang, and R. M. Winter, "An effective aodv-based flooding detection and prevention for smart meter network," *Procedia Computer Science*, vol. 129, pp. 454–460, 2018.
[24] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Computer Networks*, vol. 149, pp. 29–42, 2019.
[25] Salahuddin, Mohammad A., et al."Time-based anomaly detection using autoencoder" *2020 16th International Conference on Network and Service Management (CNSM). IEEE, 2020*.
[26] Pereira, Joao, and Margarida Silveira."Learning representations from healthcare time series data for unsupervised anomaly detection" *2019 IEEE international conference on big data and smart computing (BigComp). IEEE, 2019*.
[27] Leevy, J. L., Khoshgoftaar, T. M., Bauder, R. A., & Seliya, N. (2018). *A survey on addressing high-class imbalance in big data. Journal of Big Data*, 5(1), 1-30.
[28] H. Sedjelmaci, S. M. Senouci, N. Ansari, and A. Boualouache, "A trusted hybrid learning approach to secure edge computing," *IEEE Consumer Electronics Magazine*, vol. 11(3), pp. 30–37, 2021.