IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 March 2024, accepted 7 May 2024, date of publication 13 May 2024, date of current version 31 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3400400

RESEARCH ARTICLE

A Lightweight and Secure Authentication Scheme for Remote Monitoring of Patients in IoMT

ZOHAIB ALI[1], SABA MAHMOOD[1], KHWAJA MANSOOR UL HASSAN[2], ALI DAUD[3], RIAD ALHARBEY[4], AND AMAL BUKHARI[4]

[1]Department of Computer Science, Bahria University, Islamabad 44000, Pakistan
[2]Department of Cyber Security, Air University, Islamabad 44000, Pakistan
[3]Faculty of Resilience, Rabdan Academy, Abu Dhabi, United Arab Emirates
[4]Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia

Corresponding author: Ali Daud (alimsdb@gmail.com)

This work was supported by the University of Jeddah, Jeddah, Saudi Arabia, under Grant UJ-02-032-DR.

ABSTRACT The rise of smart health technologies has offered benefits such as remote patient monitoring, personalized therapy, and early disease detection. However this advancement has also raised concerns about security and privacy of patient data. Authentication is essential for protecting patient data and smart health devices. The existing scheme is identified with security vulnerabilities in terms of stolen verifier, impersonation, and man in middle attacks. Motivated by this, authors have presented a secure, lightweight authentication technique for smart health environments for a remote monitoring scenario employing a Multiple Factor approach and a lightweight algorithm. The scheme is verified through formal and informal analysis. The scheme demonstrated enhanced authentication performance and security with processing overhead of (0.04 milliseconds) and transmission overhead of (704 bits), in comparison to the baseline scheme. This system has the potential to improve data security and privacy in a variety of smart health scenarios.

INDEX TERMS Critical infrastructure, IoMT, authentication, remote monitoring, lightweight scheme.

I. INTRODUCTION

Smart Smart cities utilize Internet of things(IoT), including connected sensors and devices, enabled by advanced wireless communication technologies. Mobile communication has become ubiquitous, with nine out of ten people opting for mobile over landlines. The proliferation of devices like tablets, smartphones, and IoT gadgets along with modern communication tools like social media and video calling, has surged data traffic demand. Wireless networks have become integral to daily interactions and business strategies, fostering startup innovation. Our world is becoming increasingly networked as the Internet of Things (IoT) has evolved. According to projections, there will be around 75 billion devices linked to the Internet by 2025. These connections have the potential to improve decision-making and data delivery with increase risk of security concerns. The Internet of Medical Things (IOMT) has emerged to provide patients with health-related services online, such as virtual consultations with medical doctors and employees. IoT with medical devices and related sensors is referred as IOMT that can include smart gadgets, on body sensors, smart hospitals, smart critical care centres and etc. Smart wearable body sensors collect patient medical data, such as heart rate, within these systems. This data is subsequently securely transferred over the Internet to cloud-based medical systems. Doctors and other healthcare experts can use this information to monitor a patient's health state, to diagnose ailments, and provide remote medical counsel and recommendations.

To enable remote healthcare monitoring, [1] particular models and designs must be seamlessly incorporated into the patient record system to provide optimal data management. Remote Health Monitoring strives to create applications for a wide range of healthcare needs, including glucose level sensing, ECG monitoring, blood pressure monitoring, body temperature monitoring, oxygen saturation monitoring, rehabilitation systems, medical management, wheelchair management, and other critical healthcare solutions. With the

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

onset of the COVID-19 Pandemic, the Internet of Things (IoT) in medical devices has seen the introduction of linked imaging, hospital procedures, drug distribution, patient care, diagnostic tests, pharmacy control, and the evolution of health safety through smart instruments such as blood gas analyzers, thermometers, smart beds, glucose meters, ultrasound, X-rays, and I-patient biological services. Accelerometer monitors activities like physical activity levels, sleep patterns, fall detection for elderly patients, neurological conditions and more.The electrocardiogram (ECG) detects electrical activity in the heart, whereas blood pressure measures the force of blood against arterial walls. Wearable sensors, smart clothes, ECG monitors, and specialist medical gadgets are used to measure ECG and blood pressure. A pulse oximeter is a non-invasive sensor that detects a patient' s blood oxygen saturation (SpO2) and pulse rate (heart rate). Spirometer Lung function is measured by examining a person's respiratory airflow and volume, that aids in the diagnosis and management of lung disorders such as asthma.

A. MOTIVATION

In remote healthcare systems utilizing IoMT (Internet of Medical Things), ensuring patient data privacy and security is a major concern. Wireless data transfer in IoMT exposes vulnerabilities to eavesdropping, compromises privacy, and allows malicious actors to inject data leading to inaccurate diagnoses. According to a survey there were 70% targeting rate in 2023 exploiting the vulnerabilities of the IoT devices against cyberattacks [2]. This highlights the increased necessity of security in smart healthcare, particularly in the times of crisis, such as the COVID-19 epidemic, where IoMT use has increased dramatically. Given IoMT's reliance on resource-constrained sensor devices,they are unsuitable for complicated cryptographic tasks, balancing secure communication and resource-efficient operations is critical. Numerous authentication protocols have been proposed by researchers to bolster IoT device security. Some of these protocols rely on symmetric key-based encryption, using a common key for communication between IoT users and the server. However, many of these approaches have exhibited shortcomings in terms of efficiency and security.A recent authentication [3] scheme proposed for the similar scenario showed vulnerabilities against Stolen verifier, Impersonation and Man in middle attacks.

B. CONTRIBUTION

We have proposed the lightweight authentication scheme, designed specifically for smart healthcare applications in the IoMT domain for remote monitoring of patients. This paper introduces a lightweight authentication and key agreement model tailored for IoMT smart healthcare application for a health monitoring scenario. The proposed model comprises three key components, as illustrated in Figure 1. Firstly, patients are equipped with wearable devices that collect health-related data. This data is transmitted via a mobile device or tablet acting as a gateway to a medical server, where it is securely stored. Secondly, medical professionals, including doctors and nurses, access and authenticate themselves to the server to retrieve and provide healthcare advice to patients. We have validated the robustness of the proposed model against well-known attacks, such as impersonation attacks, thereby confirming its ability to meet crucial security requirements. In addition a comprehensive assessment of an authentication scheme proposed by Amintoosi et al. [3] named Slight is conducted. This led to the identification of vulnerabilities to malicious user impersonation and server impersonation attacks, alongside the local verification issue. Lightweight authentication is achieved by the use of simplified methods, symmetric cryptography, and a reduction in communication overhead. The security of the proposed model is formally verified using the Proverif tool. An informal assessment of its resilience against known attacks is also demonstrated. The proposed model achieves minimal computational complexity, specifically 0.04 milliseconds, and exhibits acceptable communication overhead when compared to related models. This positions the scheme as a suitable choice for IoMT applications, especially with sensor devices that have limited computational capabilities.The main objectives of the proposed protocol are summarized as follows.

- To develop lightweight biometric based authentication scheme
- To develop a robust IoMT authentication solution that mitigates established threats effectively.
- To develop an efficient scheme in terms of computational cost.

The upcoming sections are organized as follows: Section II delves into an exploration of related work. In Section III and IV, we have provided a detailed description and security analysis of Amintoosi et al.'s scheme [3], while Section V offers an in-depth look at the model. Section VI and VII is dedicated to the security and performance analysis of the proposed scheme. Lastly concluding remarks and future directions are discussed.

II. RELATED WORK

Smart city contains variety [4] of applications, including healthcare, homes, factories, and devices. We must implement a variety of measures, including integrity, confidentiality, availability, authorization, authentication, and non repudiation. Multiple researchers have explored and designed security mechanisms for smart cities, as well as suggested numerous authentication methods but these methods are vulnerable to different attacks. Author classify the authenticity [5] attacks into categories that includes active or passive attack, internal or external attack, key,data, physical and impersonation based attack, identity location eavesdropping manipulation and service based attack. The Rhee system has flaws that makes it ineffective against user anomalies, including impersonation, password guessing, and intruder attacks, according to Karuppiah's analysis [6]. Additional flaws in

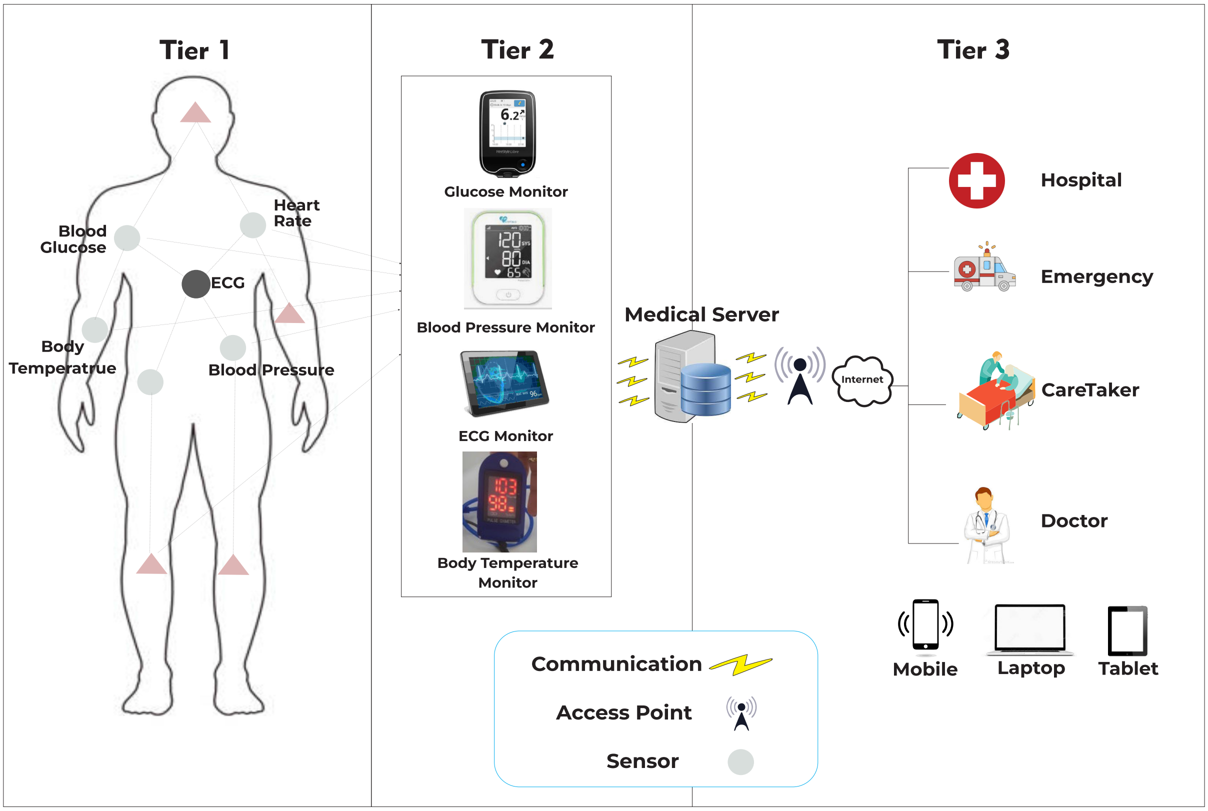


FIGURE 1. IoMT architecture.

the method includes its unstable update, modification, and password detection techniques. Adversaries have the ability to modify data or compromise smart cards if they have control of the connection between the server and users.To address these problems, Karuppiah presented a secure method that pairs domestic and foreign agents using Diffie-Hellman-generated common secret keys. According to [7], the author has created a dynamic ID-based architecture for anomaly authentication that is very resistant to intruder attacks. This system demonstrates its ability to survive known threats through thorough performance and security testing, making it a solid choice for secure mobile communications. It ensures secure connections for device users by performing checks before giving access to trustworthy networks. Tao Zhou highlighted the adversary's capabilities and underlined the relevance of session key semantic security and user anonymity in mobile situations in his study [8]. He addressed problems with wireless anonymous authentication and offered a mutual authentication framework for roaming services. Zhou's protocol passes the standards for anonymity and semantic security with flying colors. The author created the Mutual Authentication Key Algorithm (MAKA) protocol in their work [9], that combines key agreement and mutual authentication to provide secure communication between users and servers. This protocol [10] overcomes flaws discovered in prior techniques, such as replay attacks and excessive memory use. Guangquan Xu's idea entails leveraging symmetric encryption to introduce randomization, fixing anomalies with decrypted and randomly changing pseudo IDs, efficient storage with XOR and one-way hashing, and maintaining DE synchronization by keeping pseudo identities separately. This comprehensive technique resists lost card attacks, forgeries, and eavesdropping by creating session keys with three random variables, hence improving overall security. User privacy is protected in the article [11] by server-based biometric authentication and a dynamic verification table, which maintains user anonymity in a dynamic three-factor authentication key agreement approach for e-health systems. The paper also focuses efficiency by using lightweight biohash and hash algorithms to meet energy consumption and security requirements while maintaining semantic security.

In study [12], Wu's protocol's security flaws are highlighted, including susceptibility to temporary information attacks, lack of perfect secrecy, and a failure to secure user anonymity. A provably secure three-factor authentication system is proposed and rigorously tested, outperforming Wu's protocol in terms of security and efficiency.

Yan's method [13] is investigated, demonstrating its flaws. To increase the scheme's security and effectiveness, researchers recommend upgrades such as improved login and password changing procedures, user anonymity protection, and defense against password guessing attacks.

A rapid three-factor authentication technique for 5G wireless sensor networks hosting e-health systems is introduced in study [14]. This method ensures user privacy by combining biometrics, passwords, and smart cards for secure and quick authentication, as well as a multi-server design to save database expenses.

In study [15], security issues in Omid's Telecare Medical Information System(TMIS)authentication system are discovered. The suggested protocol outperforms existing recent protocols in terms of security, complexity, and communication subtleties against numerous assaults, including impersonation and user anonymity breaches.

The combination of e-health management systems on [16] and IoT raises issues such as secure connection and authentication.

In research [17], LACO is proposed as a solution for anonymity, access control, and ownership transfer in IoMT systems, with future work concentrating on hardware implementation and medical standards compliance.

The reviews [13] cited in the study Yan's TMIS system detects problems and presents a better solution that handles input correctness, anonymity maintenance, and password guessing attacks, considerably improving security in three critical areas.

The research [18] identifies security flaws in an ECC-based authentication and key agreement mechanism for TMISs, highlighting difficulties such as session-specific temporary information attacks and the lack of perfect forward secrecy. As a result, a novel anonymous and unlinkable authentication and key agreement mechanism is presented, which outperforms previous methods in terms of security and efficiency. The protocol's resistance against both active and passive threats is validated by rigorous formal security testing with the AVISPA tool, confirming its appropriateness for TMIS applications.

Tan's TMIS authentication mechanism, as detailed in [19], has security flaws that made it vulnerable to replay and denial-of-service attacks. This work presents a more secure and efficient three-factor Elliptic Curve Cryptography (ECC) based authentication and key agreement solution for TMIS. When compared to Tan's technique, the suggested scheme is more resistant to attacks and more efficient, making it a better alternative for TMIS applications.

Author describes [20] smart home systems, which use specialized electronics and sensors to remotely regulate healthcare devices, ensuring patient safety and health monitoring. TMIS is able to provide continuous healthcare services because to the growing usage of smart homes, which is fueled by telemedicine and telecare. It does, however, raise security concerns about patient privacy, which can be reduced by a proposed safe mutual authentication technique. This key agreement mechanism protects patient privacy by utilizing elliptic curve cryptography and a fuzzy extractor for biometric-based patient identification. Edge computing is used in IoT architecture, as shown by a proposal in [21]. This architecture employs a large number of data transmission nodes, which may confuse software models. The Author proposes a fog-based access control model [22] that protects the performance of cloudfog-based IoMT. For the structure, a quite well access management approach has been considered.

As explained in [23], the architecture is built around wireless sensor network (WSN) technology. A cloud-based mobile application can be used by the doctor to provide online healthcare services to a patient

The authors propose an improved security model [24] that includes authorization and authentication features. They have also proposed a novel multi-authority attribute-based encryption technique called MA-EBA to safeguard healthcare data from unauthorised access threats. This method improves device scalability and gives users fine-grained access to the system.

Wireless Body Area Networks (WBANs) report crucial patient information. The patient's body [25] is fitted with sensor nodes that establish a session key and anonymously verify it with the local server/hub node.

The researchers [11] suggested authentication with three-factor for an e-health system and used a dynamic mechanism to protect the patient's privacy. It implements biometric authentication on the server side and uses light weight hash with hash operations using bio to reduce computational costs. Semantic security is provided by the scheme.

It is critical to ensure secure connection directly between devices (D2D) in order to minimize communication delays that may occur when a third party is involved.To address these challenges of physical capture attempts on devices and lack safeguards for assuring anonymity a D2D secure access control system is required to build long-term smart healthcare. Author [26] describes a certificate-based device to device(D2D) access control mechanism for IoMT systems (D2DAC-IoMT) that makes use of elliptic curve encryption. The security of the proposed D2DAC-IoMT technique is validated using both formal and informal methods. Communication cost is 2464 bits while computational cost is 57ms.

Wu et al. [27] explain each session includes three participants including a user with device,foreign and the home agent. U firstly registers with home agent and then obtains the necessary data from HA in its service area. If U connects to a foreign network, he will able to gain assistance from FA with the assistance of HA. The author specifies a password hashes and a smart card as prerequisites for initiating a session, and then this session is being authenticate and session key is generated. The scheme provide prevention over the insider attacked by using random value and hash function, and due to session created on multiple random variable so guessing attack are also not supported. There are only three attempt with short time so forgery attack can be prohibited. Session key contain secret string so it prevent spoofing attack. It provide resistant to de synchronization attack because every participant have different authentication data.

In IoMT, radio frequency identification (RFID) authentication is widely used to identify users and end nodes. A new scheme utilizing dynamic framed slotted Aloha, an anti-collision protocol, has been proposed in [28] to prevent tag collisions in RFID systems. Three elements make up the suggested model: batch tags with RFID, readers, and servers for the backend. Each patient object has an RFID tag attached, and communication takes place across wireless channels. To reduce the price of tags and increase the effectiveness of tag identification, an RFID batch authentication method is introduced. A linear homogeneous equation is also used by the system to perform RFID batch authentication.

In [29], El Zouka proposed an authentication scheme that provides remote health monitoring of patients using secure integration of health care system and wearable medical sensor devices. The patients' physiological features are collected through wearable devices which are then communicated securely and stored in a healthcare system. This information is also sent to the doctor via sms or email in case of any abnormal condition. The proposed authentication scheme is categorized into three stages namely registration, patient login and authentication phase. Author believes that this scheme is lightweight, efficient and effective.

In [25] Li et al., proposed a lightweight anonymous authentication and key agreement scheme for two hop centralized WBAN. This scheme authenticates patient by setting up session key anonymously and in an unlinkable way. This scheme has been checked not only with BAN logic but also by using Automated Validation of Internet Security Protocols and Applications (AVISPA).

The author [30] of this study provide a user-friendly privacy-preserving authentication strategy designed to address issues in a distributed smart healthcare system. Through the formation of a secure session, our suggested technique ensures that only authorized users can enter the healthcare system. Using a password protection method, only legitimate individuals have access to edit the patient's healthcare data. The paper evaluates the security robustness and effectiveness of our authentication scheme, demonstrating its increased efficiency and security when compared to existing state-of-the-art schemes.Communication cost is 1536B. Sensors are sensitive and resource-limited devices that are used in Wireless Medical Sensor Networks (WMSNs). These sensors collect vital signs from patients and transfer the information to professionals over open channels via gateways. However, in the absence of sufficient data security, the data carried by WMSNs is vulnerable to manipulation by adversaries, potentially leading to grave consequences, [31] presents a novel categorization of authentication systems in Wireless Multimedia Sensor Networks (WMSNs), categorized by architecture. Wan et al. [32] To protect against impersonation and sensor node capture attempts, implemented a continuous authentication mechanism that uses ECC and Hash. For additional protection, difficult-to-imitate physiological [33] by combining physiological indicators with lightweight cryptographic primitives to improve security. AVISPA is used for additional security measures. In reference [34], the author used Hash and built a lightweight strategy by including mobile devices into the authentication process, as well as AVISPA for enhanced security. Alzahrani and colleagues [35] utilized Symmetric Encryption, Hash, and Bio Hash to address the shortcomings identified in [34], implementing improvements. Additionally, they adopted a cloud-based environment for enhanced functionality.In [36], the author stresses user anonymity and allows registered and verified users to access medical networks via encrypted sessions, utilizing both hash and AVISPA for increased security. The Author [37] offers a novel lightweight Speck Cryptographic Algorithm to improve healthcare data security in High-Performance Computing. In compared to traditional cryptographic procedures in cloud computing, the suggested method's experimental findings show higher security levels and a significant improvement in both data encryption speed and achievable security.

This Author [38] digs into the communication architectures and applications of the Internet of Medical Things (IoMT), focusing on security concerns and potential threats. It describes the network and adversary models of IoMT, as well as a taxonomy of security protocols such as key management and authentication. A thorough comparison assesses different protocols based on computation and communication costs, security features, and accuracy. The report concludes with recommendations for further research in the IoMT security landscape.

Through a signature forgery attack on their certificate less signature technique, [39] highlights a weakness in current cloud-centric IoMT smart healthcare systems. A new certificateless signature technique with no pairings is introduced and formally validated. As evidenced by practical performance, the findings encourage the establishment of a more secure and efficient IoMT-based healthcare system. A recent work has taken into account the protection of privacy of the physiological values of patient data for accurate disease prediction [40].

A. ADVERSARIAL MODEL

The proposed protocol is crafted with consideration of the following adversarial model, aligning with common assumptions outlined in [33]. The adversary A is assumed to possess the following capabilities:

1) Full control over the public channel, enabling interception, reversion, modification, replay, and even the transmission of fresh fabricated messages.
2) Capability to extract information from the node via power analysis; however, the shared key between the node and server remains secret and inaccessible to any adversary.
3) Adversary A may be a deceitful node or an external entity not affiliated with the system.

4) The database linked to the server is deemed inaccessible, and no adversary, including A, can access the server's private key.

III. BRIEF REVIEW AND SECURITY ANALYSIS OF AMINTOOSI ET AL.S SCHEME

A. BRIEF REVIEW OF AMINTOOSI ET AL.S SCHEME

The scheme of Amintoosi et al. [3] has three main phases, namely, registration, and authentication, transfer Ownership and password updation.

TABLE 1. Notation table of Amintoosi et al. scheme.

Notations	Description
M_s , U_i	Medical Server and i_{th} Doctor
ID_i , IDS_j	ith User Identity, jth Sensor Identity
X_j S_{id}	jth Sensor key , Server Identity
PW_i	ith User Password
D_i and Q_p and T_p	Random Number
$T1, T2, T3, T4, T5$	Current Time Stamp
Sk_u	Key of Doctor Node
Sk_u and Sk_s and Sk_p	Server Keys
Sk_p	Sensor Key
$h(.)$	One Way Hash
S_D , S_S	Session Key Doctor , Session Key Sensor
$\|\|$	Concat operator
$\oplus$	Bitwise XOR operator

B. DOCTOR REGISTRATION PHASE

The Doctor *Ui* initiates process of registration with server and requests a card for future logins. The index *i* denotes the registered doctors, initially set to zero and increase upon a new doctor's registration with the server. The process is illustrated in Figure 2 and outlined as follows.

Step 1: Doctor selects a ID (IDi), the random number (ai) and a password (pwi), and computes $\mathrm{p}_i = h(ID_i||pw_i||a_i)$ and tranfers $< pi, IDi >$ to the medical server safely.

Step 2: After receiving the registration request, the server checks the database to confirm if any other user has previously registered using the same IDi. In the presence of a prior registration, the server requests a fresh identity, else it generates a random number (bi) and evaluates $\mathrm{bI}D_i = h(b_i||ID_i), M_i = h(b_i||ID_i||bID_i), N_i = h(SID||S||b_i), Ai = Ni\oplus$ pi, and $\mathrm{B}_i = h(M_i||N_i)$.

Finally, the server saves ⟨bi, Ai, Bi⟩ on the smartcard and ⟨Ai, Mi, Bi, IDi⟩ Within the server's memory that is resistant to tampering, specifically in the database.The index i is incremented to indicate the registration of a new doctor with the server. The smartcard is then safely sent to the doctor by the server.

*Step 3:*The Doctor adds ai a random number, the smart card, resulting in storage of ⟨bi, Ai, Bi, ai⟩ on the card.

C. SENSOR REGISTRATION PHASE

- *Step 1:* The sensor Pj first chooses a random number, f j, and then computes $\mathrm{G}_j = h(IDS_j||X_j||(f_j)$ where IDSj and Xj are respectively, the sensor's identity and secret key. Then it sends ⟨Gj, f j, IDS j⟩ securely to the medical server.
- *Step 2:* S calculates $\mathrm{W}_j = h(IDS_j||s||(f_j)$ (here s The server first generates a new key using its primary key and uses it to encrypt ⟨Gj, IDS j, f j⟩ before storing it in its tamper-proof database. It increments the count j to reflect the registration of one more sensor on the server. Lastly, the server transmits the value of wj to the sensor in a secure manner.
- *Step 3:* ⟨wj, f j⟩ are kept in the sensor's tamper-proof memory.

D. AUTHENTICATION PHASE

To attain permission to view the information on the medical server, user Ui must insert their smartcard. The steps for user authentication, as illustrated in Figure 4, are as follows:

Step 1: The user Ui enter their identity with their assigned password, denoted by $ID * i$ and $pw * i$, respectively. Then smartcard computes $\mathrm{p}{*_i} = h(ID_i||pw_i||a_j), N{*_i} = (A_i \oplus p{*_i}), bID{*_i} = h(b_i||ID{*_i}), M{*_i} = h(b_i||ID *_i ||bID{*_i}), and\ B{*_i} = h(M *_i ||N *_i ||p{*_i})$. Subsequently, the system verifies if the calculated $B{*}i$ matches the stored value Bi on the smart card, in ensuring that the user is the rightful owner of the card and that it has not been stolen. Next, the smart card selects a random number $d * i$ and time stamp $T1$ then computes M1i = h($\mathrm{M}_i||N_i||T_1) \oplus$ di,and M2i = h($\mathrm{M}_i||N_i||d_i)$. The smartcard then sends ⟨M1i, T1, bi, M2i⟩ to the medical server.

Step 2: The server selects the time upon message receipt T2 and confirms |T2T1| <?T. If so, the server calculates Ni = h($\mathrm{S}_{ID}||s||b_i)$, di = h($\mathrm{M}_i||N_i||T_1) \oplus$ Mi and M2 = h($\mathrm{M}_i||Ni||di)$. and determines if what M2 i = ?M2i. If so, the user is authenticated. Next, S selects random number qp and calculates zj = h($\mathrm{d}_i||IDS_j||f_j) \oplus$ qp, wj = h($\mathrm{IDS}_j||s||f_j)\ and\ y$ j= $h(w_j||G_j||q_p)$. Lastly the server sends ⟨di, z j, Yj, T2⟩ to the sensor.

Step 3: The sensor picks a timestamp to gauge the recentness of the received message, T3 and determine |T3 T2| < ?T. If it holds, the sensor calculate qp = ⊕ zj($\mathrm{d}_i||IDS_j||f_j)$. It then selects random number Tp and calculates Gj = ($\mathrm{IDS}_j||X_j||f_j)\ and\ Yj = h(w_j||G_j||g_p)$. The sensor then checks whether $\mathrm{Y}{*j}$ equals Yj received from the server. If this is the case, it establishes that the message came from the server, and thus the server is authenticated. It then calculates skp as skp =h($\mathrm{q}_p||IDS_j||T_p).Also,\ Qj = h(G_j||fj||wj)\oplus$ Tp $and\ Authj = h(sk_p||wj||T3)$. Lastly the sensor sends ⟨Qj, T3, Authj⟨ to server.

*Step 4:*The server uses the time stamp to determine whether or not the message is new, T4 and verifies |T4 – T3|$\leq ?\Delta T$. It then authenticates the message by calculating pi = Ni⊕Ai, 'Tp = h($\mathrm{G}_j||f_j||w_j)\oplus$ Qj, Sks = h($\mathrm{q}_p||IDS_j||T_p)$ and Auths = $\mathrm{h}(\mathrm{sk}_s||w_j||T_3)$ and comparing Auths with Authj After receiving the message from the sensor, the server verifies if both values are identical, thus confirming the authenticity of the message's sender as the sensor. Subsequently, the server proceeds to compute ui = pi ⊕ Tp, vi = pi ⊕ qp, M3i =h($\mathrm{u}_i||v_i||p_i||T_4)$ and sends ⟨T4, ui, vi, M3i⟩ to the user.

Step 5: Upon obtaining the server's message, the user selects T5 to check its freshness, and verifies whether the time difference between T5 and T4 is less than or equal to a certain threshold value ΔT. If the condition is met, the user

Doctor -Ui/SmartCard		**Medical Server(S)**
Select random number a_i		
Choose ID_i, P_{wi}		
$p_i = h(ID_i\|\|pw_i\|\|a_i)$		
	$\xrightarrow{M=\{ID_i,p_i\}}$	
		Search ID_i in database
		if ID_i exist , request new ID
		else
		Select Random Number b_i
		$bID_i = h(b_i\|\|ID_i)$
		$M_i = h(b_i\|\|ID_i\|\|bID_i)$
		$N_i = h(SID\|\|S\|\|b_i)$
		$A_i = N_i \oplus p_i$
		$B_i = h(M_i\|\|N_i)$
		Store (b_i, A_i, B_i) on Smart
		Store (A_i, M_i, B_i, ID_i) on Database
		i = i + 1
	$\xleftarrow{\{SmartCard\}}$	
Add a_i to Smart card		
Stores [b_i, A_i, B_i, a_i]		

FIGURE 2. Amintoosi et al doctor registration phase.

Sensor		**Medical Server(S)**
Select random number f_j		
$G_j = h(IDs_j\|\|X_j\|\|f_j)$		
	$\xrightarrow{M=\{G_j,f_j,IDs_j\}}$	
		$W_j= h(IDs_j\|\|s\|\|f_j)$
		Stores G_j, IDs_j, f_j
		j = j + 1
	$\xleftarrow{\{W_j\}}$	
Add a_i to Smart card		
Stores [w_j, f_j] in the Temper Proof Memory		

FIGURE 3. Amintoosi et al sensor registration phase.

then calculates $M3*$ i =h($u_i||v_i||p_i||T_4$) and determine if it is the same as M3i received from the server. If so, the message is proven. The user then evaluates Tp $=$ pi $\oplus$ ui and qp $=$ pi $\oplus$ vi and then, evaluates the session key sku as Sku =h($q_p||IDS_j||T_p$)

E. OWNERSHIP TRANSFER PHASE

During this phase, the access rights of a particular patient's data (i.e., the jth sensor) that were previously granted to one doctor, are transferred to another doctor. The first doctor's access permissions to the jth sensor are then revoked. This process is illustrated in Figure 5. 1. To verify the identity of the second doctor , $U2$, the doctor inserts their smart card and inputs their ID∗2 and pw∗$_2$. This is followed by an authentication process to confirm that U2 is the rightful owner of the smart card then the smartcard computes P∗ 2 $= h(ID_2||pw_2||a_2)$, N∗ 2 $=$ A2 $\oplus$ p∗2, $bID2 = h(b_2||ID_*2)$ M∗2 $= h(b_2||ID_*2||bID_*2)$, and $B_2* = h(M_2*||N_2*||p_2*)$ and checks whether B2 $=$ B∗ 2. If not, the smart card is not selected. Otherwise, the smart card gets to pick the random number r2, and computes AID$_1$ $= h(ID1||r2)\oplus$ ID2 and $K1 = h(ID_2||r_2)$, where ID$_1$ is the identity of the first doctor (U$_1$). At the end, U$_2$ sends K$_1$, AID_1, and r$_2$ as well as the ownership transfer request in the form of ⟨ K$_1$,AID_1, r$_2$, OTRequest⟩ message to U$_1$ through the server.

2. Upon receiving the message, U1 inserts his smartcard and enters $ID*1$ and $pw*1$. To authenticate U2 as the owner of the card, the following calculations are done:

$P_1^* = h(ID_1^*||pw_1^*||a_1)$ $N_1^* = A1 \oplus p_1^*, bID_1^* = h(b_1||ID_1^*)$ $M_1^* = h(b_1||ID_1^*||bID_*1)$ $B_1^* = h(M_1^*||N_2^*||p_1^*)$

The smartcard then checks whether B1 $=$ B_1^*. If so, it is verified that the smart card belongs to U$_1$. Then, the smart card computes $ID_2^* = AID_1 \oplus h(ID_1||r_2) and K_1^* = h(ID_2^*||r_2)$, and checks whether K$\oplus$ =?K1 to ensure that the message has been sent from the second doctor U2. He then selects the random number r$_1$ and calculates BID$_1$ $= h(SID||r_1) \oplus ID_1, k_2 = h(ID1||r_1)$ and CID$_1$ $= h(SID||r_1) \oplus ID_2$, where SID is the server's identity. He also computes k$_3$ $= h(ID_2||r_2$ and k$_4$ $= h(k_2||k_3)$, and sends ⟨ k$_4$, r_1, $_r2$, BID_1,CID_1⟩ to the medical server.

3. Once the message is received at the server, it first retrieves the doctors' identities ID$_1$ $andID_2asID_1 = h(SID||r1)\oplus BID_1, k_2 = h(ID_1||r_1)$ and ID$_2$ $= h(S_ID||r_2) \oplus CID_1$. Next, in order to authenticate the message, it computes k$_3$ $= h(ID_2||r_2)$ and k $*_4$ $= h(k_2||k_3)$ and checks whether k$*_4$ $= k_4$. Once the message is verified, the server proceeds to update the Access Control List (ACL) by revoking U_1 access permissions to the jth sensor and transferring it to U$_2$. As a result, U$_1$ will no longer be able to access the data.

F. PASSWORD UPDATE PHASE

The process of updating the user's password is outlined in this section. The following steps are required to accomplish this task:.

In Step 1, the user inserts their smart card and inputs their $ID*i$ and $pw*i$. The smart card then performs a calculation to authenticate the user as the rightful owner of the smart card. p$*_i = h(ID_*i||pw_*i||a_i), N*_i = A_i \oplus p_*i, bID*_i = h(b_i||ID * i), M*_i = h(bi||ID *_i ||bID*_i), B*_i = h(M *_i ||N *_i ||p*_i)$.

Doctor -Ui / Smartcard	Medical Server - (S)	Sensor - Sj
Insert Smart Card Input ID$_i*, pw_i*$ p$_i* = h(ID_i*\|\|pw_i*\|\|a_i)$ N$_i* = A_i \oplus p_i*$ bID$_i*$=$h(b_i\|\|ID_i*)$ M$_i*$=$h(b_i\|\|ID_i*\|\|bID_i*)$ B$_i*$=$h(M_i*\|\|N_i*\|\|p_i*)$ B$_i$=B_i*		

Select Random Number d$_i$
Select Time Stamp T$_1$
M1$_i = h(M_i\|\|N_i\|\|T1) \oplus d_i$
M2$_i = h(M_i\|\|N_i\|\|d_i)$
$\xrightarrow{M1=\{M1_i,T1,b_i,M2_i\}}$
	Select Time Stamp T2
	| T2 - T1 | $\leq \triangle T$
	N$_i = h(SID\|\|s\|\|b_i)$
	d$_i = h(M_i\|\|N_i\|\|T1) \oplus M1_i$	

	M2$_i* =?M2_i$
	Select random Number q$_p$
	z$_j = h(d_i\|\|IDS_j\|\|f_j)\oplus$
	w$_j = h(IDS_j\|\|s\|\|f_j)$
	y$_j = h(w_j\|\|G_j\|\|q_p)$
	$\xrightarrow{M2=\{d_i,z_j,Y_j,T2\}}$
		Verify T3 - T2 $\leq \triangle T$
		q$_p = (z_j \oplus d_i\|\|IDS_i\|\|f_j)$
		Select random number T$_p$
		G$_j* = h(IDS_j\|\|X_j\|\|f_j)$
		Y$_j* = h(W_j\|\|G_j*\|\|q_p)$
		check Y$_j = Y_j*$
		sk$_p = h(q_p\|\|IDS_j\|\|T_p)$
		Q$_j = h(G_j\|\|f_j\|\|w_j) \oplus T_p$
		Auth$_j = h(sk_p\|\|w_j\|\|T_3)$
		$\xleftarrow{M3=\{Q_j,T_3,Auth_j\}}$

	Verify T4 - T3 $\leq \triangle T$
	p$_i = N_i \oplus A_i$
	T$_p = h(G_j\|\|f_j\|\|w_j) \oplus T_p \oplus Q_j$
	sk$_s = h(q_p\|\|IDS_j\|\|T_p)$
	Auth$_s = h(sk_s\|\|w_j\|\|T_3)$
	Auth$_s =?Auth_j$
	u$_i = p_i \oplus T_p, v_i = p_i \oplus q_p$
	M3$_i = h(u_i\|\|v_i\|\|p_i\|\|T_4)$
	$\xleftarrow{M4=\{t_4,u_i,v_i,M3_i\}}$	

Select time stamp T$_5$ Verify T5 - T4 $\leq \triangle T$ M3$_i* = h(u_i\|\|v_i\|\|p_i\|\|T_4)$ M3$_i* = M3_i$ T$_p = p_i \oplus u_i$ q$_p = p_i \oplus v_i$ sk$_u = h(q_p\|\|IDS_j\|\|T_p)$		

FIGURE 4. Amintoosi et al authentication phase.

The ownership is verified by comparing B∗ i with B_i stored on the smartcard.

Step 2 : The user enters $pw * i$ as the new password. Then, the smartcard calculates: p$*i = h(ID*i||pw**i||ai)$, $N*i = Ai \oplus p*ibID*i = h(bi||ID*i)M*i = h(bi||ID*i||bID*i)B*i = h(M*i||N*i||p*i)$. In the end, Bi is replaced by B$*i$ in the smart card.

IV. CRYPTANALYSIS OF SLIGHT SCHEME

In this portion, we demonstrate that Slight is susceptible to a stolen verifier attack so it create a possibility to cause subsequent attacks like server impersonation attacks and Sensor Impersonation Attacks.

A. STOLEN VERIFIER ATTACK

A verifier, such as a password or cryptographic key, confirms the identity of a user. When a hacker obtains unauthorized access to the verifier, which enables impersonation, the attack is known as a stolen verifier attack, also known as password or key theft. The private key of a user is essential in a cryptographic system. By stealing it, an attacker can pretend to be the user, get access to a system without authorization, or decrypt sensitive data.

B. MALICIOUS USER IMPERSONATION

Step 1: Since the adversary is a previously registered doctor, and the operation on the server including information functions A$_i$ $= N_i \oplus p_i, B_i = h(M_i||N_i)$, M$_i$ $= h(b_i||ID_i||bID_i)$,iD$_i$ $= iD$ and then stores (A$_i$, M_i, B_i, ID_i) into the database as mentioned in the setup phase or registration phase of the slight. [3]

Step 2: Since Msg is $< M1_i, T_1, b_i, M2_i >$ and its exchange publicly, the adversary can gain access to it and manipulate it. Assume adversary select his parameter $M1_i^*$, T_1^* and b_i^* instead of $M1_i, T_1, b_i$. As the adversary is an insider, he can easily access database information to calculate M2$_i$.

Step 3: As $M2_i = h(M_i||N_i||d_i)$ and attacker get M_i, N_i information using stolen verifier and the only thing now attacker want is d_i and he calculate it using $d_i = (M_i||N_i||T1||) \oplus M1_i$. Now the malicious entity can impersonate as he calculated the parameters using available information.

Doctor -U1	Medical Server - (S)	Doctor -U2
		Insert Smart Card Input ID$_2*, pw_2*$ p$_2* = h(ID_2*\|\|pw_i*\|\|a_2)$ N$_2* = A_2 \oplus p_2*$ bID$_2*$=$h(b_2\|\|ID_2*)$ M$_2*$=$h(b_2\|\|ID_2*\|\|bID_2*)$ B$_2*$=$h(M_2*\|\|N_2*\|\|p_2*)$ B$_i$=B_i* Select Random Number r$_2$ AID$_1 = h(ID\|\|r_2) \oplus ID_2$ K$_1 = h(ID_2\|\|r_2)$
	$\xleftarrow{M3=\{Q_j,T_3,Auth_j\}}$	
Input ID$_1*, Pw_1*$ p$_1* = h(ID_1*\|\|pw_i*\|\|a_1)$ N$_1* = A_1 \oplus p_1*$ bID$_1*$=$h(b_1\|\|ID_1*)$ M$_1*$=$h(b_1\|\|ID_1*\|\|bID_1*)$ B$_1*$=$h(M_1*\|\|N_1*\|\|p_1*)$ B$_1$=B_1* ID$_2* = AID_1 \oplus h(ID_1\|\|r_2)$ K$_1* = h(ID_2*\|\|r_2), K1* =?K1$ Select random number r$_1$ BID$_1 = h(SID\|\|r1) \oplus ID_1$ k$_2 = h(ID_1\|\|r1)$ CID$_1 = h(SID\|\|r1) \oplus ID_2$ k$_3 = h(ID_2\|\|r2)$ k$_4 = h(k_2\|\|k_3)$		
	$\xrightarrow{M4=\{k_4,r1,r2,BID_1,CID_1\}}$	

	ID$_1 = h(SID\|\|r_1) \oplus BID_1$
	k$_2 = h(ID_1\|\|r1)$
	ID$_2 = h(SID\|\|r_2) \oplus CID_1$
	k$_3 = h(ID_2\|\|r2)$
	k$_4 = h(k_2\|\|k_3)$
	k$_4* =?k_4$
	Update ACL for U$_1, U_2$	

FIGURE 5. Amintoosi et al ownership tranfer phase.

C. MALICIOUS SERVER IMPERSONATION

Step 1: Msg are publicly exchange using parameters $< d_i, z_j, y_j, T_2 >$

Step 2: Medical server store information G_j, IDs_j, f_j.

Step 3: d_i is calculated using above step, T_2^* is selected by adversary. Now he calculate $W_j = h(IDs_j||s||f_j)$. Here IDs_j and f_j are sent publicly while s is the server primary key, availed through stolen verifier

Step 4: $y_j = (w_j||G_j||q_p)$ here G_j is publicly available, w_j is calculated from above step and q is random number.

Step 5: $z_j = h(d_i||IDs_j||f_j) \oplus q_p$

D. LACK OF INPUT VERIFICATION

The doctor enter the information ID_i, Pw_i then generate $p_i = h(ID_i||pw_i||a_i)$ with random number. However the doctor information in slight is never inspected. Therefore if the doctor enter problematic data, accidentally or purposely the extra calculation and searching take place which increase time complexity. Thus i can avoid un necessary operation.

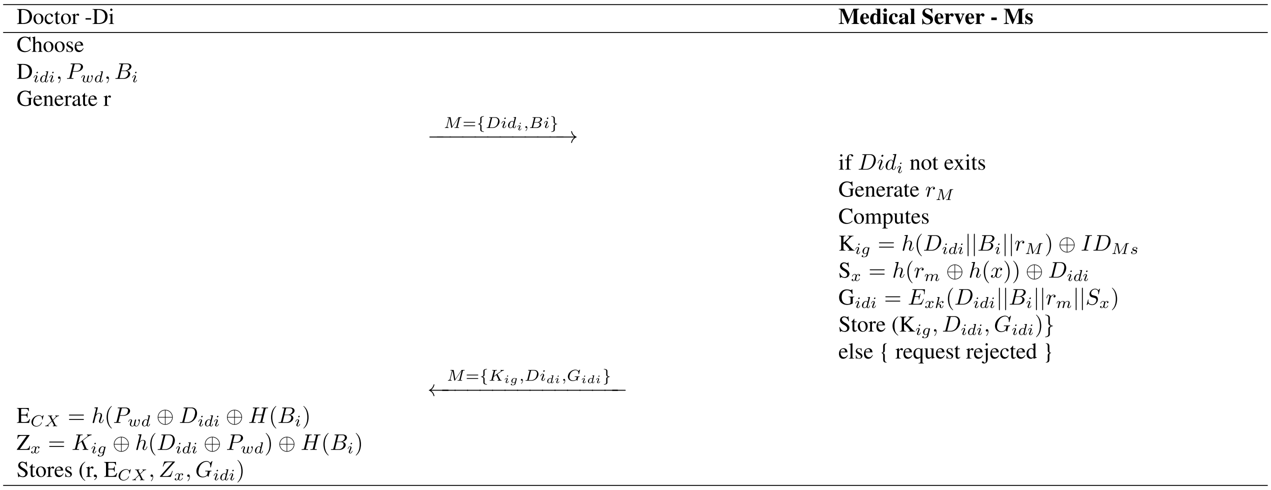
V. THE PROPOSED APPROACH

In this research section, we crafted a thorough plan to enhance smart healthcare. The proposed scheme is designed in IOMT settings for the scenario of remote monitoring of patients. IOMT belongs to critical infrastructure of any country, that is designed to gather health related data from sensors. Remote monitoring allows health practitioners to gauge the patient vitals that do not require hospital admission. These patients require continuous monitoring and are usually patients with chronic diseases. Sensors provide information related to patients vitals that can be accessed by the doctors to make timely decision. These sensor may include Diagnostic ECG sensors,Blood Glucose Sensors,Oximeter,Blood Pressure, Temperature,EEG,Accelerometer sensors to name a few.Researchers [41] in sensor design are working towards manufacturing of specialized sensor for remote patient monitoring. The proposed approach is based upon the security of the communication of these sensors with Servers and Doctors. Our strategy covers doctor and sensor registration, user authentication, and password management. As researchers, our main aim was to create a complete solution that simplifies user onboarding while guaranteeing security and confidentiality. We also prioritized a robust password-changing system. Our goal is to contribute to the improvement of smart healthcare by ensuring data security, especially as technology advances. Notation Table for our scheme is as follow: -

A. DOCTOR REGISTRATION PHASE

$i \Rightarrow$ New User request its ID which is D_{idi} from the medical server $M_s$using a secure way by giving its id, and password. Then generate a random number r

ii $\Rightarrow$ The Medical server generate a random no if the id is not already location R_m of 128bits and computes $K_{ig} =$



Doctor -Di | **Medical Server - Ms**

Choose
D_{idi}, P_{wd}, B_i
Generate r

$\xrightarrow{M=\{Did_i, Bi\}}$

if Did_i not exits
Generate r_M
Computes
$K_{ig} = h(D_{idi}||B_i||r_M) \oplus ID_{Ms}$
$S_x = h(r_m \oplus h(x)) \oplus D_{idi}$
$G_{idi} = E_{xk}(D_{idi}||B_i||r_m||S_x)$
Store ($K_{ig}, D_{idi}, G_{idi})\}$
else { request rejected }

$\xleftarrow{M=\{K_{ig}, D_{idi}, G_{idi}\}}$

$E_{CX} = h(P_{wd} \oplus D_{idi} \oplus H(B_i)$
$Z_x = K_{ig} \oplus h(D_{idi} \oplus P_{wd}) \oplus H(B_i)$
Stores (r, $E_{CX}, Z_x, G_{idi})$

FIGURE 6. Proposed doctor registration phase.

TABLE 2. Notation table of proposed scheme.

Notations	Description
S_e , M_s , D_i	Sensor Node ,Medical Server and Doctor
S_r, r, r_m , n_o	Random Numbers , Nonce
D_{id} Se_{id}	Doctor ID & Sensor ID
ID_{MS}	Medical Server ID
B_i	Biometric
x	Master Secret Key
M_{1-5}, T_{1-5}	Messages , Time
E_{xk}	Encrption
$\|\|$, $\oplus$	Concatenation operator , XOR operator
$\triangle$	Matching Algorithm
S_D , S_S	Session Key Doctor , Session Key Sensor
SM_s K_{se}	Session Key Medical Server , Sensor Secret

$h(D_{idi}||B_i||r_M) \oplus ID_{Ms}$. The Ms also computes $S_x = h(r_m \oplus h(x)) \oplus D_{idi}$ and $G_{idi} = E_{xk}(D_{idi}||B_i||r_m||S_x)$ and stores $(K_{ig}, D_{idi}, G_{idi})$ to use further.

$iii \Rightarrow$ In third step the Medical Server personalize with K_{ig}, Di_{di}, G_{idi} and then issue it to the user or doctor using secure communication channel.

$iv \Rightarrow$ The doctor computes $E_{CX} = h(P_{wd} \oplus D_{idi} \oplus H(B_i)$ $Z_x = K_{ig} \oplus h(D_{idi} \oplus P_{wd}) \oplus H(B_i)$

then the doctor stores information by the medical server $(r, E_{CX}, Z_x, G_{idi})$.

B. SENSOR REGISTRATION PHASE

$i \Rightarrow$ New Sensor generate random number S_r *thencompute* $F_i = h(Se_{id}||K_{se}||S_r)$ and send information to medical server privately. $ii \Rightarrow$ The Medical server than computes $M_j = h(Se_{id}||x||S_r||F_i)$ and stores F_i, Se_{id}, S_r and then increment the random number and encrypt Mj with its keys $E_{nc} = E_{xk}(M_j)$ and send E_{nc} toward sensor node.

$iii \Rightarrow$ In third step the Sensor stores (E_{nc}, S_r).

C. AUTHENTICATION PHASE

Authentication is conducted among the user, the medical server, and the designated sensor in this phase. Encryption and decryption are executed on the medical server (Ms). The phase includes the stages shown in Figure 8.

$\triangleright$ $i \Longrightarrow$ In Message M1: from user to medical server the use send $ID_{Ms}, V_{er}, T1$ to the medical server. In the occurrence that a user or doctor requires real-time information from a sensor Se_{id}, the user will provide its D_{id} and password P_a. Just after that a calculation and computes $E_{CX*} = h(Pwd, D_{id}, H(B_i))$ and then verify E_{CX} which is saved credential with newly entered informatina $E_{CX}*$ if both are same its means the doctor is authentic. and then the furture computation take places $Z'_x = K_{ig} \oplus (h(D_{id}, P_{wd}) \oplus H(B_i))$ $V_{er} = h(Z'_x \oplus (T_1 \oplus G_{idi})$. Then lastly user generate a request message $M1 = \{ID_{Ms}, V_{er}, T1\}$ Afterwards then the message is routed to the medical server for authentication.

triangleright $ii \Longrightarrow$ When the message M2: from Medical Server to Sensor Enc_{new}, T_2 arrives, firstly freshness is checked $T2 - T1 \leq \triangle$ T. The medical server performs decryption on G_{idi} via $(D_{idi}||B_i||r_m||S_x) = D_{xk}(G_{idi})$ and computes $\overline{S_x} = h((r_m \oplus h(x) \oplus D_{id}))$ after that $\overline{S_x}$ is verified with stored S_x if both are same its verify and then server computes $Mj_{new} = h(Se_{id}, S_r, x, F_i)$ and encrypted the Mj_{new} and create a message $M2$ and passes it to the sensor for which user want to communicate.

$\triangleright$ $iii \Longrightarrow$ Upon message M2 reception, the sensor node initially verifies the timestamp $T3 - T2 \leq \triangle T$ and then decrypt $D_{xk}(Enc_{new}) = Mj_{new}$ and extract Mj_{new} and generate random number r_b computes $Z_x = h(Se_{id}||r_b||x)$ and encrypt $Z_{xenc} = E_{xk}(Z_x, r_b)$ and send Z_{xenc} toward medical server. The medical server checked freshness and decrypt (Z_{xenc}) to get (Z_x, r_b) then computes $Zx_{new} = h(Se_{id}||r_b||x)$ and verify Zx_{new} with the stored Z_x and generate r_v and computes $V1 = h(G_{idi}, r_v, T\ 5, Mj_{new})$ and $V2_{ex} = E_{xk}(V1, Mj_{new}, r_v)$. The doctor decrypt $D_{xk}(V_{2ex}) = V1, Mj_{new}, r_v$ and computes $V1_{new} = h(G_{idi}, r_v, T5, Mj_{new})$ and Stores $(G^{new}_{idi}, Z^{new}_x, E_{cx}, r)$.

D. PASSWORD UPDATION

The proposed protocol enables a user to change their password without needing server assistance. When a user

Sensor -Se		**Medical Server - Ms**
Generate random S_r $F_i = h(Se_{id} \Vert K_{se} \Vert S_r)$		
	$\xrightarrow{M=\{F_i,S_r,Se_{id}\}}$	
		$M_j = h(Se_{id} \Vert x \Vert S_r \Vert F_i)$ Stores F_i, Se_{id}, S_r r = r +1 $E_{nc} = E_{xk}(M_j)$
	$\xleftarrow{M=\{E_{nc}\}}$	
Stores (E_{nc}, S_r)		

FIGURE 7. Proposed sensor registration phase.

Doctor -Di	**Medical Server - Ms**	**Sensor - Se**
Input D_{id}, P_{wd} Imprint B_i $E_{CX}* = h(Pwd, D_{id}, H(B_i))$ Verify if $E_{CX} \overset{?}{=} E_{CX} *$ $Z'_x = K_{ig} \oplus (h(D_{id}, P_{wd}) \oplus H(B_i))$ $V_{er} = h(Z'_x \oplus (T_1 \oplus G_{idi})$ $\xrightarrow{M1=\{ID_{Ms},V_{er},T1\}}$		
	Verify T2 - T1 $\leq \triangle T$ Compute $(D_{idi} \Vert B_i \Vert r_m \Vert S_x) = D_{xk}(G_{idi})$ $\overline{S_x} = h((r_m \oplus h(x) \oplus D_{id}))$ Verify if $\overline{S_x} \overset{?}{=} S_x$ $Mj_{new} = h(Se_{id}, S_r, x, F_i)$ $Enc_{new} = Exk(Mj_{new})$ $\xrightarrow{M2=\{Enc_{new},T_2,\}}$	
		Verify T3 - T2 $\leq \triangle T$ $D_{xk}(Enc_{new}) = Mj_{new}$ Verify $Mj_{new} = Mj$, Generate r_b $Z_x = h(Se_{id} \Vert r_b \Vert x)$ $Z_{xenc} = E_{xk}(Z_x, r_b)$ $\xleftarrow{M3=\{Z_{xenc},T4\}}$
	Verify T4 - T3 $\leq \triangle T$ $D_{xk}(Z_{xenc}) = (Z_x, r_b)$ $Zx_{new} = h(Se_{id} \Vert r_b \Vert x)$ Verify $Zx_{new} \overset{?}{=} Z_x$ Generate r_v V1 = h ($G_{idi}, r_v, T5, Mj_{new})$ $V2_{ex} = E_{xk}(V1, Mj_{new}, r_v)$ $\xleftarrow{M4=\{V2_{ex},T_5\}}$	
Verify T5 - T6 $\leq \triangle T$ $D_{xk}(V_{2ex}) = V1, Mj_{new}, r_v$ $V1_{new} = h(G_{idi}, r_v, T5, Mj_{new})$ if $V1_{new} \overset{?}{=}$ V1 Stores $(G^{new}_{idi}, Z^{new}_x, E_{cx}, r)$		

FIGURE 8. Proposed authentication phase.

needs to modify their password, they only need to insert D_{idi}, previous password P_{wd}, biometric and computes $E_{CX} = h(P_{wd} \oplus D_{idi} \oplus H(B_i)$ After verifying the previous E_{CX} the user to input a new password $P_{wd}*$. Remote patient monitoring which enable secure access to real-time patient data collected from wearable health devices, such as continuous glucose monitors, fitness trackers, and heart rate monitors.

VI. SECURITY ANALYSIS

Due to the sensitive nature of the data, authentication is crucial in smart healthcare. Protecting patient privacy and preventing unauthorized access are essential. As data travels over networks, strong authentication protects against data breaches and online dangers. Medical mistake rates are reduced when healthcare providers and patients are authorized. Networked devices are also secured to safeguard healthcare networks and patient safety.

A. FORMAL SECURITY ANALYSIS

We performed formal security analysis of the scheme in Proverif. Proverif has a good reputation for its exceptional flexibility and efficacy in analyzing cryptographic systems. This versatile tool excels at managing complex procedures such as encryption and digital signatures with ease. Its strength comes in the use of sophisticated reasoning, which allows for the rapid verification of protocols while adeptly spotting subtle security weaknesses, such as the possibility of data leaking. Because of its ability to quickly adapt to emerging cryptographic difficulties, the tool is a vital asset in the domain of formal protocol analysis. ProVerif is a powerful tool for the study of authentication systems and cryptographic protocols due to its mix of solid capabilities, user-friendly design, strong community support, and extensive documentation.The Figure 9 represents the prover if result of the proposed scheme. For example Query not attacker(encnew[]) is true:evaluates whether the entity encnew[] can be considered an attacker in the analyzed system. The result ''true'' indicates that encnew[] is confirmed not to be an attacker.

Query not attacker(zx1[]) is true:assesses whether the entity zx1[] qualifies as an attacker. The outcome ''true'' confirms that zx1[] is not considered an attacker.

Query not attacker(v3[]) is true:query examines the entity v3[] to determine if it can be classified as an attacker. The result ''true'' affirms that v3[] is not an attacker.

Query inj-event(end$_{D}octor(DID[]))$ $==>$
$inj - event(start_{D}octor(DID[]))istrue$

This query investigates whether the ending event of a Doctor action implies the occurrence of the starting event of a Doctor action in terms of injecting events. The result ''true'' indicates that there is such an implication.

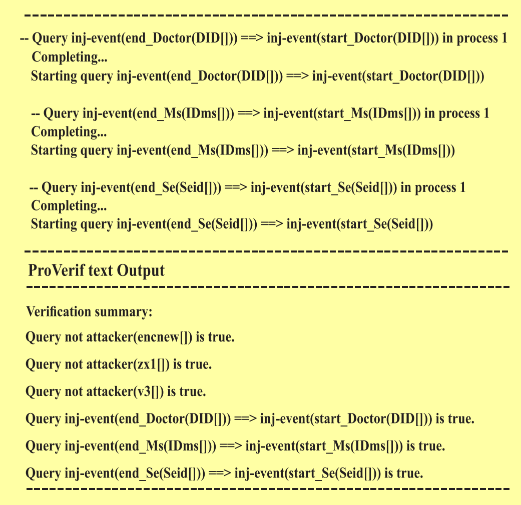
Query inj-event(end$_{M}s(IDms[]))$ $==>$
$inj - event(start_{M}s(IDms[]))istrue$:

Similarly, this query assesses whether the ending event of a Medical Service (Ms) action implies the occurrence of the starting event of a Medical Service action in terms of injecting events. The result ''true'' confirms the existence of this implication.

Query inj-event(end$_{S}e(Seid[]))$ $==>$
$inj - event(start_{S}e(Seid[]))istrue$:

This query evaluates whether the ending event of a Secondary Entity (Se) action implies the occurrence of the starting event of a Secondary Entity action in terms of injecting events. The outcome ''true'' indicates the presence of this implication.

Overall, these results suggest that the specified conditions and implications hold true within the analyzed system according to the ProVerif analysis. It is pertinent to mention that baseline protocol was simulated in ProVerif whereby it was found vulnerable to stolen verifier, impersonation attacks and man in the middle attacks that are handled in the proposed scheme.



```
 ------------------------------------------------------------------
-- Query inj-event(end_Doctor(DID[])) ==> inj-event(start_Doctor(DID[])) in process 1
  Completing...
  Starting query inj-event(end_Doctor(DID[])) ==> inj-event(start_Doctor(DID[]))

  -- Query inj-event(end_Ms(IDms[])) ==> inj-event(start_Ms(IDms[])) in process 1
  Completing...
  Starting query inj-event(end_Ms(IDms[])) ==> inj-event(start_Ms(IDms[]))

  -- Query inj-event(end_Se(Seid[])) ==> inj-event(start_Se(Seid[])) in process 1
  Completing...
  Starting query inj-event(end_Se(Seid[])) ==> inj-event(start_Se(Seid[]))

 ------------------------------------------------------------------
 ProVerif text Output
 ------------------------------------------------------------------

 Verification summary:

 Query not attacker(encnew[]) is true.

 Query not attacker(zx1[]) is true.

 Query not attacker(v3[]) is true.

 Query inj-event(end_Doctor(DID[])) ==> inj-event(start_Doctor(DID[])) is true.

 Query inj-event(end_Ms(IDms[])) ==> inj-event(start_Ms(IDms[])) is true.

 Query inj-event(end_Se(Seid[])) ==> inj-event(start_Se(Seid[])) is true.
 ------------------------------------------------------------------
```

FIGURE 9. **Proverif result.**

B. THEORETICAL SECURITY ANALYSIS

1) EAVESDROPPING ATTACK

A security risk called eavesdropping includes hackers secretly intercepting communication in search of useful information. The protocol uses session encryption and frequent updates to prevent this, making it challenging to eavesdrop on talks taking place on public channels.

2) INSIDER ATTACK

The protocol protects against insider attacks by producing distinct session parameters for each session, making attacks in later sessions impossible due to the absence of access to updated parameters. Insider attacks happen when a legitimate entity targets the system, but the protocol prevents them by preventing this from happening.

3) STOLEN CARD ATTACK

A smartcard can be attacked using power analysis since it can hold sensitive information needed for authentication. Even if the smartcard is lost, the danger can be reduced by using various authentication techniques, such as biometrics.

4) STOLEN VERIFIER

In the stolen verifier attack, verification data from earlier sessions is obtained and made unencrypted, giving any attacker access to confidential data. The suggested method eliminates the possibility of verifier theft and improves system security by substituting user-supplied information for server-side verification to prevent this.

5) TRACEABILITY

In the stolen verifier attack, verification data from earlier sessions is obtained and made unencrypted, giving any attacker access to confidential data. The suggested method eliminates the possibility of verifier theft and improves system security by substituting user-supplied information for server-side verification to prevent this.

6) REPLAY ATTACK

When an opponent intercepts and replays messages without making any changes, it is called a replay assault. The protocol uses G_{idi} updated after each session to prevent this and embeds a timestamp (T) to assure message freshness. This makes the protocol resistant to replay assaults because parameters change after each session.

7) ANONYMITY

User anonymity is essential for security applications, and the proposed protocol protects it by keeping user identities hidden throughout communication on public channels. In order to provide strong user anonymity, this is done by fully encrypting the session parameter G_{idi} and prohibiting attackers from obtaining user data through the Server Node or Sensor Node Sn.

8) PERFECT FORWARD SECRACY

In the suggested approach, user identification and G_{idi} are encrypted with a random number and multi-factor authentication, and the session is updated frequently with new values. With this strategy, forward secrecy is guaranteed since even if an attacker knows the password, they will be unable to decrypt G_{idi}.

9) DENIAL OF SERVICE

The proposed protocol demonstrates excellent resilience against denial of service attacks by using timestamps and random numbers to assure message novelty and discourage adversaries from sending repetitive messages.

10) PASSWORD GUESSING ATTACK

The proposed protocol protects against guessing attacks by updating all session settings after each session and routinely encrypting them. Since new encrypted information is used for each session, it is difficult for attackers to figure out the password through the public channel thanks to this approach.

TABLE 3. Security attributes.

S A1	Resistance to password guessing
S A2	Dos Attack
S A3	Resistance to Replay Attack
S A4	insider attack
S A5	Resistance to known session attack
S A6	Resistance to sensor
S A7	User impersonation attack
S A8	Server impersonation attack
S A9	Resistance of known-key secrecy
S A10	Implementation of perfect forward secrecy
S A11	Implementation of password update
S A12	Stolen Verifier Attack

TABLE 4. Security analysis table.

SA	[13]	[42]	[20]	[11]	[17]	[3]	
et al	Mishra	Lu	Khatoon	Zhang	Hamid	Slight	Our
$\mathbf{S}_{A1}$	×	×	Y	Y	Y	Y	Y
$\mathbf{S}_{A2}$	×	×	×	×	Y	Y	Y
$\mathbf{S}_{A3}$	×	Y	Y	Y	Y	Y	Y
$\mathbf{S}_{A4}$	Y	Y	×	×	×	Y	Y
$\mathbf{S}_{A5}$	×	×	×	×	×	Y	Y
$\mathbf{S}_{A6}$	×	×	×	×	Y	×	Y
$\mathbf{S}_{A7}$	×	×	Y	Y	Y	×	Y
$\mathbf{S}_{A8}$	×	×	Y	Y	×	×	Y
$\mathbf{S}_{A9}$	×	×	×	×	×	Y	Y
$\mathbf{S}_{A10}$	×	Y	×	Y	Y	Y	Y
$\mathbf{S}_{A11}$	Y	Y	Y	×	×	Y	Y
$\mathbf{S}_{A12}$	×	×	×	×	×	×	Y

11) MAN IN MIDDLE ATTACK

The suggested technique offers strong resilience to man-in-the-middle attacks by using continuously refreshed encrypted parameters in each new user-initiated session.

×: No ,Y: Yes

The security analysis demonstrates that our authentication system is resistant to a wide range of cyber threats. It can handle a variety of attacks and provides adequate protection for the system's overall security. This multi-defense strategy secures the environment and provides assurance that the authentication system can deal with new cyber threats.

VII. COMPARATIVE ANALYSIS

In this section, performance analysis of the scheme in comparison with Mishra et al. [13], Camara et al. [43], Khatoon et al. [20], Mehmood et al. [44], and Wong et al. [14] are presented. Additionally a comparison to the computation and communication duration with the aforementioned schemes is also mentioned.

A. COMPUTATION AND COMMUNICATION COST

The experimental procedures were conducted on a robust Ubuntu system featuring an Intel dual-core Pentium processor boasting specifications of 2.20 GHz clock speed, complemented by 2048 MB of processor and RAM, respectively. This system configuration provided a solid foundation for the comprehensive execution of the research experiments.

1) COMPUTATIONAL COST

For assessing the efficacy of authentication techniques in cyber security, computational cost in authentication, including processing power and time, is essential. In order to maintain system resilience against attacks without severe delays, it is essential to strike a balance between security and computing efficiency. The robustness of the authentication system is achieved by safeguarding sensitive data, and safeguarding user privacy by optimizing computing costs.

Table 5 delineates the symbols used for computing cost evaluations. The execution timings are presented in [45].

TABLE 5. Notation used for computational cost.

Symbol	Description height
Thf	Time required for hash Function
Ten/f	Time required for Symmetric encryption/decryption
Tmu	Time required for Scalar Multiplication of Elliptive Curve
Tad	Time required for Addition of Elliptive Curve
Tbh	Time required for biohashing height

TABLE 6. Computational cost comparison.

Scheme	Total Computation	Time (ms)
Khatoon et al. [20]	5Tmu + 12Thf + 2Ten/d	37.0299
Sharif [46]	4Tmu + 19Thf + 2Ten/d + 4Tad	29.71
Arshad [19]	4Tmu + 23Thf + 2Tad	29.43
Sharif [18]	4Tmu + 14Thf + 2Ten/d	29.41
Lu [42]	4Tmu + 14Thf	29.4172
Chen [45]	16Thf + 4Ten/d	0.522
Mishra [13]	16Thf + 3Ten/d + 2Tbh	0.4173
Wong [14]	14Th + 3Ten/d	0.3965
Zahid [44]	15Thf + 2Ten/d	0.2613
Slight [3]	22Thf	0.0507
Proposed	8Thf +6Ten/d	0.04

Hence, the estimated execution durations of Th f Ten/d, Tmu,and Tex are 0.0023 ms, 0.0046 ms, 2.226 ms, and 3.85 ms, respectively. In proposed scheme, Eight hash function operations and six Encryption Decryption are needed. So the proposed scheme incurs 8Thf +6Ten/d computation overhead. In Table 6 and Figure 10, we compared the computation time of Proposed scheme with Khatoon et al. [20] Sharif et al. [46] Arshad et al. [19] Sharif et al. [18] Lu et al. [42] Chen et al. [45] Mishra et al. [13] Wong et al. [14] Mehmood et al. [44] Slight [3]. Proposed Scheme outperforms others by incurring the total computation cost of 0.04ms, while it is 37.0299 ms for Khatoon et al. [20], 29.71 ms for Ostad-Sharif et al. [46], 29.43 ms for Arshad and Nikooghadam [19], 29.41 ms for Ostad-Sharif et al. [18], 29.417 ms for Lu et al. [42], 0.522 ms for Chen et al. [45], 0.4173 ms for Mishra et al. [13], 0.3965 ms for Wong et al. [14] , 0.2613 ms for Mehmood et al. [44].Furthermore, as depicted in Table 4, the Proposed Scheme demonstrates stronger resistance against security threats.

B. COMMUNICATION COST

We also assess proposed scheme's communication efficiency during the login and authentication phase by measuring the length of exchanged messages in bits. The breakdown of communication costs includes 160 bits for identity, 32 bits for the timestamp,128 bits for encryption/decryption, 320 bits for elliptic curve point multiplication, 32 bits for the realm, and 32 bits for random number generation, along with 160 bits for the output hash function as described in the Table 7. The findings from the comparison of communication overhead, detailed in Table 8 highlight that our scheme maintains an acceptable level of communication efficiency when compared to similar schemes.

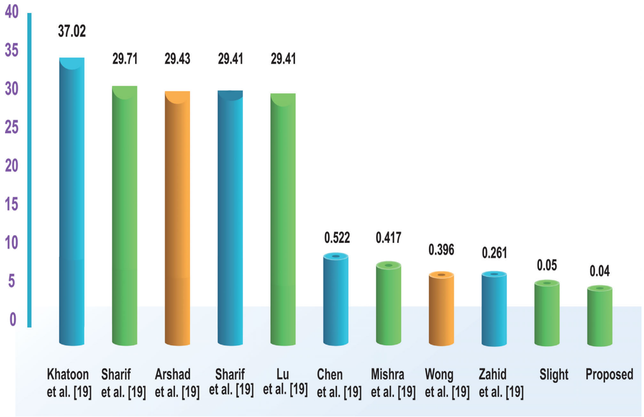


FIGURE 10. The computation cost.

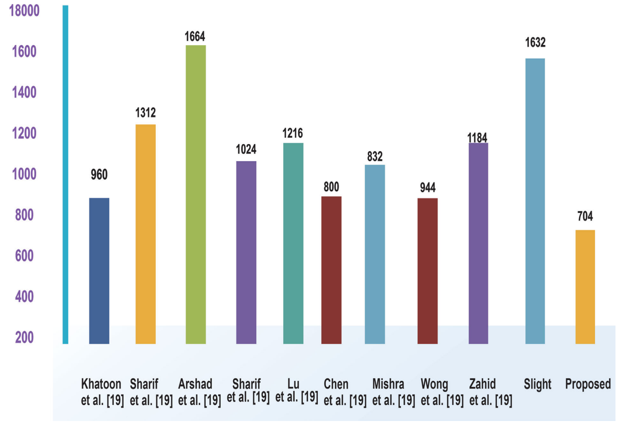


FIGURE 11. The communication in bits.

TABLE 7. Communication cost units.

Term	Communication Cost
Sending Identity	160bits
Time Stamp	32bits
Encryptiong, Decryption	128bits
Elliptic Curve Point Mulitplication	320bits
Realm	32bits
Random Number	32bits
Output HashFunction	160bits

C. PERFORMANCE EVALUATION

In this section the proposed method is compared to previous relevant studies addressing communication and computing costs. As shown in the table 9 the Amintoosi et al scheme [3] required 22Thf computation function and computation cost of 0.05 along with communication cost of 1632Bits while the proposed scheme required 8Thf and 6Ten/d function

TABLE 8. Communication cost comparison.

Scheme	1st Message	2nd	3rd	4th	Total
Khatoon et al. [20]	480	480	Nil	Nil	960
Sharif [46]	672	640	Nil	Nil	1312
Arshad [19]	704	800	160	Nil	1664
Sharif [18]	640	608	Nil	Nil	1024
Lu [42]	512	512	192	Nil	1216
Chen [45]	128	160	512	Nil	800
Mishra [13]	320	352	160	Nil	832
Wong [14]	320	184	320	120	944
Zahid [44]	512	512	160	Nil	1184
Slight [3]	384	384	352	512	1632
Proposed	544	352	352	352	704

with the computational cost of 0.04 and communication cost of 704 Bits.

TABLE 9. Performance evaluation.

Scheme	Total Computation	Comp (ms)	Comm (Bits)
Khatoon et al. [20]	5Tmu + 12Thf + 2Ten/d	37.0299	960
Sharif [46]	4Tmu + 19Thf + 2Ten/d + 4Tad	29.71	1312
Arshad [19]	4Tmu + 23Thf + 2Tad	29.43	1664
Sharif [18]	4Tmu + 14Thf + 2Ten/d	29.41	1024
Lu [42]	4Tmu + 14Thf	29.4172	1216
Chen [45]	16Thf + 4Ten/d	0.522	800
Mishra [13]	16Thf + 3Ten/d + 2Tbh	0.4173	832
Wong [14]	14Th + 3Ten/d	0.3965	944
Zahid [44]	15Thf + 2Ten/d	0.2613	1184
Slight [3]	22Thf	0.0507	1632
Proposed	8Thf +6Ten/d	0.04	704

VIII. DISCUSSION

Smart healthcare systems are rapidly utilizing IoMT (Internet of Medical Things). It facilitates in the reduction of unnecessary hospital charges, the more easy connection of patients with their doctors, and the secure transfer of medical data over communication networks. However as discussed earlier these systems suffer security threats. We have developed an authentication scheme for the scenario of remote monitoring of patients in an IOMT setup. Through formal and informal verification it is achieved that in terms of computing and communication the proposed scheme is the most cost-effective. It improves security by preventing well-known attacks including stolen verifier, user impersonation, and server impersonation. Previous such technique was vulnerable to these attacks with greater cost.A thorough security analysis highlights that authentication solution can withstand a wide variety of attacks. By strengthening the security environment and assuring trust in the authentication system's ability to counter new cyberthreats, this multi-defense approach improves security by using encrypted session frequent updated timestamp and biometrics along with the cost effectiveness.

A. LIMITATION

In case if an adversary manages to uncover or replicate an individual's biometric details, such as fingerprints, rectifying the situation becomes challenging, compromised biometric data poses a persistent security threat over an extended period.

IX. CONCLUSION

Given recent advancements in the Internet of Medical Things (IoMT), protecting patient privacy is a critical problem that requires attention. This study first looked at the authentication technique developed by Amintoosi et al. [3] for IoMT and revealed its vulnerability of stolen verifier and subsequently impersonation attacks. Then we have worked to improve smart healthcare authentication in four crucial areas. Firstly the proposed solution improves medical data security by addressing vulnerabilities such as stolen verifiers and password encryption. By streamlining login processes and minimizing breaches, proposed strategy not only improves security but also lowers overall expenditures by transmission cost of 704 bits and processing to 0.04 Ms. The proposed approach speeds up procedures without sacrificing safety, resulting in more efficient operations. We also prioritized ease of use for healthcare professionals and patients while maintaining security by inclusion of bio metrics. Extensive security evaluations and comparative analysis confirmed its robustness and efficiency, resulting in its suitability for remote health monitoring scenario, where privacy and operational efficiency are critical.

X. FUTURE WORK

Healthcare authentication has improved significantly, however there are still many areas that need further research and development. Advanced biometric techniques, such as facial recognition, can improve security even further and make it simpler for consumers.

ACKNOWLEDGMENT

This project is funded by UJ-02-032-DR funding provided by University of Jeddah, Jeddah, Saudi Arabia.

REFERENCES

[1] M. Alshamrani, "IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 8, pp. 4687–4701, Sep. 2022.

[2] S. A. Baho and J. Abawajy, "Analysis of consumer IoT device vulnerability quantification frameworks," *Electronics*, vol. 12, no. 5, p. 1176, Feb. 2023.

[3] H. Amintoosi, M. Nikooghadam, M. Shojafar, S. Kumari, and M. Alazab, "Slight: A lightweight authentication scheme for smart healthcare services," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107803.

[4] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102494.

[5] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, pp. 1–41, May 2017.

[6] M. Karuppiah and R. Saravanan, "A secure authentication scheme with user anonymity for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 84, no. 3, pp. 2055–2078, Oct. 2015.

[7] M. Karuppiah, S. Kumari, X. Li, F. Wu, A. K. Das, M. K. Khan, R. Saravanan, and S. Basu, "A dynamic ID-based generic framework for anonymous authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 93, no. 2, pp. 383–407, Mar. 2017.

[8] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*, vol. 10, no. 4, pp. 1370–1379, Dec. 2016.

[9] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in global mobility networks," *J. Netw. Comput. Appl.*, vol. 107, pp. 83–92, Apr. 2018.

[10] P. Gope and T. Hwang, "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 1–8, Feb. 2016.

[11] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for E-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.

[12] T.-Y. Wu, L. Yang, Z. Lee, S.-C. Chu, S. Kumari, and S. Kumar, "A provably secure three-factor authentication protocol for wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–15, Apr. 2021.

[13] D. Mishra, J. Srinivas, and S. Mukhopadhyay, "A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 10, pp. 1–10, Oct. 2014.

[14] A. M.-K. Wong, C.-L. Hsu, T.-V. Le, M.-C. Hsieh, and T.-W. Lin, "Three-factor fast authentication scheme with time bound and user anonymity for multi-server E-health systems in 5G-based wireless sensor networks," *Sensors*, vol. 20, no. 9, p. 2511, Apr. 2020.

[15] K. Shahzad, M. U. Farooq, M. Zeeshan, and S. A. Khan, "Adaptive multi-input medium access control (AMI-MAC) design using physical layer cognition for tactical SDR networks," *IEEE Access*, vol. 9, pp. 58364–58377, 2021.

[16] I. Masood et al., "A blockchain-based system for patient data privacy and security," *Multimedia Tools Appl.*, 2024, doi: 10.1007/s11042-023-17941-y.

[17] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for E-health systems in IoT," *Future Gener. Comput. Syst.*, vol. 96, pp. 410–424, Jul. 2019.

[18] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC," *Int. J. Commun. Syst.*, vol. 32, no. 5, p. e3913, Mar. 2019.

[19] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 12, pp. 1–12, Dec. 2014.

[20] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, "Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," *IEEE Access*, vol. 7, pp. 47962–47971, 2019.

[21] O. Akrivopoulos, I. Chatzigiannakis, C. Tselios, and A. Antoniou, "On the deployment of healthcare applications over fog computing infrastructure," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jul. 2017, pp. 288–293.

[22] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-aware efficient fine-grained data access control in Internet of Medical things based fog computing," *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[23] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary, and C.-M. Chen, "CSEF: Cloud-based secure and efficient framework for smart medical system using ECC," *IEEE Access*, vol. 8, pp. 107838–107852, 2020.

[24] N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany, and A. Elchouemi, "Enhanced e-health framework for security and privacy in healthcare system," in *Proc. 6th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, Apr. 2016, pp. 75–79.

[25] 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," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[26] S. A. Chaudhry, A. Irshad, J. Nebhen, A. K. Bashir, N. Moustafa, Y. D. Al-Otaibi, and Y. B. Zikria, "An anonymous device to device access control based on secure certificate for Internet of Medical things systems," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103322.

[27] F. Wu, X. Li, L. Xu, S. Kumari, and A. K. Sangaiah, "A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion," *Comput. Electr. Eng.*, vol. 68, pp. 107–118, May 2018.

[28] J. Kang, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang, "An ultra light weight and secure RFID batch authentication scheme for IoMT," *Comput. Commun.*, vol. 167, pp. 48–54, Feb. 2021.

[29] H. A. El Zouka, "An authentication scheme for wireless healthcare monitoring sensor network," in *Proc. 14th Int. Conf. Smart Cities, Improving Qual. Life Using ICT, IoT*, 2017, pp. 68–73.

[30] S. Das and S. Namasudra, "A lightweight and anonymous mutual authentication scheme for medical big data in distributed smart healthcare systems," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, pp. 1–12, 2022, doi: 10.1109/TCBB.2022.3230053.

[31] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: A survey," *Social Netw. Comput. Sci.*, vol. 3, no. 5, p. 382, Jul. 2022.

[32] T. Wan, L. Wang, W. Liao, and S. Yue, "A lightweight continuous authentication scheme for medical wireless body area networks," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 6, pp. 3473–3487, Nov. 2021.

[33] S. A. Chaudhry, H. Naqvi, M. S. Farash, T. Shon, and M. Sher, "An improved and robust biometrics-based three factor authentication scheme for multiserver environments," *J. Supercomput.*, vol. 74, no. 8, pp. 3504–3520, Aug. 2018.

[34] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 43, no. S1, pp. 619–636, Jul. 2019.

[35] B. A. Alzahrani, A. Irshad, K. Alsubhi, and A. Albeshri, "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT," *Int. J. Commun. Syst.*, vol. 33, no. 11, p. e4423, Jul. 2020.

[36] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, Feb. 2022.

[37] M. AbdulRaheem, G. B. Balogun, M. K. Abiodun, F. A. Taofeek-Ibrahim, A. R. Tomori, I. D. Oladipo, and J. B. Awotunde, "An enhanced lightweight speck system for cloud-based smart healthcare," in *Proc. 4th International Conference*, 2021, pp. 363–376.

[38] N. Garg, M. Wazid, J. Singh, D. P. Singh, and A. K. Das, "Security in IoMT-driven smart healthcare: A comprehensive review and open challenges," *Secur. Privacy*, vol. 5, no. 5, p. e235, Sep. 2022.

[39] F. Xu, S. Liu, and X. Yang, "An efficient privacy-preserving authentication scheme with enhanced security for IoMT applications," *Comput. Commun.*, vol. 208, pp. 171–178, Aug. 2023.

[40] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Privacy management of patient physiological parameters," *Telematics Informat.*, vol. 35, no. 4, pp. 677–701, Jul. 2018.

[41] N. Montaseri, Z. Khodkar, J. Abouei, W. G. Whittow, and K. N. Plataniotis, "A conformal leaky-wave antenna design for IoMT-based WBANs," *IEEE Access*, vol. 11, pp. 46719–46733, 2023.

[42] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 39, no. 3, pp. 1–8, Mar. 2015.

[43] C. Camara, H. Martín, P. Peris-Lopez, and M. Aldalaien, "Design and analysis of a true random number generator based on GSR signals for body sensor networks," *Sensors*, vol. 19, no. 9, p. 2033, Apr. 2019.

[44] Z. Mehmood, A. Ghani, G. Chen, and A. S. Alghamdi, "Authentication and secure key management in E-health services: A robust and efficient protocol using biometrics," *IEEE Access*, vol. 7, pp. 113385–113397, 2019.

[45] R. Chen, Y. Mou, and M. Zhang, "An improved anonymous DoS-resistant authentication protocol in smart city," *Wireless Netw.*, vol. 28, no. 2, pp. 745–763, Feb. 2022.

[46] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *J. Med. Syst.*, vol. 43, no. 1, p. 10, Jan. 2019.

ZOHAIB ALI received the M.S. degree in information security from Bahria University, Islamabad, Pakistan, in 2023. His research interests include cyber security, artificial intelligence, and machine learning.

SABA MAHMOOD received the Ph.D. degree in computer science from International Islamic University Islamabad, Pakistan. She is currently a Senior Assistant Professor with the Computer Science Department, Bahria University, Islamabad, where she is also administering the master's programs of the department. She has extensive academic and administrative experience of 14 years. Her research interests include trust, smart health, data science for cyber security, the IoT, machine learning, and social network analysis.

KHWAJA MANSOOR UL HASSAN received the Ph.D. degree in information security from the Military College of Signals, NUST. He has demonstrated his expertise in cybersecurity by conducting numerous audits for the Ministries of Pakistan as a member of the Country-Level Cybersecurity Audit Team, National Center of Cyber Security (NCCS). With ten years of experience in cyber security, information technology audits, internal audits, risk management, offensive pentesting, and applied cryptography, he is a seasoned professional in the field of cybersecurity. He is currently an Assistant Professor with the Cyber Security Department, Air University.

ALI DAUD received the Ph.D. degree in computer science from Tsinghua University, Beijing, China, in July 2010. He has 13 years of post-Ph.D. experience in teaching, supervision, and research at B.S., M.S., and Ph.D. levels. He is currently a Full Professor with the Faculty of Resilience, Rabdan Academy, Abu Dhabi, United Arab Emirates. He has taken part in many research projects as well and has written and acquired many research funding. He has proven and extensive experience in data mining, artificial intelligence (machine learning/deep learning) applications to social networks, data science, natural language processing, and the Internet of Things. He has published more than 100 research papers in reputed international impact factor journals and conferences.

RIAD ALHARBEY is currently an Assistant Professor with the Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. He has published many high-quality research papers in reputable international journals and conferences. He has taken part in many research projects as well. His research interests include data science, data mining, and artificial intelligence.

AMAL BUKHARI is currently an Assistant Professor with the Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. She has published several articles in reputable international journals. Her research interests include medical data science, bioinformatics, machine learning, and deep learning.