Design of Lightweight Authentication Scheme For Low Power Internet of Medical Things(IoMT)

1st Akash Poudel
Department of CSE
NIT Rourkela
Rourkela, India
poudelakash28@gmail.com

2nd Sujata Mohanty
Department of CSE
NIT Rourkela
Rourkela, India
sujatam@nitrkl.ac.in

3rd Manabhanjan Pradhan
Department of CSE
NIT Rourkela
Rourkela, India
mannpradhan@protonmail.com

***Abstract*—The Internet of Medical Things plays a key role in contemporary healthcare systems by leveraging sensor technology to monitor essential physiological parameters such as blood glucose levels, heart rate, and body temperature. However, safeguarding the integrity and confidentiality of the collected patient data and ensuring the security of these sensors is of utmost importance. Mitigating potential risks such as unauthorised sensor access or tampering with the transmitted data is imperative. When it comes to the Internet of Medical Things, authentication mechanisms must address various attack vectors, including but not limited to offline password guessing and insider impersonation. Previous research efforts have proposed user authentication schemes for the Internet of Medical Things; however, these schemes exhibited vulnerabilities to different attacks, jeopardising patient information confidentiality. An enhanced authentication scheme designed explicitly for resource-constrained Internet of Things sensors in healthcare contexts has been presented to tackle all these weaknesses. This scheme encompasses utilising hash functions and XOR operations tailored to suit the unique requirements of such low-spec sensors. Moreover, we have rigorously validated the proposed scheme's security using the ProVerif cryptographic protocol verification tool, demonstrating its robustness against adversarial threats. Notably, our scheme has also exemplified superior performance compared to existing protocols in terms of both security and efficiency.**

***Index Terms*—Internet of Medical Things, healthcare, sensors, vital signs, security, authentication, attack techniques, user authentication, vulnerabilities**

I. Introduction

The Internet of Medical Things (IoMT) has revolutionised healthcare by integrating smart devices and sensors, making it easier to access patients' physiological information but raising concerns about security and privacy. Specialised security protocols, such as lightweight key agreement protocols, are needed to protect sensitive data. This paper explores design considerations for such protocols, focusing on security requirements, resource constraints, and critical factors for secure and efficient communication in an IoMT Setup. The Internet of Medical Things (IoMT) environment demands specialised methods to protect privacy and mitigate security threats [1]. Lightweight security protocols, such as authentication and key agreement (AKA) protocols, are necessary for secure data transmission. Several researchers have proposed enhanced AKA protocols that outperform existing protocols while maintaining performance. Several key security requirements must be met to ensure secure communication within an IoMT configuration, including session key agreement, user anonymity, and mutual authentication [2]. Defences should be implemented to protect against attacks such as masquerading, impersonation, replay, man-in-the-middle techniques and known session key attacks [3]. Various risks and challenges have been identified in the security of the IoMT environment, such as the manipulation of healthcare sensors by an unknown adversary, potential exposure of personal patient information, and the impact of protocols that require high computational power and communication. A suggested lightweight key agreement mechanism addresses resource limits in IoMT devices while balancing security needs and risks. The protocol uses lightweight primitives to generate session keys between users and sensor nodes/IoMT Devices. This reduces the computational and communication strain of IoMT devices [4] [5]. Compared to similar solutions, the protocol is designed to be efficient regarding communication, storage, and computing costs. It resists common attacks in IoT environments, such as replay attacks and MITM attacks [5]. To solve the resource limits, the protocol produces a shared symmetric key after two communication rounds without human interaction [5]. ProVerif examined the proposed security protocol and demonstrated its ability to withstand several attacks in an IoT setup. The protocol has minimal communication costs and is more computationally efficient than comparable solutions. The suggested authentication methodology for medical IoT applications addresses resource restrictions using lightweight operations such as XOR and hash algorithms. [5]. A lightweight key agreement protocol can increase security in IoMT devices, and the protocol is designed for health-related IoT solutions with resource constraints [4] [5]. Therefore, the protocol can address all the concerns for the IoMT environment, such as security, privacy and resource constraints.

This study seeks to conduct a security review of the proposed authentication mechanism. We will propose, implement and test the protocol in a real-world environment to determine its usability and functionality. Second, we will conduct a formal security study with ProVerif to demonstrate the protocol's resilience to known threats. Finally, an informal security study will be undertaken to determine the mechanism's resilience to

979-8-3503-7700-2/24/$31.00 © 2024 IEEE

various known attacks. By combining these techniques, we want to give a thorough knowledge of protocols security and usability in real-world circumstances.

The paper is divided into numerous sections; in section II, all the previous attempts by other researchers have been discussed thoroughly. Section III discusses the preliminaries required to understand the scheme, such as the System and Threat Model. Similarly, Sections IV and V include thorough explanations of the suggested scheme and security analysis(formal and informal). Finally, section VI evaluates the performance of the proposed protocol in terms of computation and communication cost.

II. Related Work

Several academics have developed a variety of authentication systems to safeguard the privacy and security of user data. Wu et al. [6] presented a strategy using pre-computing in the communication process to reduce the time-consuming exponential computations, enhancing efficiency and security. However, Debiao et al. [7] identified Wu et al.'s approach is particularly vulnerable to impersonation and insider attacks. Debiao et al. proposed an improved scheme with enhanced security and performance to address these weaknesses, making it suitable for integrating low-power mobile devices in IoMT environments. Similarly, Masud et al. [8] focused on security in wireless sensor networks (WSNs), highlighting weaknesses in existing authentication schemes such as susceptibility to offline guessing attacks and lack of strong forward security. They implemented an enhanced three-factor authentication system for WSNs, backed by formal proofs and analyses, demonstrating robustness against various security vulnerabilities.

Recent works of Panchami et al. [9] also proposed a secure and lightweight mechanism optimised for the IoMT applications. Their scheme emphasises data integrity, confidentiality, and availability while also considering the resource constraints of IoMT devices. Fotouhi et al. [10] developed a hash-chain-based authentication technique for wireless body area networks (WBANs) in IoT. Their approach intends to enable safe access to patient data, addressing concerns over data privacy and security in WBANs. Xu et. al [11] identified vulnerabilities in existing cloud-centric IoMT systems and proposed a new certificateless signature (CLS) scheme to enhance security. Their scheme underwent formal security analysis and demonstrated practicality for real-world deployment. Ming et. al [12] suggested a three-factor authentication mechanism to protect patient data in IoMT systems. Challa et.al [13] addressed security flaws in a recent user authentication approach for healthcare sensor networks and provided a proven three-factor authentication and key agreement mechanism. Their protocol allows for dynamic node addition and updates while maintaining high security and low communication costs. Together, these studies advance the security and privacy of healthcare IoT systems, enabling safer and more efficient healthcare data management.

TABLE I
Notations

Symbol	Description
ID_i	Unique Identifier
PW_i	Password
$h(.)$	One-Way Hash Function
PID_i	Psuedo Identity
r_1	Random Number
MSK	Master Secret Key of Gateway Server
Δt	Maximum Time Delay
$T_u, T_s, T_d,$	Timestamps by the User, Server and Device respectively
$\oplus$	Exclusive OR(XOR) operation
$\|\|$	Concatenation
SK_{ij}	Session Key

III. Preliminaries

This section covers the protocol's preliminaries, including the protocol notations, system model, and threat model.

A. System Model

The Gateway Server (GS), a trusted registration authority, users who will access the data, and IoMT Devices placed in hospitals for remote sensing of patient data are the primary participants. The gateway server is responsible for registering and issuing unique secret parameters and IDs for users and IoMT devices. Fig 1 depicts the system model of the IoMT Setup.

1) **Gateway Server**: The gateway server handles registration, authentication, and communication between the user and the IoMT device.
2) **User**: The doctor or operator who wants to view the patient's physiological data or prior records.
3) **IoMT Device**: A device equipped with sensors that captures the patient's important physiological information. The data is sent over a Gateway Server.

B. Threat Model

The Threat Model was based on the extensively adopted Dolev-Yao Model (DY) [14]. According to its definition, the communication link between two entities is open and

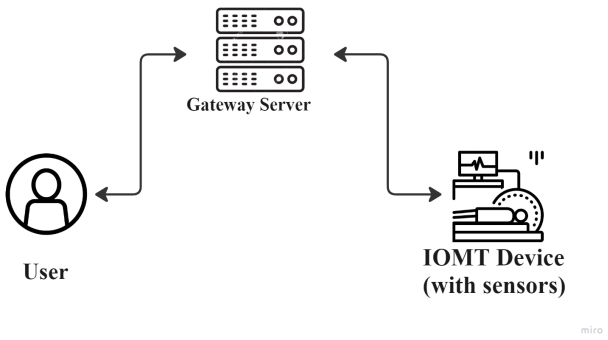

Fig. 1. System Model

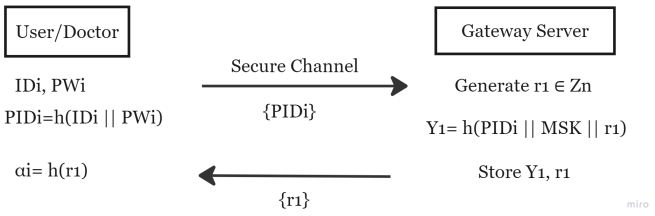

Fig. 2. User Registration Phase

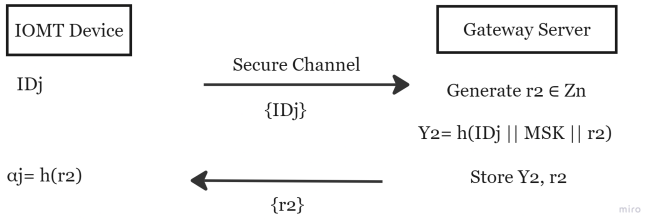

Fig. 3. IoMT Device Registration Phase

unsecured, with endpoints that are not trusted. An attacker can capture all network communications and delete or alter those broadcast over the public channel. We regard the gateway server as trustworthy, and the attacker will not compromise it. We further assume that the IoMT Device employed is not vulnerable to capture by an unknown attacker.

IV. Proposed Scheme

We proposed a lightweight mutual authentication mechanism for the IoMT divided into four major phases: *i. System Setup Phase*, *ii. User Registration Phase*, *iii.IoMT Device Registration Phase*, and *iv. Authentication and Key Agreement Phase*. Each of them has been described below:

1) **System Setup Phase**: The gateway server generates its Master Secret Key(MSK) and saves it secretly in this phase. It selects a one-way collision-free hash function $h(.)$ and made available to other devices and users.
2) **User Registration Phase**: In this step, each User (U_i) must register via a secure connection to the Gateway Server. A User registers to the Gateway Server in the following steps and shown in Fig 2:
   - The user inputs their (ID_i) and their Password (PW_i). It calculates the PID_i as h($ID_i \ || \ PW_i$) and sends the PID_i to the Gateway Server via a secure communication channel
   - The Gateway Server computes Y_i as h($PID_i \ || \ MSK \ || \ r1$) and stores Y_i, r_1 to the database. It sends out r_1 to the User.
   - The user finally, stores α_i securely as h(r_1).
3) **IoMT Device Registration Phase**: During this step, an IoMT Device uses a secure channel to register with the Gateway server. It follows the stages below, and the graphical depiction is shown in Figure 3:
   - The IoMT Device selects any ID as ID_j and sends it to the Gateway Server over a secure channel.
   - The Gateway Server generates $r_2 \in \mathbb{Z}^*$ and calculates Y_2 as $h(ID_j||MSK||r_2)$. It stores the values Y_2 and r_2 securely and sends out r_2 to the IoMT Device.
   - The IoMT Device stores the $h(r_2)$ as α_j securely.
4) **Authentication and Key Agreement Phase**: After a user (U_i) and the IoMT Device (V_j) become a registered user, they undergo a series of authentication exchanges. Once the authentication has been completed, they can communicate securely. The authentication and key agreement phases follow the indicated stages, and a thorough description is provided in Figure 4:
   - The user (U_i) enters their ID_i and their PW_i, computes their pseudo-identity as $PID_i = h(ID_i||PW_i)$ and generates a timestamp as T_u. The user sends a request to the Gateway Server using the PID_i and the T_u.
   - The Gateway Server, on receiving an authentication request from a user, checks whether $T_u \leq \Delta t$, if it doesn't satisfy, it rejects the authentication request. It fetches MSK, r_1 and computes Y_1^{new} as h($PID_i^* \ || \ MSK \ || \ r1$) and checks whether, $Y_1^{new} \stackrel{?}{=} Y_1$, if they're equal, it proceeds further with the request; otherwise, the request is immediately terminated.
   - The IoMT Device sends an authentication request to the Gateway Server by sending its ID_j with a timestamp T_d.
   - The Gateway Server, on receiving the authentication request from the IoMT Device, it checks whether $T_d \leq \Delta t$, if it doesn't satisfy, it immediately rejects the authentication request. It fetches MSK, r_2 and computes Y_2^{new} as h($ID_j^* \ || \ MSK \ || \ r2$) and checks whether, $Y_2^{new} \stackrel{?}{=} Y_2$, if they're equal, it proceeds further with the request; otherwise, the request is immediately terminated.
   - Once the User and the IoMT device requests have been verified, we generate $Y_3 = h(r_1 \oplus r_2)$. It generates a timestamp, t_s and sends it out to the User and the IoMT Device.
   - The User on receiving Y_3 and t_s calculates $\alpha_j = Y_3^* \oplus \alpha_i$ and finally computes the session keys as $SK_{ij} = h(\alpha_i||\alpha_j||t_s)$.
   - The IoMT Device on receiving Y_3 and t_s calculates $\alpha_i = Y_3^* \oplus \alpha_j$ and finally computes the session keys as $SK_{ji} = h(\alpha_i||\alpha_j||t_s)$.

V. Security Analysis

The formal and informal security assessments for our authentication scheme have been described in this section. We utilised the ProVerif tool for formal analysis in order to demonstrate the security and robustness of the protocol.

A. Formal Security Analysis

Using the ProVerif tool, we offer the formal security analysis of the suggested scheme in this section. For the

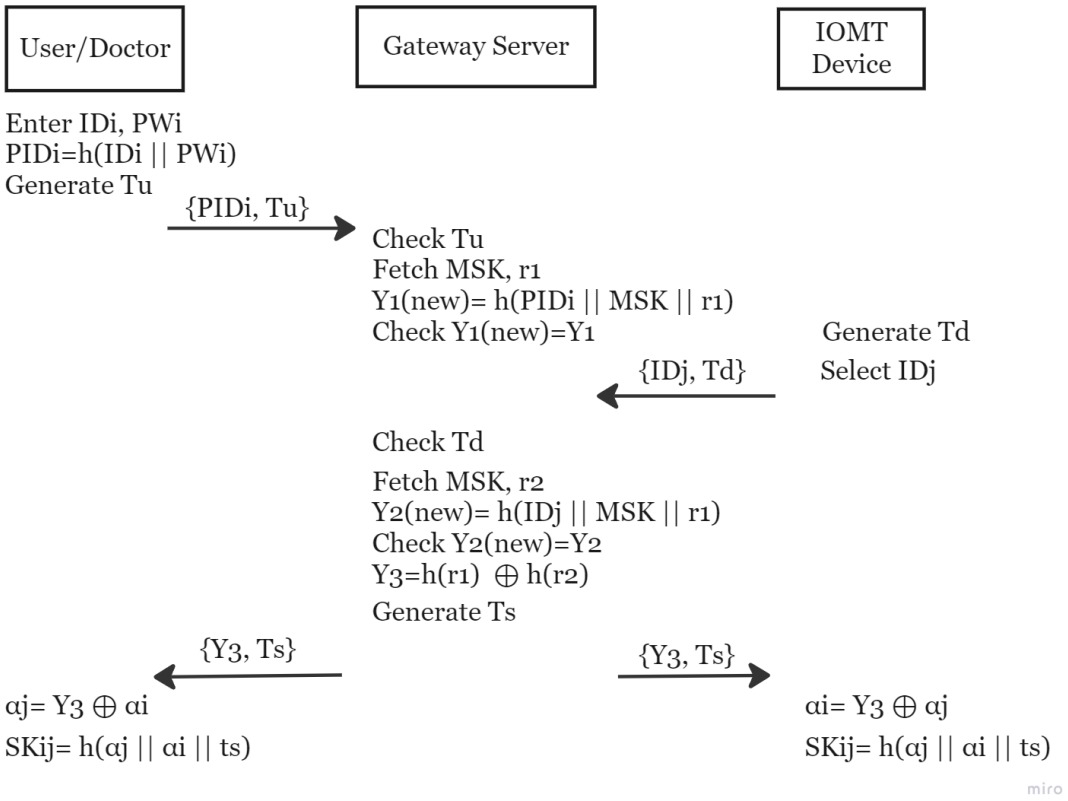

Fig. 4. Authentication and Key Agreement Phase

```
--------------------------------------------------------------
Verification summary:

Query inj-event(UserAuthed) ==> inj-event(UserStarted) is true.

Query inj-event(IOMTAuthed) ==> inj-event(IOMTStarted) is true.

Query not attacker(Skij[]) is true.

Query not attacker(PWi[]) is true.

--------------------------------------------------------------
```

Fig. 5. Result of Formal Security Analysis on ProVerif

verification purposes, we have used the following types of channels: *i. User-Gateway Server Private Channel* for Registration purposes *ii. User-Gateway Server Public Channel* for Authentication and further communication. *iii. IoMT-Gateway Server Private Channel* for Registration purposes *iv. IoMT-Gateway Server Public Channel* for Authentication and further communication. The hash, XOR and the concatenation operation are represented by the methods $h(), xor()$, and $con()$, respectively. The Session Key is represented as $SKij$ between the User and the IoMT Device. The event $UserStarted()$ represents the authentication process for the user has started, and the $UserAuthed()$ event represents the User has been authenticated successfully. Similarly, the event $IoMTStarted()$ represents the authentication process for the IoMT Device has started, and the $IoMTAuthed()$ event represents the IoMT Device has been authenticated successfully. We ran $queryinj - event(UserAuthed()) ==> inj - event(UserStarted())$. and $queryinj - event(IoMTAuthed()) ==> inj - event(IoMTStarted())$ and found both of the events. The results obtained from the formal security analysis has been shown in Figure 5

B. Informal Security Analysis

This section presents the informal security analysis of the suggested authentication mechanism and demonstrates its resilience to different types of attacks:

1) **Password Guessing:** First a User (U_i) enters their identity (ID_i) and Password(PW_i) the user computes the PID_i which is h($ID_i||PW_i$) and sends it. Since we are using a one-way collision-resistant hash function $h(.)$ it would be impossible to guess the password and gain access from an attacker's perspective because an attacker would require both their identity (ID_i) and Password(PW_i) for the process.
2) **Man-In-The-Middle Attack(MITM):** An attacker positions themself between the sender and the recipient in a man-in-the-middle attack in order to listen in on the other side. In our scheme, even if the adversary is able to intercept the communication, they still need the MSK

and the nonce r_i generated by the server to compute the messages further required for authentication.

3) **Replay Attack:** Even if the attacker gets access to parameters such as PID_i, Y_3, which are essential for the authentication, the server and every other associated entity check for the timestamp every time a new message has been sent and verify the timestamp. If the timestamp T_u is not verified, then the session is rejected making it difficult for the attacker to gain further access.
4) **Masquerading Attack:** In this type of attack, an attacker may attempt to pretend to be a user, the gateway server or an IoMT Device; however, since we have registered each entity with their identities like PID_i and the attacker finds it challenging to deduce the registered identification of the User or the IoMT device because their identities are confirmed once again throughout the authentication process. Hence, an impersonation attack is not possible.
5) **Modification Attack:** A modification attack is an attack where an attacker modifies, deletes or inserts new messages in the existing message being transmitted. Even if the attacker tries to modify, insert or delete parameters, the server will immediately detect and not proceed further with the authentication.
6) **Sybil Attack:** In a Sybil attack, an unknown adversary can generate numerous fictitious identities and submit requests to the server. The server keeps a database of all the registered users and the IoMT devices using their unique identities such as PID_i and ID_j. The server simply rejects any identity not present in the database at the time of authentication.

VI. Performance Analysis

The performance of our mechanism has been assessed in this part of the paper using two standard parameters: computation cost and communication cost. Our scheme outperformed the prior ones by a large margin when we compared the calculation and communication expenses of other pre-existing systems with their execution times. The proposed model is implemented on MacOS, having an Apple M1 CPU with 3.2 GHz and 8GB Memory. To simulate an IoMT device/Sensor Node, we used a Raspberry Pie 400 Desktop with ARM Cortex A72 on a 64-bit Raspian OS having a 1.8GHz CPU. All the sensor nodes, gateway servers and the user used Python version 3.9.19.

A. Computational Cost

The scheme comprises hashing operations at the user, gateway server and the IoMT Device. Various schemes by Chouhan et al. [15], Challa et.al [13], Chien et.al [12], and Foutouhi et.al [10] and it was found that the proposed scheme was comparatively better than all the previous schemes in terms of computation cost. On implementing various schemes, we found T_h to be 0.0009 ms for a single hash operation, T_{enc} to be 0.216 ms for symmetric encryption, T_{dec} to be 0.222 ms for symmetric decryption, T_{fe} to be 0.0218 ms for the fuzzy extraction and T_{hs} to be 0.0042 for single hash operation at the sensor node, T_{ecm} to be 0.02186 ms for the ECC multiplication. A comparison between various schemes is shown in Table III and Figure 6.

TABLE II
Computation Cost

Column 1	Computation Cost	Exeuction Time(ms)
User	$3*T_h$	0.0027
Gateway Server	$6*T_h$	0.0054
IoMT Device	$2*T_{hs}$	0.0085
	Total	0.0166

TABLE III
Comparison of Schemes

Scheme	Computation Cost	Execution Time(ms)
[15]	14 T_h + 7 T_{enc} + 7T_{dec}	3.0786
[13]	19 T_h + 3 T_{ecm} + T_{fe}	0.1045
[12]	25 T_h + 6 T_{hs} + T_{fe}	0.0699
[10]	27 T_h + 7 T_{hs}	0.0541
Proposed	9 T_h +2T_{hs}	0.0166

B. Communication Cost

For the communication cost analysis, the messages transferred between the involved entities, such as the user, the Gateway Server and the IoMT Device/ Sensor Node, were considered. For the sake of simplicity, we have taken the ID, Random Number or Nonce to be 128 bits long, the timestamp to be 64-bit long, and have used SHA-2 hash, giving out 256 bits. The user sends out PID, T_u, which is 256+64= 320 bits. Similarly, the IoMT server sends out 128+64=192 bits, and finally, the Gateway Server sends out Y_3 and T_u, which is 256+64+256+64= 640 bits. The total communication cost is 1792 bits, including the registration phase. A comparison between the previous all the previous schemes is shown in the Table IV and the Figure 7.

VII. Conclusion

Finally, the comprehensive analysis conducted in this study supports the notion that the suggested cryptographic method for the authentication of low-power IoMT devices stands out among existing options. Notably, it accomplishes this distinction by clearly reducing computation and communication overhead. Furthermore, the suggested approach's adaptability broadens its usage outside the context of IoMT only. The significantly low resource consumption implies its possible application in a larger range of scenarios involving geographically distant sensor networks or battery-powered devices. By

TABLE IV
Communication Bits for Different Schemes

Scheme	Communication Bits
[15]	2176
[13]	2305
[12]	5376
[10]	5504
Proposed	1792

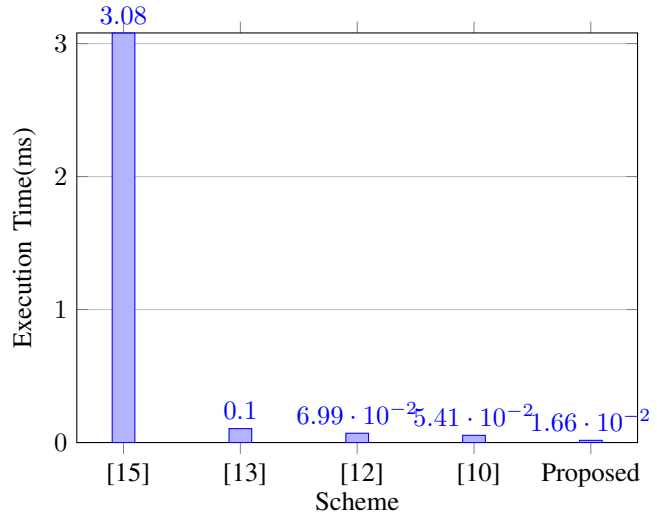

Fig. 6. Comparison of Execution Time

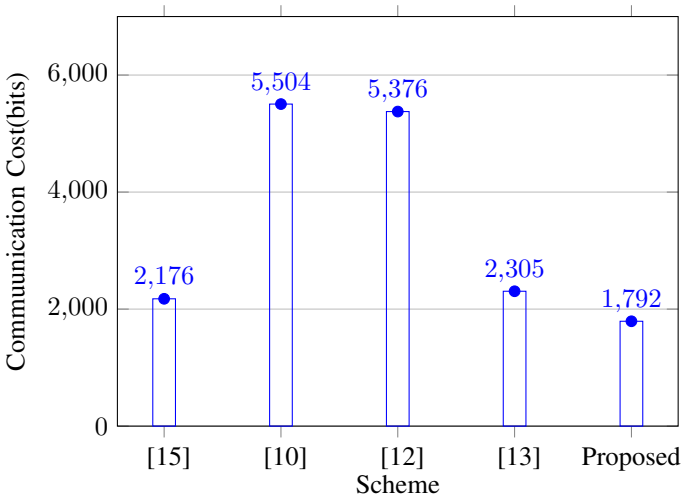

Fig. 7. Communication Cost for Different Schemes

providing a basis for the creation of ever more efficient and secure solutions, our study lays the path for future characterised by strong and long-term information security.

References

[1] M. Osama, A. A. Ateya, M. S. Sayed, M. Hammad, P. Pławiak, A. A. Abd El-Latif, and R. A. Elsayed, "Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions," *Sensors*, vol. 23, no. 17, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/17/7435

[2] D. Singh, B. Kumar, S. Singh, and S. Chand, "A secure iot-based mutual authentication for healthcare applications in wireless sensor networks using ecc," *International Journal of Healthcare Information Systems and Informatics*, vol. 16, pp. 21–48, APR 2021. [Online]. Available: https://dx.doi.org/10.4018/ijhisi.20210401.oa2

[3] K. Kim, J. Ryu, Y. Lee, and D. Won, "An improved lightweight user authentication scheme for the internet of medical things," *Sensors*, vol. 23, no. 3, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/3/1122

[4] T.-Y. Wu, L. Wang, and C.-M. Chen, "Enhancing the security: A lightweight authentication and key agreement protocol for smart medical services in the ioht," *Mathematics*, vol. 11, no. 17, 2023. [Online]. Available: https://www.mdpi.com/2227-7390/11/17/3701

[5] S. Szymoniak and S. Kesar, "Key agreement and authentication protocols in the internet of things: A survey," *Applied Sciences*, vol. 13, no. 1, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/1/404

[6] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, Jun 2012. [Online]. Available: https://doi.org/10.1007/s10916-010-9614-9

[7] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, Jun 2012. [Online]. Available: https://doi.org/10.1007/s10916-011-9658-5

[8] 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 of Things Journal*, vol. 9, no. 4, pp. 2649–2656, 2022.

[9] P. V., R. Marion Lincy G., M. Mary Mathews, and S. Justine, "A provably secure,privacy-preserving lightweight authentication scheme for peer-to-peer communication in healthcare systems based on internet of medical things," *Computer Communications*, vol. 212, p. 284–297, Dec 2023.

[10] M. Fotouhi, M. Bayat, A. K. Das, H. A. Far, S. M. Pournaghi, and M. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot," *Computer Networks*, vol. 177, p. 107333, Aug 2020.

[11] F. Xu, S. Liu, and X. Yang, "An efficient privacy-preserving authentication scheme with enhanced security for iomt applications," *Computer Communications*, vol. 208, p. 171–178, Aug 2023.

[12] C.-M. Chen, S. Liu, X. Li, S. H. Islam, and A. K. Das, "A provably-secure authenticated key agreement protocol for remote patient monitoring iomt," *Journal of Systems Architecture*, vol. 136, p. 102831, Mar 2023.

[13] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers amp; Electrical Engineering*, vol. 69, p. 534–554, Jul 2018.

[14] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[15] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical iot networks," *Computer Communications*, vol. 166, p. 154–164, Jan 2021.