A Comprehensive Authentication Taxonomy and Lightweight Considerations in the Internet-of-Medical-Things (IoMT)

Azlina binti Ahmadi Julaihi[1], Md Asri Ngadi[2], Raja Zahilah binti Raja Mohd Radzi[3]
Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia[1, 2]
Faculty of Engineering, Universiti Teknologi Malaysia, Johor, Malaysia[3]
Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Sarawak, Malaysia[1]

***Abstract*—The potential of Internet-of-Things (IoT) in healthcare is evident in its ability to connect medical equipment, sensors, and healthcare personnel to provide high-quality medical expertise in remote locations. The constraints faced by these devices such as limited storage, power, and energy resources necessitate the need for a lightweight authentication mechanism that is both efficient and secure. This study contributes by exploring challenges and lightweight authentication advancement, focusing on their efficiency on the Internet-of-Medical-Things (IoMT). A review of recent literature reveals ongoing issues such as the high complexity of cryptographic operations, scalability challenges, and security vulnerabilities in the proposed authentication systems. These findings lead to the need for multi-factor authentication with a simplified cryptographic process and more efficient aggregated management practices tailored to the constraints of IoMT environments. This study also introduces an extended taxonomy, namely, Lightweight Aggregated Authentication Solutions (LAAS), a lightweight efficiency approach that includes a streamlined authentication process and aggregated authentication, providing an understanding of lightweight authentication approaches. By identifying critical research gaps and future research directions, this study aims to provide a secure authentication protocol for IoMT and similar resource-constraint domains.**

Keywords*—*Lightweight authentication; Aggregated Authentication' Multi-Factor Authentication (MFA); Internet-of-Medical Things (IoMT)

I. Introduction

In the age of the Internet of Things (IoT), the integration of devices and networks has spread to the healthcare industry, resulting in the Internet of Medical Things (IoMT). These networks comprise interconnected medical equipment, sensors, and systems that allow for real-time observation, data collection, and analysis, improving patient care and healthcare delivery efficiency [1]. However, the use of IoT devices in medical settings raises concerns about security and privacy. Unauthorized access to these networks can result in data breaches, and exposing sensitive patient information necessitates robust security measures, particularly in the realm of authentication. It is critical to safeguard against unauthorized access and other cyber threats to ensure a secure and trustworthy authentication mechanism in IoMT environments.

Authentication as described by NIST, is the legitimacy of one's identity and an authenticator [2]. In general, authentication is the process of verifying the identity of a user, entity, or device attempting to access a network or system. Authentication is essential to all facets of private access, including access control to data and resources that are only available to specific entities. These processes include verifying credentials like passwords, digital certificates, or biometric information against a known set of registered identities in an authentication server or directory.

Authentication in IoMT is a multifaceted challenge due to the diverse range of devices, communication protocols, and the stringent requirements for data integrity and privacy. Traditional authentication methods, such as password-based schemes, are often inadequate in this context due to their susceptibility to various attacks, including replay attacks, man-in-the-middle (MITM) attacks, and impersonation attacks. Consequently, there has been a significant shift towards adopting more sophisticated authentication mechanisms, such as token-based, biometric, and multi-factor authentication (MFA) protocols. Despite these advancements, existing authentication protocols in IoMT still face several limitations. Many protocols are either too complex, resulting in increased computational overhead which is unfit for resource-constraint devices, or weak cryptographic techniques that are insufficiently secure against emerging threats. Thus, the development of lightweight authentication schemes, especially for IoMT, has been the subject of several studies to cater to resource limitations while providing secure communication and data exchange within the medical network.

This study aims to look further into lightweight approaches using various authentication credentials and their efficiency. Thus, this review attempts to evaluate the lightweightness approaches used and the limitation of existing authentication mechanisms in IoMT to give healthcare providers insight into best practices for securing these networks. This study also presents the background study of authentication solutions using a lightweight approach. Furthermore, current literature that employed a lightweight approach for IoMT is reviewed to obtain a better understanding of the requirements for healthcare settings. Thus, this study presented two contributions which are an extended authentication taxonomy, emphasizing lightweight approaches and multi-factor authentication solutions based on the existing work by Alsaeed and Nadeem [3], and a review of recent existing works on authentication mechanisms using a lightweight approach that is particularly suited for IoMT environments. By categorizing and analyzing these protocols, this study seeks to highlight existing gaps and suggest potential areas for further research and development.

The remainder of this study is organized as follows. Section II illustrates the background study of the multi-factor authentication mechanism focusing on lightweight approaches. The extended authentication taxonomy is introduced in Section III with two lightweight authentication efficiency approaches: streamlined authentication process and aggregated authentications. Section IV presents a review of recent (2020-2024) related works on existing authentication mechanisms in IoMT. A discussion of the review is presented in Section V with identified research gaps and future works. Finally, the conclusion is included in Section VI.

II. Background Study

The healthcare industry has undergone a significant transformation with the advent of the Internet of Medical Things (IoMT). IoMT refers to the interconnected system of medical devices and applications that communicate through networking technologies to collect, analyze, and transmit health data [4]. This interconnected network allows for continuous, real-time monitoring of patients, leading to improved healthcare delivery, personalized treatment plans, and enhanced patient outcomes [5]. The integration of IoMT in healthcare has revolutionized traditional practices, making remote monitoring, telemedicine, and mobile health (mHealth) increasingly viable and effective.

With the increasing deployment of IoMT devices, ensuring the security and privacy of sensitive medical data has become a paramount concern [6]. Authentication is the first security layer and a critical security mechanism that verifies the identity of users and devices, ensuring that only authorized entities can access the system to protect from malicious security threats and data breaches [7]. Given the sensitive nature of medical data, any compromise can have severe implications, including incorrect diagnosis, treatment errors, and potential harm to patients.

As depicted in Fig. 1, a typical access system within an IoMT environment to ensure secure and efficient access control and data integrity across interconnected medical devices adopted from Anca et al. [8]. Access control has two important counterparts: the authentication and authorization processes, to enforce permissions for legitimate users or devices. Various factors such as passwords, biometrics, tokens, and multi-factor authentication are used when a user or a device wishes to attempt the system and the authentication mechanism will verify these credentials against stored data or through real-time verification. The author incorporates a lightweight mechanism into the authentication process model to ensure that the authentication process is efficient and uses minimal computational resources. On the other hand, the authorization database plays an important role in storing relevant credentials and permissions, in which the system administrator manages to maintain system integrity. Putting all together, this highlights the importance of integrating lightweight solutions to handle the difficulties presented by the heterogeneous and resource-constraint in IoMT ecosystem without sacrificing scalability or performance.

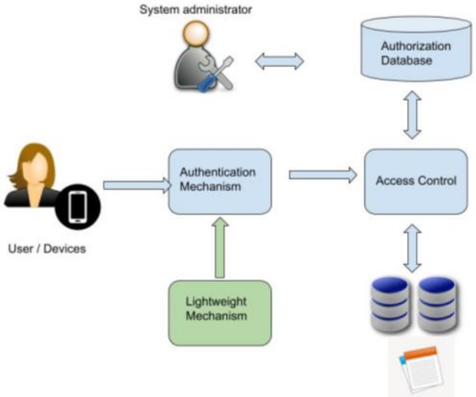

Fig. 1. Typical access system integrating lightweight mechanism in the authentication process (adopted from Anca et al. [8]).

Additionally, the diversity of devices and communication protocols used in IoMT environments necessitates adaptable and interoperable authentication solutions. As of March 2020, IEEE has published a new architectural standard for IoT, in response to the numerous unstandardized frameworks of IoT that have been proposed by researchers and industry. The goal of this standard is clear, to facilitate heterogeneous interaction, system interoperability, and the industry's continued development and scalability. According to one of the two standards, the P2413.1 RASC - Standard for a Reference Architecture for Smart City, defines a Reference Architecture with a four-layer architecture: device layer, communication network layer, IoT platform layer, and application layer [9]. Fig. 2 is the potential design used to develop IoMT authentication-role-specific architecture with reference to the P2413.1 RASC architecture.

In Fig. 2, the architecture of IoMT typically involves multiple layers: the device layer, communication layer, IoT platform layer, and application layer. Each layer faces unique security threats, and robust authentication mechanisms are essential to safeguard the entire IoMT ecosystem. The device layer comprises numerous wearable devices and medical sensors that collect medical information [10, 52]. This layer initiates the authentication process with basic verification of devices and initial user authentication, ensuring that data collected from legitimate sources is securely transmitted. Next is the network layer, which uses technologies such as Wi-Fi, Bluetooth, and cellular networks for secure data transmission and network authentication to healthcare providers and cloud services to prevent unauthorized access [11]. Moving up, at the IoT platform layer, intermediate authentication mechanisms are implemented to verify the integrity of data and devices before further processing or transmission to the cloud. Finally, the application layer encompasses comprehensive authentication and authorization processes, ensuring that only verified users and devices can access sensitive medical data and analytics services.

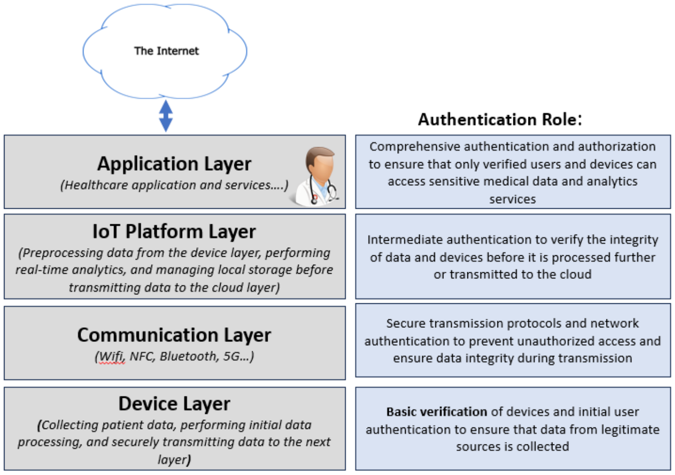
The Internet
Authentication Role:
Application Layer
(Healthcare application and services....)
Comprehensive authentication and authorization to ensure that only verified users and devices can access sensitive medical data and analytics services
IoT Platform Layer
(Preprocessing data from the device layer, performing real-time analytics, and managing local storage before transmitting data to the cloud layer)
Intermediate authentication to verify the integrity of data and devices before it is processed further or transmitted to the cloud
Communication Layer
(Wifi, NFC, Bluetooth, 5G...)
Secure transmission protocols and network authentication to prevent unauthorized access and ensure data integrity during transmission
Device Layer
(Collecting patient data, performing initial data processing, and securely transmitting data to the next layer)
Basic verification of devices and initial user authentication to ensure that data from legitimate sources is collected

Fig. 2. IoMT authentication-role-specific architecture.

Further discussion on authentication is not complete without a reference to the four levels of security assurance. According to NIST, there are four levels of security assurance for authentication processes [12]. This structured framework provides specific requirements for identity proofing, authentication methods, and threat resistance vary depending on the level as depicted in Fig. 3.

There are several authentication levels and processes involved in authentication for IoMT. A typical usually involves 1) device registration, 2) user registration-this process verifies the identity of the users accessing the IoMT system, and 3) data access control, which ensures that only authorized users can access sensitive medical data. Each stage requires a robust authentication mechanism (in Fig. 2) to ensure the integrity and confidentiality of the transmitted health information At Level 1, device registration. In this stage, medical devices are registered with the healthcare network, often involving the generation and exchange of cryptographic keys. Basic verification using a simple authentication mechanism might be used at the device layer, suitable for initial health data collection. Moving up to Level 2, a more robust identity verification and single-factor authentication would be applied at the communication layer, to resist security attacks such as replay and eavesdropping for secure data preprocessing and transmission. Level 3 and Level 4 are essential in the cloud layer, where multi-factor authentication and strong encryption methods are used to safeguard information during data analysis and long-term storage. This setup offers protection against cyber-attacks like MITM attacks ensuring that only authorized users and devices can access important medical data. This hierarchical application of assurance levels provides as a basis across the IoMT architecture to ensure a thorough security approach is established, tailored to the needs and capabilities of each layer.

However, the unique characteristics and distributed nature of IoMT devices present several challenges for a robust authentication mechanism making it challenging to implement complex and computationally intensive authentication protocols. Moreover, limited processing power and memory in many resource constraints IoMT devices pose challenges for deploying strong authentication mechanisms like multi-factor authentication (MFA) or cryptographic techniques. These constraints necessitate the development of lightweight, yet secure authentication solutions tailored to the capabilities of IoMT devices. Thus, it is imperative to have an authentication mechanism that can minimize computational and communication overhead as well as energy consumption while maintaining robust security measures. There are a few possible existing authentication approaches in the IoMT system which include approaches like lightweight cryptography, lightweight multi-factor authentication, and lightweight hybrid anomaly detection [5]. For instance, lightweight cryptographic algorithms such as elliptic curve cryptography (ECC) and physically unclonable functions (PUFs), offer strong security with reduced resource requirements [13], [14], [15], [16]. In general, the characteristics of any lightweight algorithms can be defined as follows:

1) Low computational complexity: Algorithms that require fewer computational cycles to execute [17].

2) Minimal memory usage: Less memory is used for both code and authentication data [18].

3) Energy efficiency: Optimized for low power consumption, crucial for battery-operated devices [19].

4) Small key sizes: Use of smaller cryptographic keys to reduce processing overhead while maintaining security [20].

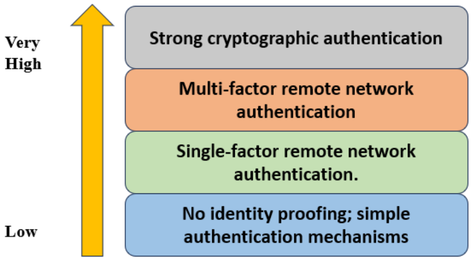
Very High
Low
Strong cryptographic authentication
Multi-factor remote network authentication
Single-factor remote network authentication.
No identity proofing; simple authentication mechanisms

Fig. 3. Four security assurance levels by NIST.

Researchers focusing on developing authentication solutions strive to find a balance between security and resource efficiency to address security risks in IoMT environments. Efforts in lightweight authentication research often concentrate on creating solutions to meet this need. Many studies have investigated aspects of lightweight cryptography and authentication schemes in the wider IoT context, but a focused look within the specific IoMT realm is lacking. Research efforts have mostly focused on cryptographic techniques, with varying attention to the details of data transmission and authentication within IoMT. The works of Sallam and Beheshti [21] have added a lot to understanding the applicability of lightweight cryptography and studies ongoing developments in the realm of IoT, but there's a gap in having a thorough streamlined authentication approach specific to IoMT is still lacking. As the number of connected medical devices and the complexity of IoMT environments grow, ensuring efficient authentication at scale becomes increasingly crucial to meet the healthcare industry's demands. Moreover, while some studies have talked about potential attacks on lightweight cryptography, there's not much literature systematically analyzing the aggregated authentication mechanism necessary in IoMT. The authors aim to fill these gaps by putting together and critically looking at the existing knowledge, and finding areas where more investigation is needed. Through this, the authors hope to offer an updated and consolidated understanding of lightweight cryptography and authentication in IoMT, pushing forward improvements in the security of healthcare IoT systems. Nonetheless, despite these limitations and challenges, continued research and development in lightweight authentication mechanisms are necessary to enhance security efficiency, particularly in healthcare settings.

III. Extended Authentication Taxonomy

A well-defined taxonomy for authentication on the Internet of Medical Things (IoMT) is essential to enhance the understanding of this complex topic and address the interrelationships among various elements within IoMT systems. In recent years, numerous security solutions have been created and put forth. However, it remains considerably challenging to produce a competent solution for authentication in a resource-constrained network. One of the main challenges is to provide a lightweight authentication solution, tamper-proof to security threats for IoT applications specifically in the field of medical IoT. The extended taxonomy is built upon an existing authentication taxonomy by Alsaeed and Nadeem [3]. There are seven main perspectives in Alsaeed and Nadeem's taxonomy. The taxonomy is further categorized by the authors according to the following axes:

- Authentication Factors comprised of Type of Credentials, Authentication Levels, and Authentication Procedure. This study will focus on the type of credentials used in the authentication processes in recent literature as different types of credentials have varied impacts on the lightweightness of an authentication process. Authentication Procedures consist of One-way authentication verifies one entity to another, two-way (mutual) authentication verifies both entities to each other, and three-way authentication involves a third trusted entity in the process. The selection of credentials should align with the specific limitations and needs of the IoMT environment, ensuring a balance between lightweightness and security.

- Authentication Schemes which refer to authentication architectures and authentication categories. Authentication architectures include both centralized and decentralized architectures, which are further divided into flat and multi-level approaches. Authentication categories differentiate between static and continuous authentication.

- Authentication attacks, address various authentication attacks and the measures taken to prevent them, such as resistance to guessing, impersonation, man-in-the-middle attacks, etc.

- The fourth axe is on the authentication solutions which include basic authentication methods, key-agreement used in authentication, cryptography-based and certificate-based schemes. And finally, the extended taxonomy on lightweight authentication mechanisms. The lightweight mechanism includes streamlined authentication processes and aggregated authentication which include approaches designed to optimize performance by reducing computational and communication overhead, resource usage, and response time, which are key attributes of efficiency in authentication protocols.

Furthermore, several key aspects must also be considered when designing a lightweight authentication mechanism for IoMT to ensure that the system is secure, efficient, and compatible with resource-constrained devices such as medical devices. These aspects can be categorized into four aspects: Security robustness, Lightweight Efficiency approach, Compatibility approach, and Usability approach. This study explores two areas in terms of multi-criteria authentication taxonomy based on the work of Alsaeed and Nadeem [3] and Agrawal and Ahlawat [22].

1) Security robustness: Firstly, the security mechanism must be robust. The security approach primarily focuses on the authentication strength such as using strong cryptographic methods and multi-factor authentication[23], [24], [25], [26]. One of the challenges is that implementing robust encryption without significantly impacting device performance can be difficult.

2) Lightweight efficiency approach: The efficiency for authentication should cover the key design considerations such as the low computational overhead that can adapt to IoMT devices with limited processing power by employing lightweight cryptographic algorithms [27], [28]. Recent advancements in lightweight cryptographic algorithms have shown significant potential in improving the efficiency of IoMT authentication processes. Using lightweight cryptographic primitives such as Elliptic Curve Cryptography (ECC) and hash functions provides strong security with minimal computational resources [15], [29]. Thus, selecting the right cryptographic primitives in the authentication process is crucial. For instance, the work of Chatterjee et al. [29] demonstrated the effectiveness of ECC and hash-based schemes in IoT security, highlighting their suitability for resource-constrained devices. Furthermore, the integration of aggregated authentication techniques such as batch processing and shared key generation, streamlines the authentication process, reduces communication overhead, and improves scalability, making them suitable for dynamic IoMT environments where devices frequently join and leave the network.

3) Compatibility approach: Some of the well-known standard protocols such as OAuth 2.0 or FIDO are required to ensure the authentication mechanism is interoperable with a wide range of IoMT devices and platforms. Scalability remains the biggest hurdle within the IoMT ecosystem due to the growing number of devices and diverse platforms.

4) Usability approach: The usability approach centers around the authentication process that should never be overlooked. The authentication factors should be user-friendly employing methods such as biometric authentication for ease of use [30]. Challenges include designing authentication mechanisms that are both user-friendly and secure can be conflicting goals.

This study will further investigate lightweight efficiency approaches to fulfill the study goal. To identify the best authentication efficiency approaches for lightweight mechanisms were studied through existing recent literature. In a survey by El-hajj et al. [31], the author provides a comprehensive review of lightweight authenticated encryption for IoT devices, using a multi-criteria classification approach. The authors evaluate various aspects of authentication methods to assess their strengths and weaknesses, including security robustness, computational efficiency, scalability, simplicity of implementation, resilience to attacks, compatibility with existing systems, and usability. By considering these evaluation parameters, the authors compare the efficiency of different authentication techniques in IoT applications. The assessment of lightweight design, multi-factor authentication, and encryption technique usage provides insights into the efficiency and effectiveness of authentication methods in securing IoT devices while optimizing resource utilization.

In another survey done by Agrawal and Ahlawat [22], they review the authentication schemes based on three different parameters which are lightweight, multi-factor authentication, efficient, and encryption technique usage. According to the authors, these three classifications based on their reviews are important considerations in determining authentication efficiency. They also compared the efficiency of different authentication techniques in IoT applications and assessed whether any of the criteria used are preferred to ensure efficient operation in resource-constraint IoMT environments. The authentication protocols can be designed according to various factors. Two-factor authentication consists of utilizing user identification and biometric data to grant access to the IoMT system [32]. On the other hand, multi-factor authentication is the combining different elements such as user possession, inheritance and knowledge credentials to increase security [33], [34]. Many authentication approaches rely on multi-factors to enhance security and provide more resilient authentication solutions to protect from any adversary breach [26]. Thus, the presence of multi-factor authentication needs to be considered in the comparison to determine the efficiency of the authentication method [19].

On the other hand, the authors Samal et al. [35], classified authentication protocols into five different domains which are mutual authentication, one-time password, public key cryptography, zero-knowledge proof, and digital signature. They further classified three different categories for cryptographic algorithms such as 1) Encryption algorithms, 2) Signature algorithms, and 3) Hashing algorithms. These cryptographic techniques should be implemented efficiently to avoid the excessive computational burden of IoMT devices [35].

Thus, taking into account the analysis from the previous section, this study provides the extended version (Lightweight Aggregated Authentication Solutions, LAAS) of the authentication solutions taxonomy by Alsaeed and Nadeem [3] by adding in another authentication solution, namely under the lightweight approach, with its two methods; streamlined authentication process and aggregated authentication, as shown in Fig. 4 (illustrated in dashed rectangle box) to be well-suited for a resource-constraint environment such as IoMT. The details of these two methods are discussed in the next subsections.

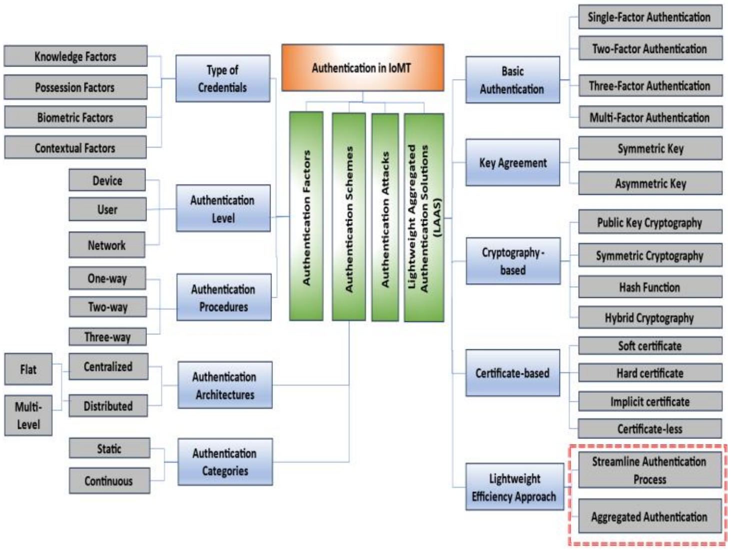

Fig. 4. Extended taxonomy for authentication in IoMT.

B. Lightweight Efficiency Approaches

1) Streamlined authentication process: It has been observed in recent years that lightweight authentication schemes were being proposed by numerous researchers at different times to increase system efficiency. According to Alsaeed and Nadeem [3], the number of exchanged messages during authentication processes will immediately affect the authentication scheme performance. Reducing the number of messages in an authentication protocol can be a strategy to make the algorithm lightweight, but it is not the sole criterion. As depicted in Fig. 4, the authors used an extended term to refer to this lightweight approach in authentication which is a streamlined authentication process that refers to the reduction in the complexity and number of steps involved in the authentication process. These lightweight authentication algorithms typically involve based on the usage of multiple factors such as 1) Symmetric key lightweight protocols, a lightweight algorithm that is being used during the pre-shared key exchanges, secure and shorter key sizes for encryption and decryption operations. 2) Hardware-assisted lightweight solutions such as PUF-based authentication 3) Biometric-based authentication like fingerprint recognition or 4) Simplified cryptography primitives, such as XOR, concatenation, and hash operations to support processing capabilities of IoT devices. Current literature agrees that streamlined authentication processes in authentication are the key essential in any lightweight solutions to enhance security while minimizing resource scarcity and computational complexity [3], [13], [36], [37]. Often, simpler cryptographic operations are used such as using only hashing and XOR to minimize the overhead complexity so that it is lightweight enough for a resource-constraint environment [38], [39], [40], [41]. Therefore, all the above factors are vital aspects of streamlined authentication, enhancing the practicality and performance of security mechanisms in real-time, high-frequency authentication scenarios in IoMT and similar applications. However, the challenge is to streamline the authentication process and keep a high level of security. In the context of the IoMT environment, this is crucial as we are dealing with time-sensitive healthcare applications, thus a high level of security is the utmost priority.

2) Aggregated authentication: Implementing a robust authentication mechanism in IoMT poses several challenges. As pointed out in the previous section, resource constraints in IoMT devices are the main challenge as these devices often have limited computational and energy resources, and the possible authentication solution is to make them lightweight. Apart from these main challenges, scalability issues are nothing new in IoMT environments. Handling the growing number of connected devices and users with one-to-one communication is inefficient for the massive communication required by today's IoMT-based applications.

Aggregated authentication in IoMT refers to combining authentication processes into a single operation, enhancing efficiency and reducing communication overhead [42]. Several techniques are involved such as aggregating multiple authentication requests into a single process (batch processing) [43] and hierarchical aggregation which typically involves multi-level aggregation where data is aggregated at local/edge nodes before being sent to central servers [44]. These approaches are tailored to address the unique constraints of IoMT environments, ensuring that authentication processes are both secure and efficient.

This approach is particularly beneficial in environments where numerous small transactions occur frequently, as it can significantly reduce overhead, improve processing efficiency, and enhance overall system performance. In the context of lightweight authentication, aggregated authentication can be leveraged to streamline authentication processes, especially in systems like the IoMT where multiple authentication requests might occur simultaneously from various medical devices and sensors. By bundling these requests, the system can handle them more efficiently, minimizing computational load and reducing latency. This method aligns well with the principles of lightweight authentication, which aim to provide secure, efficient, and low-overhead authentication mechanisms suitable for resource-constrained environments. Therefore, incorporating aggregated authentication into lightweight authentication schemes can further enhance their efficiency and effectiveness, making them an attractive solution for real-time, high-frequency authentication scenarios in IoMT and other similar applications.

IV. Related Works

To address the need for lightweight multifactor authentication schemes, several research works have been conducted in recent years. In [45], they proposed a lightweight multifactor authentication [51] scheme for cellular networks, exclusively 5G, and a trust-based blockchain architecture for VANET to mitigate major communication attacks using blockchain technology. In a subsequent paper, they extended this work to propose a lightweight multifactor authentication security scheme for a multi-hop scenario using timestamping, one-way hash function, Blind-Fold Challenge scheme with public key infrastructure with reduced authentication overhead, computation cost, and communication cost [23]. They also contributed to this area by proposing a lightweight multifactor authentication protocol for multi-gateway WSNs using hash functions and XOR operations. Additionally, Xue et al. [41] used lightweight cryptographic primitives to propose a lightweight three-factor anonymous authentication approach in multi-gateway WSNs using hash functions and XOR operations. These works collectively demonstrate the ongoing efforts to develop efficient and secure lightweight multifactor authentication schemes for various network scenarios, including cellular networks, WSNs, and healthcare applications.

In another research effort, Atiewi et al. [46] introduced a lightweight multifactor secured smart card-based user authentication for cloud-IoT applications, emphasizing the importance of scalability and security in big data IoT systems. To tackle the resource-constraint issues in the IoMT, it is significant to use lightweight multi-factor cryptographic algorithms, such as block ciphers and hash functions to enhance data confidentiality, integrity, and secure authentication [28]. Hash functions and block ciphers are a few examples of lightweight cryptographic algorithms that can be applied in IoT devices to achieve strong protection against unauthorized access and data breaches. These cryptographic primitives, which offer effective encryption, safe authentication methods, and data integrity verification are necessary to guarantee the security of the system.

On the other hand, Gumis et al. [24], proposed a biometric blockchain-based multifactor privacy-preserving authentication scheme for Vehicular Ad Hoc Networks (VANETs). The scheme employs Physical Unclonable Functions (PUF) and one-time dynamic pseudo-identities as authentication factors, providing lightweight and privacy-preserving authentication for VANETs. PUFs have gained widespread use in user authentication protocols, leveraging a device's distinct physical characteristics for authentication rather than easily replicable passwords and secret keys [47], [48].

In a related study, Malik et al. [49] proposed a lightweight certificate-based authentication scheme for IoT devices and networks, introducing L-ECQV, a lightweight certificate profile of ECQV implicit certificates, and suggesting the inclusion of PUFs for multi-factor authentication. The study provides insights into certificates and PUFs in lightweight authentication protocols, contributing to the development of an enhanced two-factor authentication protocol. Additionally, the work by Ebrahimabadi et al. [50] addressed the threat of PUF modeling by employing multifactor authentication, including a shared cryptographic key alongside the Challenge Response Pair (CRP), to enhance the resilience of authentication protocols for IoT devices. This illustrates ongoing efforts to counter specific security threats through multifactor authentication, contributing to the advancement of lightweight authentication mechanisms for IoT environments.

Other related work includes researchers working on the same authentication area using the blockchain model proposing various approaches and evaluating their work against various security threats using formal or informal security analysis on the Internet of Medical Things. The work of [39], [44], and [45] proposed that apart from using multifactor authentication and lightweight cryptography to enhance security and optimize efficiency, it is essential to integrate blockchain technology between IoT and cloud environments that could provide an additional layer of security and transparency, ensuring the integrity of data and transactions. Thus, it is crucial to have a balance of security and efficiency for resource-constrained WSN nodes, considering factors such as energy consumption and computational overhead.

Therefore, the comparison of several recent related works on authentication is selected and discussed in Table I. These fourteen related works (2020-2024) on multi-factor authentication are selected in the domain of Internet-of-Medical-Things (IoMT) and Blockchain. The reviews are done based on the authors' contributions and summarize the findings reflecting on the extended authentication taxonomy (as depicted in Fig. 4). The results are shown in Table I.

V. Discussion

As shown in Table I, there's a variety of authentication methods that have been employed in recent works, particularly within the context of IoMT. The first column insights are on the type of credentials. The most widely used model in the authentication process is often based on a combination of user identity, passwords, and biometric information. These multi-factor authentications are used in more recent studies to enhance security further. Using only single-factor authentication schemes, such as device information, pseudo-identities, and user tokens, is less prevalent compared to multi-factor authentication solutions. The reviewed articles show various lightweight authentication approaches suitable for resource-constrained environments such as in IoMT. Many of the proposed solutions emphasize a lightweight approach which is critical for resource-constraint IoMT devices. Common ones include the use of lightweight cryptographic algorithms (e.g., ECC), physically unclonable functions (PUFs), and lightweight cryptographic primitives such as XOR and hash functions are common. Most of the existing works implement a combination of asymmetric and symmetric cryptography, including Rivest–Shamir–Adleman (RSA) and secure hash algorithms. Some authentication solutions avoid the complexity of traditional certificate management by implementing implicit or soft certificates. Schemes like group authentication techniques based on Shamir's Secret Sharing (SSS) algorithm are employed to streamline the authentication process by reducing the number of blockchain transactions. Alsaeed et al. [53] proposed work, distribute authentication credentials among multiple entities (e.g., fog nodes), and combine only a sufficient number as part of streamlining the authentication process to help reduce computational and communication overhead. It can be seen that some of the recent works proposed lightweight authentication schemes, utilizing solutions such as PUFs or blockchain technology, but they often still encounter significant increases in their computational overhead and complexity. Apart from that, not every proposed work addressed scalability issues, particularly concerning the computational overhead, resource utilization, and the management of key and authentication data. This is highlighted in protocols that rely heavily on blockchain technology or those with complex key management schemes. The limitations of each reviewed work are also presented in Table I in the last column.

In addition to reviewing the recent related works on authentication (as shown in Table I), a conceptual validation of the established benchmarks in the field is conducted against the proposed lightweight authentication approach. This validation focuses on varying levels of computational efficiency, security robustness, and scalability comparing them against the proposed method to illustrate its advantages and identify potential areas for further improvement. The conceptual validation table is presented in Table II.

As depicted in Fig. 4, the Lightweight Efficiency approach is a crucial authentication solution in IoMT environments, where resource constraints such as limited processing power are common. The techniques reviewed in Table II demonstrate varying degrees of efficiency, from high efficiency to medium, and low efficiency. High efficiency depicts those methods that involve low computational overhead, fast processing times, or require minimal resources, making them suitable for resource-constrained environments. Existing methods that struggle with low scalability suffer performance degradation as the system grows. Medium security is for methods that provide adequate security but may have vulnerabilities that could be exploited under certain conditions.

TABLE I. REVIEW OF RECENT RELATED WORKS

Related Works (2020-2024)	***Authentication Factors***	***Authentication Solutions***						***Limitations***
	Type of Credentials	***Lightweight Approach***		***Basic Authentication***	***Key Agreement***	***Cryptography-based***	***Certificate-based***	
		Streamline Authentication Process	***Aggregated Authentication***					
Edge IoMT authentication protocol [54]	Pseudo-identity	No	No, single process	Single-Factor	Symmetric	Asymmetric ECC	Certificate-less	Computational Overhead Potential to replay attacks.
A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care [18]	Password and Device Authentication	Yes, PUF-based, Simplified cryptography primitives	No, single process	Multi-Factor	Symmetric key generation	Hash function	No	The reliance on device authentication can be a limitation if the device is stolen, as it could potentially be used to gain unauthorized access. Potential to side-channel attacks.
A Lightweight and Secure Authentication Scheme for Remote Monitoring of Patients in IoMT [34]	User Identity, Biometrics, and Password	Yes, lightweight	No, single process	Multi-Factor	Symmetric and Asymmetric key generation	Hash function XOR operation Asymmetric ECC	No	Implementation Complexity
A framework introduces a group authentication technique [53]	Authentication Token	Yes, non-interactive and efficient	Yes, group key agreement reduces blockchain transactions. Hierarchical aggregation	Single-Factor	Group Authentication - Shamir's Secret Sharing (SSS) algorithm.	Asymmetric ECC Hash function	No	Implementation Complexity Potential vulnerability if fog node is compromised
Design of a novel lightweight and fast membership authenticated group key agreement scheme for resource-constrained IoMT devices [55]	User Tokens	Yes, non-interactive and efficient, Simplified cryptography primitives	Yes, group key agreement combines processes	Single-Factor	Binary symmetric polynomials	XOR operation		Potential vulnerability if the Membership Registration Center (MRC) is compromised Complexity issues
Development of a Privacy-Protection Authentication Management Protocol [56]	User ID, Password and Biometric Information	No	No	Multi-Factor	Symmetric	Hash function	No	Computational overhead. Scalability concern.
Proposal of a lightweight anonymous authentication scheme based on consortium blockchain in the IoMT [57]	User ID, Password and Biometric	Yes, lightweight	No	Multi-Factor	Pre-shared, Symmetric	Hash function XOR operation	Soft and Implicit Certificates	High complexity High computational cost

Develop a blockchain-based security system with light cryptography for user authentication security [58]	Biometric, Password	Yes, lightweight Biometric-based authentication	No	Multi-Factor		Symmetric Secure hash algorithm 256 (SHA-256) Shift-AES	Soft and Implicit Certificates	Computational overhead Scalability challenges The scheme may be prone to Biometric Spoofing.
Develop a framework that utilizes fog node computing in a Blockchain-based IoMT framework [59]	Device Information	Yes	No	Multi-Factor	Elliptic Curve, Digital Signature Algorithm (ECDSA), Diffie-Helman	Hash function	-	Complexity in implementation due to the integration of multiple technologies.
Design a blockchain-based secure authentication system to safeguard Electronic Health Record (EHR) data transferred over open channels. [60]	User identity, password, and Biometric information	Yes, lightweight Biometric-based authentication	No	Multi-Factor	RSA	Hash function XOR operation Symmetric AES	-	High computational cost due to the complexity of the authentication process
A novel approach to authentication using mobile agents, elliptic curve cryptography, and a challenge/response mechanism in IoT-based healthcare systems [61]	Challenge/ response system with a secret commitment key	Yes	No	Multi-Factor	Public-key cryptography	Hash function XOR operation Asymmetric ECC	No	High complexity Adoption and integration challenges
A lightweight authentication protocol that uses Physically Unclonable Functions (PUFs) to establish a connection between a fog node and a smart device [62]	Physical Unclonable Function (PUFs)	Yes, Implicit Certificates	No	Multi-Factor	Asymmetric	Asymmetric ECC	Implicit Certificates	High complexity Key management issues
An improved three-factor-based data authentication scheme (TDTAS) [63]	Smart card, password, and biometric information	Yes, lightweight	No (Individual Device Authentication)	Multi-Factor	Asymmetric	Asymmetric ECC Hash function XOR	Hard Certificates	High computational cost Scalability concern Lack of formal verification
A novel blockchain-based authentication and key agreement protocol tailored for secure health data sharing within a cooperative hospital network [64]	User's identity, password, and Biometric information	Yes	No	Multi-Factor	Asymmetric	Asymmetric ECC	Soft and Implicit Certificates	Scalability issues Computational overhead for storing and managing authentication data

TABLE II. CONCEPTUAL EVALUATION OF THE RECENT RELATED WORKS

Ref	Efficiency	Security Robustness	Scalability	Advantages
[54]	High	Medium	Medium	Efficient ECC-based authentication. Privacy-preserving pseudo-identity. Robust against various attacks.
[18]	High	Medium	Medium	Efficient authentication using lightweight cryptography. Anonymity and privacy preservation. Robust against replay, MITM, and impersonation attacks.
[34]	High	High	Medium	Lightweight authentication for remote monitoring applications.
[53]	Medium	Medium	High	Supports scalability by allowing many devices to be authenticated efficiently.

[55]	High	Medium	High	Lightweight and efficient with XOR operations. Scalable. Robust against various attacks with forward and backward secrecy.
[56]	Medium	High	Medium	Strong security with blockchain and Chebyshev chaotic maps. Privacy-preserving with user anonymity. Comprehensive security analysis.
[57]	Medium	High	Medium	Lightweight and efficient with XOR and hash functions. Scalable with consortium blockchain. Robust security with anonymity protection.
[58]	Medium	Medium	Medium	Lightweight cryptography with Shift-AES. Achieve security with blockchain integration. Privacy-preserving hybrid authentication
[59]	Medium	High	Medium	Comparable efficiency with fog computing. Scalability through decentralized blockchain and IPFS. Robust security with ECDSA
[60]	Medium	High	Medium	Robust security with blockchain and RSA. Comprehensive security analysis. Privacy-preserving multi-factor authentication.
[61]	Medium	High	Medium	Robust security with ECC and blockchain. Distributed processing with mobile agents. Anonymity and privacy preservation.
[62]	Medium	High	Medium	Ensure user anonymity, cross-fog authentication, and efficiency without the need for a trusted third party.
[63]	Medium	Medium	Medium	Strong security with ECC and multi-factor authentication. User anonymity and privacy protection
[64]	Medium	Medium	Low	Removed the dependency on centralized storage.

From Table II, the work of Soleymani et al. [54] demonstrates high efficiency, and medium scalability with modest security, making it suitable for moderately sized IoMT deployments where security is paramount, but resource constraints are a high priority. They prioritize efficiency using pseudo-identities. However, this approach often involves trade-offs, such as reduced security robustness in the case of replay attacks where an attacker captures and reuses valid pseudo-identity credentials to gain unauthorized access in subsequent sessions. The proposed method builds on these approaches by employing streamlined cryptographic operations that incorporate nonces or timestamps into the authentication process to ensure that each session or transaction is unique minimizing computational overhead while maintaining a robust security profile, thus offering a more balanced solution for resource-constrained environments.

For many existing IoMT authentication techniques, scalability continues to be a major concern. The work of [53] and [55] demonstrates high scalability as both introduce group-based authentication to reduce the computational load associated with individual transactions. While these solutions attempt to streamline the authentication process via blockchain and group key agreement, they often introduce additional complexity. The proposed approach, however, addresses these challenges by aggregating authentication tasks using only simple cryptographic operations such as XOR or lightweight block ciphers and consolidating multiple authentication steps into fewer, more efficient processes. This approach reduces the complexity typically associated with group authentication and ensures that the proposed method can effectively scale to meet the increasing demands of IoMT networks without compromising performance or security.

Furthermore, the work of Rani and Tripathi [64] in their “Blockchain-Based Authentication and Key Agreement Protocol" is evaluated as having medium efficiency and security with low scalability indicating its limitations in large-scale, resource-constrained IoMT networks. The proposed method addresses these challenges by enhancing efficiency through lightweight cryptographic algorithms that are specifically designed for resource-constraint environments such as ECC over RSA for key agreement, using batch processing to authenticate multiple individual transactions, and minimizing the overall computational and communication overhead. This comparative evaluation helps to identify which methods are best suited for specific applications, particularly where the balance between these critical factors is essential.

In summary, the following research gaps are identified:

- Complexity and scalability of lightweight authentication algorithms. Despite several efforts made by the researchers to streamline authentication processes, many lightweight protocols still exhibit significant complexity. This complexity results from an authentication scheme that involves multiple steps, interactions, credentials (biometric authentication, fuzzy extraction, blockchain), key management, and integration of advanced cryptographic algorithms, which could limit the efficiency and scalability that is needed for a bigger-scale implementation in the IoMT ecosystem.
- Insufficient focus on Aggregated Authentication. Although some works streamline the authentication process by introducing aggregated authentication approaches such as group key agreements, these solutions are not widely adopted. Moreover, they introduce new vulnerabilities, particularly if key components are compromised. It is important to develop a robust security mechanism for aggregated authentication systems.

Thus, based on the identified research gaps in recent related works, this study intends to make recommendations for future work that addresses these issues. Consequently, the following are recommended for this study's future efforts.

- To design simplified cryptographic protocols that are lightweight and scalable. This involves streamlining cryptographic operations within the authentication processes with efficient key management techniques while maintaining robust security. For instance, further exploration of lightweight block ciphers offering lower computational overhead could be beneficial.

- One of the key challenges in IoMT is minimizing the communication overhead associated with the authentication process. Future work should explore methods for reducing the number of authentication messages exchanged between entities, thereby creating a low communication overhead. This could involve designing protocols that aggregate or combine authentication messages without compromising security. Streamlining the communication flow is essential for ensuring the efficiency and scalability of authentication protocols in large, distributed IoMT networks.

- To develop adaptive group aggregation authentication techniques to address scalability issues in large-scale IoMT setups. Innovations in group key management might include the use of hierarchical key distribution schemes or dynamic rekeying methods that can adjust key distribution processes based on network demands and usage patterns, thereby enhancing both security and scalability.

- To identify necessary requirements for designing authentication algorithms that can mitigate majority security attacks in communication. This includes addressing vulnerabilities that arise from multi-factor authentication, group authentication schemes, and the use of lightweight cryptographic primitives. Future efforts should aim to create comprehensive security frameworks that can pre-emptively address potential attack vectors, ensuring that authentication protocols remain secure as they scale.

- To implement the proposed authentication algorithms and evaluate their performance to ensure robustness.

VI. Conclusion

The current research trend in lightweight cryptography and authentication algorithms is developed to provide a secure, efficient, and scalable solution tailored to the unique requirements of the IoMT devices and infrastructure. However, striking a balance between robust security and efficient authentication performance is a significant challenge. Although a great deal of research has been done to guarantee high security in various IoT applications, potential adversary attacks are still valid and exist in our modern days. Hence, the exploration of lightweight authentication methods, decentralized authentication models, and advanced cryptographic techniques is the future research direction in the field of authentication mechanisms in IoMT.

This paper provides a comprehensive analysis of lightweight authentication methods within the context of IoMT. Therefore, two contributions have been proposed in this study, and they are:

- The study contributes to a thorough review of existing works on lightweight efficiency approach, focusing on streamlined authentication processes and aggregated authentication protocols with other current authentication solutions proposed by the authors. This review also highlighted the limitations of each approach and suggested the current state of lightweight multi-factor authentication approaches that can be used as a basis or guidance for future efforts to develop a more robust, secure, and scalable authentication protocol.

- This study also introduces the development of extended taxonomy (LAAS) for lightweight authentication protocols, emphasizing streamlining the authentication process and managing aggregated authentications. This taxonomy hopes to promote consistency against different authentication studies and contributes to the knowledge base for future researchers to develop more secure and efficient authentication mechanisms for IoMT and other similar environments.

As a conclusion, this study investigates the essential role of lightweight authentication in IoMT (Internet of Medical Things). Ensuring a secure and efficient authentication mechanism is vital to any healthcare system from malicious threats that can compromise sensitive medical data. The study analyzes recent related works on how lightweight approaches, particularly in streamlining authentication processes using various approaches such as multi-factor authentication, and other authentication solutions to identify its significant research gaps such as high computational cost, high complexity, and security vulnerabilities. It suggests that the authentication field requires further exploration to achieve more lightweight, secure, and scalable solutions. The proposed work suggests enhancing these authentication protocols through a streamlined authentication process using a more simplified cryptographic operation, multi-factor authentication, adaptive group management, and a secure encryption technique usage with the integration of advanced technologies like blockchain or AI. In a nutshell, this comprehensive review necessitates continuity for future development and innovations to safeguard the confidentiality, integrity, and functionality of the IoMT system.

Acknowledgment

The researchers express their gratitude to Universiti Teknologi Malaysia and Universiti Malaysia Sarawak for their valuable support in this study.

References

[1] N. Li et al., “A review of security issues and solutions for precision health in Internet-of-Medical-Things systems,” Secur. Saf., vol. 2, p. 2022010, 2023, doi: 10.1051/sands/2022010.

[2] S. Radack, “ELECTRONIC AUTHENTICATION: GUIDANCE FOR SELECTING SECURE TECHNIQUES,” 2004.

[3] N. Alsaeed and F. Nadeem, “Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues,” Appl. Sci., vol. 12, no. 15, p. 7487, Jul. 2022, doi: 10.3390/app12157487.

[4] M. A. Khan, I. U. Din, T. Majali, and B.-S. Kim, “A Survey of Authentication in Internet of Things-Enabled Healthcare Systems,” Sensors, vol. 22, no. 23, p. 9089, Nov. 2022, doi: 10.3390/s22239089.

[5] A. H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, “IoMT amid COVID-19 pandemic: Application, architecture, technology, and security,” J. Netw. Comput. Appl., vol. 174, p. 102886, Jan. 2021, doi: 10.1016/j.jnca.2020.102886.

[6] Y. Sun, F. P.-W. Lo, and B. Lo, “Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey,” IEEE Access, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[7] A. Kogetsu, S. Ogishima, and K. Kato, “Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy, and Trustworthiness,” Front. Genet., vol. 9, p. 167, Jun. 2018, doi: 10.3389/fgene.2018.00167.

[8] Anca D. Jurcut, Pasika Ranaweera, Lina Xu, “Chapter 2 Introduction to IoT Security,” in IoT security: Advances in authentication, 2020, pp. 27–64. [Online]. Available: https://onlinelibrary-wiley-com.ezproxy.utm.my/doi/10.1002/9781119527978.ch2

[9] “IEEE Standards Association,” IEEE Standards Association. Accessed: Jul. 19, 2024. [Online]. Available: https://standards.ieee.org

[10] N. Nanayakkara, M. N. Halgamuge, and A. Syed, “SECURITY AND PRIVACY OF INTERNET OF MEDICAL THINGS (IOMT) BASED HEALTHCARE APPLICATIONS: A REVIEW,” 2019.

[11] F. Gu, J. Niu, L. Jiang, X. Liu, and M. Atiquzzaman, “Survey of the low power wide area network technologies,” J. Netw. Comput. Appl., vol. 149, p. 102459, Jan. 2020, doi: 10.1016/j.jnca.2019.102459.

[12] W. E. Burr et al., “Electronic Authentication Guideline,” National Institute of Standards and Technology, NIST SP 800-63-2, Nov. 2013. doi: 10.6028/NIST.SP.800-63-2.

[13] S. Das, S. Namasudra, S. Deb, P. M. Ger, and R. G. Crespo, “Securing IoT-Based Smart Healthcare Systems by Using Advanced Lightweight Privacy-Preserving Authentication Scheme,” IEEE Internet Things J., vol. 10, no. 21, pp. 18486–18494, 2023, doi: 10.1109/JIOT.2023.3283347.

[14] O. B. J. Rabie, S. Selvarajan, T. Hasanin, G. B. Mohammed, A. M. Alshareef, and M. Uddin, “A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs),” Int. J. Inf. Secur., vol. 23, no. 1, pp. 51–80, Feb. 2024, doi: 10.1007/s10207-023-00748-1.

[15] M. R. Servati and M. Safkhani, “ECCbAS: An ECC based authentication scheme for healthcare IoT systems,” Pervasive Mob. Comput., vol. 90, 2023, doi: 10.1016/j.pmcj.2023.101753.

[16] S. Yu and Y. Park, “A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions,” IEEE Internet Things J., vol. 9, no. 20, pp. 20214–20228, 2022, doi: 10.1109/JIOT.2022.3171791.

[17] S. Yu and K. Park, “SALS-TMIS: Secure, Anonymous, and Lightweight Privacy-Preserving Scheme for IoMT-Enabled TMIS Environments,” IEEE Access, vol. 10, pp. 60534–60549, 2022, doi: 10.1109/ACCESS.2022.3181182.

[18] M. Masud et al., “A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care,” IEEE Internet Things J., vol. 8, no. 21, pp. 15694–15703, 2021, doi: 10.1109/JIOT.2020.3047662.

[19] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, and J. Chang, “Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT,” IEEE Internet Things J., vol. 9, no. 22, pp. 22501–22515, Nov. 2022, doi: 10.1109/JIOT.2022.3176192.

[20] V. S. Naresh, S. Reddi, and V. D. Allavarpu, “Lightweight secure communication system based on Message Queuing Transport Telemetry protocol for e - healthcare environments,” Int. J. Commun. Syst., vol. 34, no. 11, p. e4842, 2021.

[21] S. Sallam and B. D. Beheshti, “A Survey on Lightweight Cryptographic Algorithms,” in TENCON 2018 - 2018 IEEE Region 10 Conference, Oct. 2018, pp. 1784–1789. doi: 10.1109/TENCON.2018.8650352.

[22] S. Agrawal and P. Ahlawat, “A Survey on the Authentication Techniques in Internet of Things,” in 2020 IEEE International Students’ Conference on Electrical,Electronics and Computer Science (SCEECS), Bhopal, India: IEEE, Feb. 2020, pp. 1–5. doi: 10.1109/SCEECS48394.2020.86.

[23] A. S. Khan et al., “Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network,” IEEE Access, vol. 11, pp. 20524–20541, 2023, doi: 10.1109/ACCESS.2023.3249969.

[24] M. A. U. Gumis et al., “Biometric Blockchain-based Multifactor Privacy Perserving Authentication Scheme for VANETs,” J. IT Asia, vol. 9, no. 1, pp. 97–107, Nov. 2021, doi: 10.33736/jita.3851.2021.

[25] M. Fakroon, F. Gebali, and M. Mamun, “Multifactor authentication scheme using physically unclonable functions,” Internet Things, vol. 13, p. 100343, Mar. 2021, doi: 10.1016/j.iot.2020.100343.

[26] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” Cryptography, vol. 2, no. 1, p. 1, Jan. 2018, doi: 10.3390/cryptography2010001.

[27] A. K. Singh and A. Garg, “Authentication protocols for securing IoMT: current state and technological advancements,” in Securing Next-Generation Connected Healthcare Systems, Elsevier, 2024, pp. 1–29. doi: 10.1016/B978-0-443-13951-2.00004-0.

[28] S. Windarta, S. Suryadi, K. Ramli, B. Pranggono, and T. S. Gunawan, “Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions,” IEEE Access, vol. 10, pp. 82272–82294, 2022, doi: 10.1109/ACCESS.2022.3195572.

[29] U. Chatterjee, S. Ray, S. Adhikari, M. K. Khan, and M. Dasgupta, “An improved authentication and key management scheme in context of IoT-based wireless sensor network using ECC,” Comput. Commun., vol. 209, pp. 47–62, Sep. 2023, doi: 10.1016/j.comcom.2023.06.017.

[30] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” Ibm Syst. J., vol. 40, no. 3, pp. 614–634, 2001, doi: 10.1147/sj.403.0614.

[31] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A Survey of Internet of Things (IoT) Authentication Schemes,” Sensors, vol. 19, no. 5, p. 1141, Mar. 2019, doi: 10.3390/s19051141.

[32] X. Li, J. Niu, M. Karuppiah, S. Kumari, and F. Wu, “Secure and Efficient Two-Factor User Authentication Scheme with User Anonymity for Network Based E-Health Care Applications,” J. Med. Syst., vol. 40, no. 12, p. 268, Dec. 2016, doi: 10.1007/s10916-016-0629-8.

[33] I. Velásquez, “Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication,” CLEI Electron. J., vol. 24, no. 1, Apr. 2021, doi: 10.19153/cleiej.24.1.9.

[34] Z. Ali, S. Mahmood, K. Mansoor Ul Hassan, A. Daud, R. Alharbey, and A. Bukhari, “A Lightweight and Secure Authentication Scheme for Remote Monitoring of Patients in IoMT,” IEEE Access, vol. 12, pp. 73004–73020, 2024, doi: 10.1109/ACCESS.2024.3400400.

[35] M. Samal, S. Ray, and M. Dasgupta, “A Short Survey of Authentication Protocols in context of Internet of Things,” in 2023 IEEE 7th Conference on Information and Communication Technology (CICT), Jabalpur, India: IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/CICT59886.2023.10455531.

[36] 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, p. 1122, Jan. 2023, doi: 10.3390/s23031122.

[37] 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, 2022, doi: 10.1109/JIOT.2021.3080461.

[38] F. Rafique, M. S. Obaidat, K. Mahmood, M. F. Ayub, J. Ferzund, and S. A. Chaudhry, “An Efficient and Provably Secure Certificateless Protocol for Industrial Internet of Things,” IEEE Trans. Ind. Inform., vol. 18, no. 11, pp. 8039–8046, Nov. 2022, doi: 10.1109/TII.2022.3156629.

[39] A. Gupta, M. Tripathi, S. Muhuri, G. Singal, and N. Kumar, “A secure and lightweight anonymous mutual authentication scheme for wearable devices in Medical Internet of Things,” J. Inf. Secur. Appl., vol. 68, 2022, doi: 10.1016/j.jisa.2022.103259.

[40] J. Chang, Q. Ren, Y. Ji, M. Xu, and R. Xue, “Secure medical data management with privacy-preservation and authentication properties in smart healthcare system,” Comput. Netw., vol. 212, 2022, doi: 10.1016/j.comnet.2022.109013.

[41] L. Xue, Q. Huang, S. Zhang, H. Huang, and W. Wang, “A Lightweight Three-Factor Authentication and Key Agreement Scheme for Multigateway WSNs in IoT,” Secur. Commun. Netw., vol. 2021, pp. 1–15, Jun. 2021, doi: 10.1155/2021/3300769.

[42] S. S. Vankayalapati, S. Mookherji, and V. Odelu, “A Security Enhanced Authentication Protocol.” 2024. doi: 10.1109/icicv62344.2024.00129.

[43] P. Roychoudhury, B. Roychoudhury, and D. Kr. Saikia, “Hierarchical Group Based Mutual Authentication and Key Agreement for Machine Type Communication in LTE and Future 5G Networks,” Secur. Commun. Netw., vol. 2017, pp. 1–21, 2017, doi: 10.1155/2017/1701243.

[44] M. Usman, M. A. Jan, and D. Puthal, “PAAL: A Framework Based on Authentication, Aggregation, and Local Differential Privacy for Internet of Multimedia Things,” IEEE Internet Things J., vol. 7, no. 4, pp. 2501–2508, Apr. 2020, doi: 10.1109/JIOT.2019.2936512.

[45] A. S. Khan et al., “Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks,” IEEE Access, vol. 10, pp. 31273–31288, 2022, doi: 10.1109/ACCESS.2022.3159686.

[46] S. Atiewi et al., “Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography,” IEEE Access, vol. 8, pp. 113498–113511, 2020, doi: 10.1109/ACCESS.2020.3002815.

[47] M. N. Aman, M. H. Basheer, and B. Sikdar, “A Lightweight Protocol for Secure Data Provenance in the Internet of Things Using Wireless Fingerprints,” IEEE Syst. J., vol. 15, no. 2, pp. 2948–2958, Jun. 2021, doi: 10.1109/JSYST.2020.3000269.

[48] P. Gope, Y. Gheraibia, S. Kabir, and B. Sikdar, “A Secure IoT-Based Modern Healthcare System With Fault-Tolerant Decision Making Process,” IEEE J. Biomed. Health Inform., vol. 25, no. 3, pp. 862–873, Mar. 2021, doi: 10.1109/JBHI.2020.3007488.

[49] M. Malik, Kamaldeep, M. Dutta, and J. Granjal, “L-ECQV: Lightweight ECQV Implicit Certificates for Authentication in the Internet of Things,” IEEE Access, vol. 11, pp. 35517–35540, 2023, doi: 10.1109/ACCESS.2023.3261666.

[50] M. Ebrahimabadi, M. Younis, and N. Karimi, “A PUF-Based Modeling-Attack Resilient Authentication Protocol for IoT Devices,” IEEE Internet Things J., vol. 9, no. 5, pp. 3684–3703, Mar. 2022, doi: 10.1109/JIOT.2021.3098496.

[51] J. Ambareen and P. M, “Secured Wireless Sensor Network Protocol using Rabin-assisted Multifactor Authentication,” Int. J. Comput. Netw. Inf. Secur., vol. 14, no. 4, pp. 60–74, Aug. 2022, doi: 10.5815/ijcnis.2022.04.05.

[52] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, “A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks With IoT Notion,” IEEE Syst. J., vol. 15, no. 1, pp. 1120–1129, Mar. 2021, doi: 10.1109/JSYST.2020.2981049.

[53] N. Alsaeed, F. Nadeem, and F. Albalwy, “A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing,” Future Gener. Comput. Syst., vol. 151, pp. 162–181, 2024.

[54] S. A. Soleymani, S. Goudarzi, M. H. Anisi, A. Jindal, N. Kama, and S. A. Ismail, “A Privacy-Preserving Authentication Scheme for Real-Time Medical Monitoring Systems,” IEEE J. Biomed. Health Inform., vol. 27, no. 5, pp. 2314–2322, May 2023, doi: 10.1109/JBHI.2022.3143207.

[55] C. Hsu, L. Harn, Z. Xia, Z. Zhao, and H. Xu, “Fast and Lightweight Authenticated Group Key Agreement Realizing Privacy Protection for Resource-Constrained IoMT,” Wirel. Pers. Commun., vol. 129, no. 4, pp. 2403–2417, 2023, doi: 10.1007/s11277-023-10239-0.

[56] J. Miao, Z. Wang, Z. Wu, X. Ning, and P. Tiwari, “A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things,” Expert Syst. Appl., vol. 237, p. 121329, Mar. 2024, doi: 10.1016/j.eswa.2023.121329.

[57] S. Wu, A. Zhang, J. Chen, G. Peng, and Y. Gao, “A Blockchain-Assisted Lightweight Anonymous Authentication Scheme for Medical Services in Internet of Medical Things,” Wirel. Pers. Commun., vol. 131, no. 2, pp. 855–876, 2023, doi: 10.1007/s11277-023-10457-6.

[58] I. Hagui, A. Msolli, A. Helali, and F. Hassen, “Based blockchain-lightweight cryptography techniques for security information: A verification secure system for user authentication,” presented at the 2021 International Conference on Control, Automation and Diagnosis, ICCAD 2021, 2021. doi: 10.1109/ICCAD52417.2021.9638751.

[59] S. R. Mallick, R. K. Lenka, P. K. Tripathy, D. C. Rao, S. Sharma, and N. K. Ray, “A Lightweight, Secure, and Scalable Blockchain-Fog-IoMT Healthcare Framework with IPFS Data Storage for Healthcare 4.0,” SN Comput. Sci., vol. 5, no. 1, p. 198, Jan. 2024, doi: 10.1007/s42979-023-02511-8.

[60] V. Kumar, R. Ali, and P. K. Sharma, “A secure blockchain-assisted authentication framework for electronic health records,” Int. J. Inf. Technol., Feb. 2024, doi: 10.1007/s41870-023-01705-w.

[61] H. Idrissi and P. Palmieri, “Agent-based blockchain model for robust authentication and authorization in IoT-based healthcare systems,” J. Supercomput., Oct. 2023, doi: 10.1007/s11227-023-05649-7.

[62] X. Jia, M. Luo, H. Wang, J. Shen, and D. He, “A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things,” IEEE Internet Things J., vol. 9, no. 21, pp. 21838–21850, Nov. 2022, doi: 10.1109/JIOT.2022.3181609.

[63] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, “A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System,” IEEE Internet Things J., vol. 10, no. 17, pp. 15087–15099, Sep. 2023, doi: 10.1109/JIOT.2023.3264565.

[64] D. Rani and S. Tripathi, “Design of blockchain-based authentication and key agreement protocol for health data sharing in cooperative hospital network,” J. Supercomput., vol. 80, no. 2, pp. 2681–2717, Jan. 2024, doi: 10.1007/s11227-023-05577-6.