Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 3, August, 2026, pp. 388-403
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 213

Capability-Aware Authentication Mechanisms in the Internet of Medical Things (IoMT): A Systematic Literature Review

Fatima.G.Abdullah[1], Tayseer S. Atia[1]
[1] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq.

Article Info

Article history:

Received Jun.,05,2026
Revised Jul.,20,2026
Accepted Aug.,19,2026

Keywords:

Internet of Medical Things, IoMT
Authentication
Healthcare Security ,
Lightweight Authentication
Capability-Aware
Classification

ABSTRACT

The Internet of Medical Things (IoMT) has become an important component of modern healthcare systems by enabling continuous patient monitoring, remote healthcare services, and real-time medical data exchange. Despite these benefits, securing communications among interconnected medical devices remains a significant challenge due to the sensitive nature of healthcare information and the resource limitations of many IoMT devices. Authentication plays a central role in addressing these challenges by preventing unauthorized access and establishing trust among communicating entities. This paper presents a systematic literature review of authentication mechanisms developed for IoMT environments. Following the PRISMA 2020 methodology, relevant studies were collected from major scientific databases and analyzed according to their authentication techniques, security characteristics, and resource requirements. Unlike many existing reviews, this study adopts a capability-aware perspective by classifying authentication mechanisms according to the resource characteristics of the target devices, including ultra-constrained devices, resource-constrained devices, and resource-rich systems.The review shows that hash-based and physically unclonable function (PUF)-based approaches are generally suitable for highly constrained medical devices due to their low computational and energy requirements. For wearable and smart sensing devices, elliptic curve cryptography (ECC) and lightweight mutual authentication schemes provide a practical balance between security and efficiency. In contrast, resource-rich environments such as edge gateways and healthcare servers can support more sophisticated mechanisms, including public key infrastructure (PKI), blockchain-based authentication, and hybrid approaches. The findings indicate that no single authentication mechanism can satisfy the requirements of all IoMT environments. Instead, authentication design should consider both security requirements and device capabilities. The review also highlights current challenges related to scalability, heterogeneity, adaptive authentication, and post-quantum security, while identifying emerging opportunities for future IoMT authentication frameworks.

Corresponding Author:

Fatima.G.Abdullah
Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq.
Email: fatimah.g@aliraqia.edu.iq

1. INTRODUCTION

The IoMT is one of the most essential technologies for modern health care systems. By connecting implantable medical devices, wearable sensors, health monitoring systems, and cloud-based medical services with each other, the IoMT allows for continuous collection and exchange of health-related information so that health care providers improve the way they diagnose, treat and monitor patients [1],[2]. The growing use of IoMT has increased healthcare accessibility, especially in remote monitoring applications and smart healthcare settings.

While the benefits of IoMT are substantial, security and privacy remain serious concerns for these systems. Compared to traditional Internet of Things (IoT) environments, IoMT devices handle highly sensitive information that includes physiological measurements, patient records and diagnostic results. A breach in security can not only violate a patient's privacy but also affect clinical decision making and the quality of healthcare [3],[4]. As healthcare infrastructures become more interlinked, protecting medical data and providing secure communications among devices has become a priority.

Authentication is one of the key components in securing an environment that utilizes IoMT because it serves as the first line of defence against unauthorised access or malicious activities [5]. The purpose of an authentication mechanism is to verify the identity of users, devices, medical credentials, and medical servers before exchanging sensitive data. By implementing effective authentication protocols, health care resources can be protected against impersonation attacks, replay attacks, man-in-the-middle attacks, and unauthorised access [6].There is much need for trustworthy authentication in order to ensure that authenticated users can securely exchange keys and access control across a distributed healthcare network. Currently, designing effective Internet of Medical Things (IoMT) authentication solutions is challenging due to the wide diversity between the types of devices used as well as limitations associated with many of the sensors. The majority of wearable and implantable medical devices and wireless body area network (WBAN) sensors have significant limitations regarding their computational capabilities, memory capabilities, communication bandwidth, and battery power [7]. Because of these issues, traditional cryptographic techniques impose a significant amount of computational overhead, create latency on communication, and required a significant amount of energy, all of which negatively affect the performance and life of the devices [8].

To address these challenges, researchers have proposed numerous lightweight authentication mechanisms based on various cryptographic techniques, including hash functions, elliptic curve cryptography (ECC), physically unclonable functions (PUFs), blockchain-based approaches, and hybrid security frameworks [5], [9]. Although these mechanisms offer different levels of security and efficiency, selecting an appropriate authentication solution for a specific IoMT environment remains challenging due to the heterogeneity of medical devices and their resource limitations. Existing studies have primarily evaluated authentication mechanisms based on their cryptographic foundations, security properties, and resistance to specific attacks. However, limited attention has been given to the relationship between authentication mechanisms and the resource capabilities of the devices on which they are deployed.

From a practical perspective, IoMT environments encompass a wide spectrum of devices, ranging from ultra-constrained implantable sensors with strict limitations in energy, memory, and computational resources to resource-rich gateways, edge nodes, and healthcare servers capable of supporting advanced security protocols. Consequently, an authentication mechanism that performs effectively in one device category may not be suitable for another. This diversity creates a significant challenge in selecting authentication solutions that achieve an appropriate balance between security requirements and resource constraints. To address this gap, this systematic literature review adopts a capability-aware perspective and classifies authentication mechanisms into three categories: ultra-constrained devices, resource-constrained devices, and resource-rich systems. A comparative analysis is then conducted to evaluate the suitability, advantages, limitations, and security characteristics of authentication mechanisms across these categories. This capability-aware framework provides practical guidance for selecting authentication solutions that align with both device capabilities and healthcare security requirements

2. RESEARCH METHODOLOGY

The review followed the PRISMA 2020 [10] guidelines to ensure a systematic and objective selection of appropriate literature. The review sought to identify and summarize existing authentication mechanisms within Internet of Medical Things [IoMT] environments, with a focus on evaluating their suitability across different devices and resource profiles.

Studies were collected using a wide variety of scientific databases including: IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and MDPI. This selection of databases was made based on their comprehensive

coverage of cybersecurity, IoT in healthcare, and authentication-related research. Publications identified through the search were published in a timeframe of 2019-2026, although a small number of earlier studies were included to provide background information on IoMT architecture and authentication technologies such as ECC and PUFs.

A Boolean search strategy was used to identify appropriate literature based on specific keywords associated with IoMT and authentication such as “Internet of Medical Things”, “Healthcare IoT”, “Authentication”, “Mutual Authentication”, “Identity Management”, “ECC”, “PUF”, “Blockchain”, and “Lightweight Authentication”.

Peer-reviewed journal articles and conference papers, published in English, were the only resources selected for the review to ensure relevance and quality. Studies focused on encryption without authentication, studies irrelevant to healthcare environments, duplicates, editorials, or non-peer-reviewed were excluded from the review.

The selection process was representative of the PRISMA 2020 [10] workflow. 55 records were identified from the selected databases. Upon removal of ten duplicate records, 45 studies remained to be screened based on title and abstract. Of those identified in this phase, 9 studies were excluded. These studies were excluded because they did not relate specifically to IoMT authentication, had a more general focus on IoT security and did not provide meaningful discussion of authentication mechanisms. The remaining 36 studies were further assessed through full-text assessment, with five additional studies excluded due to language, publication type, or lack of authentication-based content. Consequently, 31 studies were included in the qualitative review.

Information was extracted from each study related to authentication techniques, security characteristics, computation requirements, communication overhead, energy consumption and validation methods, and analyzed independently.

Due to the nature of the authentication protocols and evaluation methods, a qualitative synthesis approach was employed to analyze the information; thus rejecting statistical meta-analysis. The studies included in the final review were organized based on target IoMT devices .thus facilitating a direct comparison of authentication mechanisms and the identification of the most appropriate mechanisms for the various types of healthcare environments. A PRISMA 2020 flow diagram, described in Figure 1, demonstrates the study identification, screening, eligibility assessment and inclusion processes

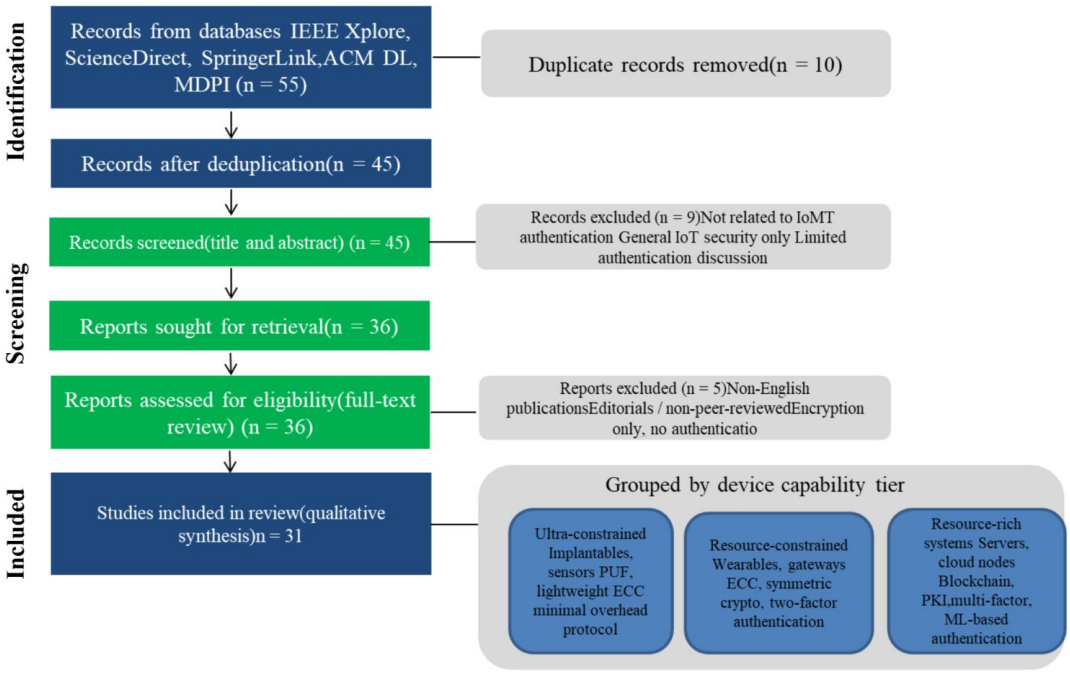

Figure 1. PRISMA 2020 flow diagram of the study selection process and capability-based classification of the included studies.

3. IOMT ENVIRONMENT AND AUTHENTICATION REQUIREMENTS

To design effective IoMT authentication, one must understand the environment's architecture, security requirements, and resource constraints. Consequently, this section outlines these foundational factors, which vary significantly across diverse healthcare devices

3.1 IOMT ARCHITECTURE

The Internet of Medical Things (IoMT) is frequently constructed as a multiple-tiered architectural approach to obtain, transmit, process, and archive health-related information in a systematic fashion. This structure allows for smooth communication between medical devices and healthcare professionals and between medical devices and healthcare information systems in order to support a number of different types of applications, such as remote patient management,

chronic disease management, and emergency health services [11], [12]. Figure2 provides a representative example of IoMT architectures consisting of numerous layers.

The Device Layer functions as the lowest layer in terms of architecture, consisting of wearable biosensors, implanted medical devices, smart medical equipment, and patient monitoring systems. This layer produces physiological measurements such as pulse rate, blood pressure, blood glucose, and body temperature. However, many of the medical devices in this layer have very limited resources, including a limited battery life, limited processing capacity, and limited memory resources; therefore, any security measures deployed on the Device Layer must be able to offer security that is lightweight and consume very little energy [13].

The Edge Layer functions as the intermediate layer between medical devices and cloud infrastructures and comprises gateways, edge servers, and fog-computing nodes. Edge Computing nodes aggregate data from multiple medical devices and send it on to the upper layers of the architecture. Besides reducing network congestion, the Edge Layer should provide local processing and very fast response times to time-sensitive health events. Because of the Node's larger computing capacity, more robust authentication and access-control mechanisms can be deployed at the edge than can be at the Device Layer [14].

The Cloud Layer is the highest layer in the IoMT architecture and consists of large-scale storage, centralized management, and advanced data analytics. The Cloud Layer combines data from EHR's (electronic health records), decision-support systems, and machine-learning-based applications to assist healthcare providers in diagnosis and treatment. Because the Cloud Layer processes life-sustaining data; therefore, it is critical that robust authentication and identity-management processes are implemented to ensure that only authorized users are able to gain access to the information in the Cloud Layer while simultaneously maintaining the privacy of the patient [15].

Although working together to assist in providing health services, the different layers of the IoMT architecture differ significantly regarding the types of computation, modes of communications, and security requirements; hence, an authentication mechanism designed for one layer will not be suitable for use in another layer. Therefore, considering the different layers in the IoMT architecture is critical in evaluating various options for providing authentication in heterogeneous IoMT environments

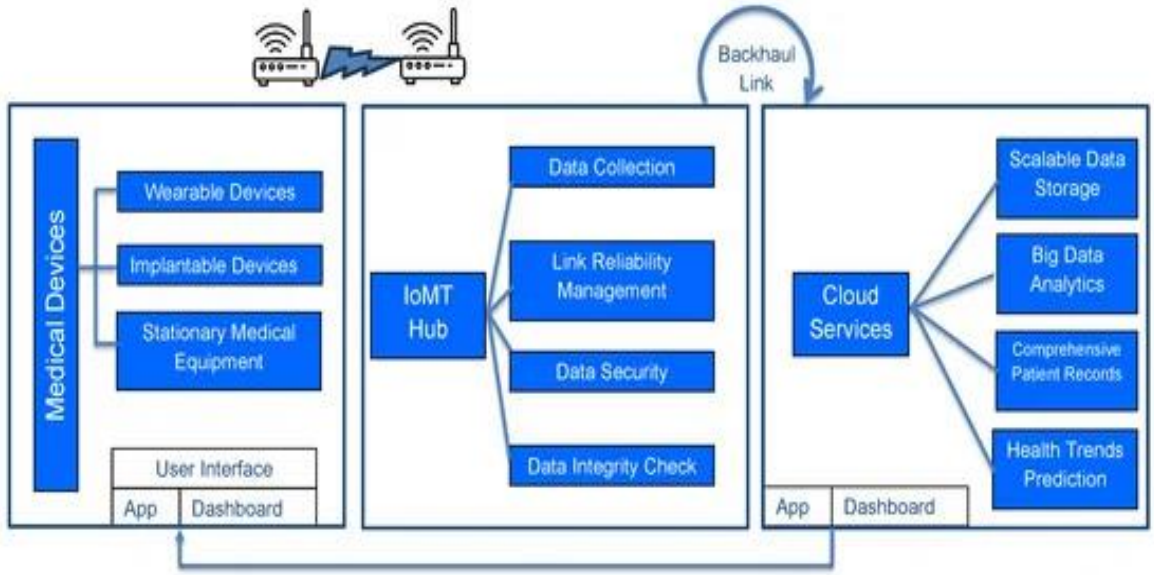

Figure 2. Three-layer IoMT architecture consisting of device, edge, and cloud layers[16].

3.2 SECURITY REQUIREMENTS

Due to the sensitive nature of medical care information, Internet of Medical Things (IoMT) has a need for built in security mechanisms. Because medical devices continuously create, transmit, and store patient-related data, they are viewed as prime targets for cyberattack. For this reason, authentication mechanisms specifically designed for IoMT systems must meet a number of necessary security requirements to ensure the delivery of trusted and secure healthcare [3]‹[5]. One of the most critical requirements is confidentiality, which ensures that sensitive medical information is only accessed by those with appropriate authorization. In order to maintain patient trust and comply with regulations governing the handling of healthcare data, it is critical that patient records, physiological measurements, and clinical data are kept confidential from unauthorized disclosure [17]. Another important requirement is integrity, which ensures that medical information remains accurate and unaltered during both storage and transmission. If healthcare data is not kept accurate and unaltered, there is an increased risk of making inaccurate diagnoses or inappropriate medical decisions, both of which can have serious implications for patient safety [18].Additionally, availability is particularly vital to the healthcare environment timely access to healthcare data can be crucial to saving lives. Hence, authentication mechanisms must provide their intended security without introducing significant latencies or causing interruptions to clinical operations [19]. Privacy is a key requirement in IoMT systems healthcare-related information is viewed as very sensitive, personal information. Privacy mechanisms should prevent unauthorized parties from tracking users, identifying patients, or deriving confidential health conditions from communication patterns, in addition to protecting the data contents [18]‹[20]. Finally, mutual authentication is a requirement to establish a trust relationship between two or more communicating entities in IoMT systems. Entities should authenticate the identity of each other using an authentication mechanism before exchanging medical information. The implementation of mutual authentication within IoMT systems will help to ensure that impersonations, replay attacks and man-in-the-middle (MITM) attacks do not succeed, thus enhancing the overall security of IoMT infrastructures [21]. When considered together, confidentiality, integrity, availability, privacy, and mutual authentication represent the core principles underlying secure authentication frameworks associated with IoMT environments. Therefore, an authentication mechanism should aim to achieve a proper balance between these security objectives while still being compatible with the resource-constrained and operationally-limited capabilities of medical devices.

3.3 RESOURCE CONSTRAINTS

Many IoMT devices operate under strict resource limits, which will have a noticeable effect on how the devices are designed and subsequently authenticated. Many will have to maintain low power consumption and high levels of performance, while continuously functioning for extended periods; this is the case for wearable sensors, implantable medical devices, and portable monitoring systems [19][22].

One of the main limitations facing these types of devices is energy consumption, as many of them use batteries and need to operate for long periods (generally measured in weeks) without needing to be frequently charged or replaced. Therefore, when using authentication protocols that include high levels of cryptographic operation or a high frequency of message exchange, there is an increase in the energy consumed by the devices, which reduces their total life span [23].

In addition to energy constraints, IoMT devices have very little memory available in their limited resource environments due to the fact that many of the medical sensors will have limited storage capacity, making it difficult to implement authentication schemes, such as those requiring large cryptographic keys or certificates or significant amounts of data stored in security databases. Therefore, in a resource-constrained healthcare environment, it is extremely likely that memory-efficient security mechanisms will be preferred over larger security mechanisms[13].

Another significant challenge is the limited computation capability of IoMT devices. Additionally, as many of these devices contain low-power processors that are not designed to handle computationally intensive cryptographic algorithms well, authentication mechanisms for IoMT systems must carefully define the trade-off between strength of security and computational overhead to minimize the degradation of device performance [21].

Lastly, communication resources for IoMT devices can be very difficult due to their limited bandwidth, unstable wireless links, and use of low-power networking technologies. Furthermore, the excessive communication overhead generated by authentication processes can add significant delays to processing times or cause excessive amounts of energy to be consumed and can further decrease the reliability of the healthcare services provided through using the IoMT device. These types of issues are even more important for systems requiring real-time monitoring and rapid response times [19]،[24].

Given the identified constraints, it is clear that there is a need for IoMT devices to implement authentication mechanisms that provide adequate security, while limiting energy consumption, memory usage, computational costs, and overhead in communications. Achieving this balance is one of the biggest challenges in securing the IoMT environment during its initial design and deployment..

4. CAPABILITY-AWARE CLASSIFICATION OF AUTHENTICATION MECHANISMS

Authentication mechanisms in IoMT are designed for devices with different resource capabilities and operational requirements. Therefore, selecting an appropriate authentication approach depends not only on security requirements but also on the computational, memory, and energy constraints of the target device. Based on the reviewed literature, authentication mechanisms can be classified into three categories: authentication for ultra-constrained devices, resource-constrained devices, and resource-rich systems.

4.1 AUTHENTICATION FOR ULTRA-CONSTRAINED DEVICES

Within the IoMT ecosystem, ultra-constrained devices are defined as the resource-limited portion of the ecosystem. The ultra-constrained category includes mainly implantable medical devices (IMD), wireless body area network (WBAN) sensors and miniature sensor devices which can monitor human health by continuously collecting a variety of physiological data such as heart rate, blood pressure, glucose level and body temperature [13], [25]. Each of these devices usually has a very small battery capacity, is limited in terms of memory resources, and has very low computing power; therefore, traditional methods of authentication cannot be easily implemented.

In the healthcare domain, an authentication protocol must provide sufficient security without excessively increasing power usage or communication overhead. For ultra-constrained devices, resource efficiency is as important as security itself, since excessive cryptographic operations can shorten the life of ultra-constrained devices as well

affect the continuity of services [26]. As result, lightweight methods of authentication have been established as the preferred authentication solution for ultra-constrained devices.

Among the many suggested solutions, hash-based authentication schemes have been more widely accepted due to their relatively low computational complexity and memory storage requirements. Using hash functions, devices can verify their identities and authenticate messages, while expending fewer computing resources compared to the resources required to implement public-Key cryptographic algorithms. Reports indicate that hash-based protocols can provide a suitable level of security while using very little energy; therefore, these types of authentication mechanisms make ideal solutions for implantable and WBAN-based applications in the healthcare industry [6].

Another emerging method for providing a lightweight authentication scheme is the use of Physically Unclonable Functions (PUFs). Unlike traditional authentication methods that require secret key(s) to store on a device, PUF based methods establish the identity of a device based on the unique physical characteristics that are created during the manufacturing process. This characteristic can help reduce memory usage and provide resistance to the physical cloning of devices, which is especially valuable to ultra-constrained healthcare devices [27]. The increasing popularity of PUF based authentication methods as a lightweight alternative for securing medical sensors and implantable devices has emerged in recent years.
According to the literature reviewed, both hash-based and PUF-based authentication mechanisms exhibit excellent suitability for ultra-constrained IoMT devices, primarily because both types of authentication mechanisms have low computing overheads and require very little storage; therefore, both types of authentication mechanisms are viable alternatives for environments in which achieving energy efficiency and lightweight operation are key design factors. Table 1 provides a summary of capability-aware authentication mechanisms that can be utilized by ultra-constrained IoMT devices.

Table 1. Capability-aware authentication mechanisms for ultra-constrained IoMT devices.

Device Type	Resource Constraints	Authentication Technique	Main Benefits	Limitations
Implantable Medical Devices (IMDs)	Extremely limited battery, memory, and computation	Hash-Based Authentication	Low computational overhead, energy efficient	Limited scalability and advanced security features
WBAN Sensors	Limited energy and processing capability	Hash-Based Authentication	Fast authentication and low communication cost	Vulnerable if poorly designed
Implantable Medical Devices	Limited secure storage capability	PUF-Based Authentication	No secret-key storage, resistance to cloning attacks	Requires dedicated hardware support
Miniature Medical Sensors	Low memory and energy resources	Lightweight PUF-Based Schemes	Reduced storage requirements and lightweight operation	Hardware variability may affect reliability

4.2 AUTHENTICATION FOR RESOURCE-CONSTRAINED DEVICES

Many resource-constrained devices are included in the current IoMT ecosystem. This group of devices includes wearable health care devices, smart medical sensors, fitness trackers and portable monitoring systems that continuously gathering and transmitting data related to patients. Although these devices provide more computational and storage resources than devices that are implantable and add-on WBANs have, they also have limitations associated with battery capacity, processing power, and communication efficiency [1], [5].

The increase in the use of wearables in health care technology has led to an increased demand for authentication mechanisms that can provide an increased level of security without adding to the overhead of a device's performance. As it generally is the case with devices of this type, there are often many times when sensitive medical information is exchanged between these devices and their associated gateways, mobile applications and health care servers, therefore the authentication protocols need to be able to protect these communications while still allowing for a quick response from their devices as well as minimizing battery usage [6].
As a result of the above, many researchers have chosen to use Elliptic Curve Cryptography (ECC) as a viable mechanism for implementation on wearable and smart sensing devices. The other strength of ECC, when compared to traditional public-key cryptography, is that ECC provides comparable security with smaller key sizes and as such provides lower computational and communication costs, making it very attractive to the health care industry, where

more robust security assurances are required but cannot hold the overhead associated with high cost cryptographic processes [28].

The other class of protocols that have received a lot of attention as a means to provide security for IoMT devices is lightweight mutual authentication. Lightweight mutual authentication allows two or more communicating entities to verify one another's identities before they exchange sensitive information, thus reducing the possibility of impersonation or unauthorized access. The rationale for utilizing the lightweight mutual authentication technique in IoMT environments is to provide additional security to IoMT entities while utilizing minimal resources. Due to the above, lightweight mutual authentication has become a popular design technique in wearable health care and smart medical sensing environments [29].

In conclusion, the literature indicates that many resource-constrained devices benefit from using very efficient authentication mechanisms that maximize both security and efficiency. Due to their size and efficient design, hash-based approaches continue to be used by highly constrained devices; however, ECC-based and lightweight mutual authentication mechanisms provide a greater level of protection and flexibility for wearables and smart sensors and place no significant performance burden on conventional public key infrastructures. Table 2 describes the capability aware authentication mechanisms discussed above that are appropriate for use on resource-constrained IoMT devices, along with their respective benefits and associated challenges.

Table 2. Capability-aware authentication mechanisms for resource-constrained IoMT devices.

Device Type	Authentication Technique	Rationale	Advantages	Challenges
Wearable Healthcare Devices	ECC-Based Authentication	Moderate computational capability allows lightweight public-key cryptography	Strong security with reduced key sizes	Higher computational cost than hash-based schemes
Smart Medical Sensors	ECC-Based Authentication	Suitable balance between security and resource consumption	Reduced communication and storage overhead	Energy consumption remains a concern in long-term deployments
Wearable Devices	Lightweight Mutual Authentication	Frequent communication requires secure identity verification	Improved resistance to impersonation and replay attacks	Additional communication exchanges may increase latency
Portable Monitoring Systems	Lightweight Mutual Authentication	Supports secure interactions with gateways and healthcare servers	Balanced security and efficiency	Performance depends on protocol design

4.3 AUTHENTICATION FOR RESOURCE-RICH DEVICES

Upper layers contain resource rich devices which form the IoMT infrastructure. This includes edge gateways, hospital servers, cloud connected healthcare platforms, and centralized management systems. Resource rich devices differ from wearable sensors and implantable devices in that resource rich devices contain greater processing capabilities, storage capabilities, and communication functions. Because of this, resource-rich devices support more advanced authentication and security mechanisms than wearable sensors and implantable devices [1],[19].

Within healthcare environments, these resource-rich devices act as central access points for aggregation of data, access control security and service management. Because of this, security breaches at these resource rich device levels can affect a large volume of medical data stored on a number of different connected devices. Therefore, the authentication mechanisms for resource-rich devices in healthcare environments generally emphasize strong security, scalability, and trust management versus resource efficiency[26].

The Public Key Infrastructure (PKI) is one commonly used authentication mechanism for resource-rich devices. PKI authentication utilizes Digital Certificates and Certificate Authorities that are trusted to establish secure identity and validation for entities communicating over the internet. PKI's ability to provide centralized trust management in a scalable way makes it an excellent fit for hospital information systems, healthcare servers and medical networks on an enterprise level[30].

Block chain technology is also an emerging authentication mechanism. Block chain technology utilizes Distributed Ledger Technology to provide decentralized trust, transparency and tamper resistant records. In healthcare applications, Block chain can assist and authenticate processes through lessening the dependency on a centralized authority and providing greater integrity of data maintained by multiple stakeholders. Because of these benefits, Block chain authentication mechanisms are receiving increased attention in the IoMT research literature, particularly in the context of inter-organizational healthcare environments[9].

Recent studies have increasingly focused on hybrid authentication mechanisms that integrate multiple security technologies, including PKI, blockchain, biometrics, and lightweight cryptography. These approaches aim to combine the advantages of different security methods while overcoming their individual weaknesses.Hybrid authentication mechanisms will allow the benefits of all mechanisms to be utilized while also mitigating the limitations of each individual mechanism. The use of hybrid mechanism is particularly beneficial in complex healthcare ecosystems where many types of devices and types of security are required to co-exist[31].

The literature review shows that resource rich devices are capable of employing authentication mechanisms that are prohibitively expensive to deploy on constrained medical sensor devices. Therefore, PKI based authentication mechanisms, Block chain based authentication mechanisms and hybrid authentication mechanisms are more appropriate for deploying on Edge Gateways, Hospital Servers, and Healthcare Management Platforms where strong security, scalability, and trust management are a top concern. Table 3 summarizes the category of authentication mechanisms which resource rich IoMT devices can support, along with their Benefits and Challenges of Implementing.

Table 3. Capability-aware authentication mechanisms for resource-rich IoMT devices

Device Type	Authentication Technique	Rationale	Advantages	Challenges
Edge Gateways	PKI-Based Authentication	Sufficient computational resources for certificate management	Strong identity verification and trust management	Certificate lifecycle management
Hospital Servers	PKI-Based Authentication	Supports large-scale healthcare infrastructures	Scalable and widely adopted	Increased administrative complexity
Edge Gateways	Blockchain-Based Authentication	Capable of supporting distributed trust mechanisms	Enhanced integrity and decentralization	Storage and latency overhead
Healthcare Platforms	Blockchain-Based Authentication	Supports multi-stakeholder healthcare environments	Tamper-resistant authentication records	Integration complexity
Hospital Servers	Hybrid Authentication	Combines multiple security technologies	Improved flexibility and security	Higher implementation complexity
Healthcare Management Systems	Hybrid Authentication	Suitable for heterogeneous IoMT environments	Adaptable to diverse security requirements	Increased deployment cost

5. COMPARATIVE ANALYSIS

The studies analyzed in this review show that device capabilities are a key factor in determining how an IoMT authentication mechanism is designed. As outlined in the prior section, different healthcare environments have different authentication requirements. A protocol that works well for an implantable sensor may not provide

sufficient security for a hospital server, and it is often impractical to implement resource-intensive authentication mechanisms on devices that rely on battery power.

Two lightweight approaches remain the primary authentication mechanism of choice for ultra-constrained devices like implantable medical devices and WBAN sensors. Hash-based authentication schemes are commonly used because they have low computational and communication costs; however, PUF-based schemes also reduce the need for secure key storage. Together these two approaches are well-suited for environments where energy efficiency is a primary consideration.

Resource-constrained devices, such as wearable healthcare devices and smart medical sensors, have sufficient resources available to support stronger authentication mechanisms while still operating under resource constraints . The ECC-based authentication schemes developed for resource-constrained devices have been widely researched as they provide stronger protection from a cryptographic standpoint than lightweight hashing schemes without introducing the overhead associated with traditional public key cryptography solutions. Consequently, lightweight mutual authentication protocols have been developed for use between entities to strengthen the trust relationship while maintaining an acceptable performance level.

Resource-rich devices such as edge gateways, hospital servers, and healthcare management platforms can implement more robust authentication mechanisms. PKI-based authentication solutions continue to be popular due to their mature capabilities in trust management and scalability. Blockchain-based solutions are receiving increasing attention as they enhance the trust environment by providing decentralized trust and tamper-resistance in record management. Hybrid authentication solutions are also becoming an increased focus for complex healthcare ecosystems that require multiple layers of security protection.

The comparison provided in Table 4 demonstrates a clear correlation between increased security and increased computational and communication costs. Therefore, no single authentication mechanism is appropriate for all IoMT environments. The decision regarding what authentication mechanism to use should be based primarily on the available resources of the device and the security requirements of the specific application. This finding supports the capabilities-informed focus of this review while also demonstrating the importance of an authentication mechanism design that aligns with the device capabilities.

Table 4. Comparative analysis of authentication mechanisms across different IoMT device classes

Ref.	Authentication Technique	Device Class	Energy Cost	Computation Cost	Security Level
[25]	Hash-Based Authentication	Ultra-Constrained	Low	Low	Medium
[27]	PUF-Based Authentication	Ultra-Constrained	Low	Low	Medium–High
[28]	ECC-Based Authentication	Resource-Constrained	Medium	Medium	High
[29]	Lightweight Mutual Authentication	Resource-Constrained	Medium	Low–Medium	High
[30]	PKI-Based Authentication	Resource-Rich	High	High	Very High
[9]	Blockchain-Based Authentication	Resource-Rich	High	High	Very High
[31]	Hybrid Authentication	Resource-Rich	Medium–High	Medium–High	Very High

6. SECURITY ANALYSIS

In IoMT environments, security is one of the most significant criteria for evaluating the reliability of authentication methods. Due to the continued transfer of sensitive health information between medical devices, an authentication method should be designed to prevent the most common attacks associated with device identity, channel and system availability methods. The literature suggests that although most IoMT authentication methods are designed to

mitigate the same set of threats, the level of security protection is determined by both the authentication method used and the capabilities of the devices for which it is being used [3], [26].

Replay attacks are commonly cited as one of the main attacks discussed in the research literature concerning IoMT authentication. In replay attacks, an adversary captures a previously transmitted authentication message (the initial authentication message) and attempts to send that same authentication message through the IoMT, potentially gaining access to the device without being authenticated. To mitigate this attack, a number of IoMT authentication methods implement mechanisms for establishing freshness of communication messages through timestamps, nonces, and challenge-response mechanisms [21], [26].

Another widely discussed attack is the man-in-the-middle (MITM) attack. In a MITM attack, an attacker positions herself between two legitimate parties and attempts to capture or alter the communication between them. Generally, an authentication method employing mutual authentication and a secure method for establishing a temporary authenticated session will provide a greater degree of security with respect to a MITM attack. It is widely accepted that authentication methods based on ECC, PKI, and blockchain technology are effective in mitigating the risk of MITM attacks due to the robust mechanisms they employ for verifying the identity of both parties [5], [19].

Impersonation attacks pose a serious risk to healthcare entities because malicious persons attempt to assume the identity of authenticated users, medical devices, and healthcare servers in order to successfully gain access to medical records or healthcare services that would require an authenticated identity. As a result, most of the authentication methods reviewed in this paper incorporated identity verification mechanisms to ensure that only users/entities that can be identified as authorized are able to participate in the communication process [6], [21].

Insider attacks are characterized by successful unauthorized attempts to access an IoMT system made by users that have legitimate access to the system. The characteristics of insider attack vectors make them more difficult to handle than traditional external attack vectors. The reviewed research shows authentication systems with a combination of access control, trust management, and comprehensive identity management generally provide significantly more protection against insider attacks than authentication systems without these comprehensive features, especially within resource-rich healthcare settings [3], [20].

Denial-of-Service (DoS) attacks are another significant security concern for IoMT devices, particularly resource-constrained medical devices. DoS attacks typically occur when an attacker floods a device with excessive authentication requests or generates excessive communication traffic causing a loss of available device resources. This is especially true for battery powered devices, where additional communication reduces battery life. Because of this, lightweight authentication methods typically attempt to minimize communication and computation overhead as a method of defense against DoS threats [19], [23].

Research conducted in this study indicates that no authentication method can provide absolute security protection against all attacks; however, an authentication method that combines robust identity verification, mutual authentication, and efficient resource utilization will demonstrate the best security performance across multiple types of IoMT environments. Therefore, choosing an authentication method based on the specific security needs of the IoMT environment and the manufacturer of the end devices is highly recommended. Table 5 summarizes the overall security capabilities of each authentication mechanism reviewed in relation to all identified threats associated with IoMT environments, including replay attacks, man-in-the-middle attacks, impersonation attacks, insider threats and Denial-of-Service attacks.

Table 5. Security analysis of authentication mechanisms in IoMT

Authentication Technique	Replay Attack	MITM Attack	Impersonation Attack	Insider Attack	DoS Attack	Overall Security
Hash-Based Authentication	✓	✓	✓	Partial	Partial	Medium
PUF-Based Authentication	✓	✓	✓	Partial	Partial	Medium–High
ECC-Based Authentication	✓	✓	✓	✓	Partial	High
Lightweight Mutual Authentication	✓	✓	✓	Partial	Partial	High
PKI-Based Authentication	✓	✓	✓	✓	✓	Very High
Blockchain-Based Authentication	✓	✓	✓	✓	✓	Very High
Hybrid Authentication	✓	✓	✓	✓	✓	Very High

7. OPPORTUNITIES AND CHALLENGES RELATED TO AUTHENTICATION OF IOMT DEVICES

The literature pertaining to this topic indicates that significant advancements have been made in the area of investigation of IoMT in relation to the creation of new and enhanced methods of authentication. However, there are still numerous barriers that have the potential to hinder the long-term implementation of many of these solutions. As the healthcare industry continues to develop a more interconnected ecosystem through new and improved technologies, these barriers must be addressed to establish a framework of authentication that achieves security, efficiency, and adaptability in real-world environments.

Another point of observance through the literature was the lack of adaptability of current forms of authentication. There are currently a number of authentication mechanisms that have been developed, but the vast majority operate under predetermined (fixed) parameters regardless of any changes that may occur with respect to the capabilities of devices, network conditions, or security threats. While these mechanisms may provide adequate levels of security in controlled environments, they do not provide flexibility that is essential for devices within an ever-changing healthcare environment where both devices and security requirements may differ widely[1],[26].

Another challenge relates to the gap between prototype systems for authentication and actual deployment. Most of the mechanisms used to authenticate devices have either been tested using simulations or through theoretical analyses. There is a large gap in the literature examining the actual performance of authentication methods on live devices in the healthcare environment. Therefore, there remain a number of questions regarding long-term reliability, interoperability and operational feasibility[1],[19].

Scalability is another important aspect of future development of IoMT ecosystems and should be addressed. Future IoMT Ecosystems are expected to operate on large quantities of interconnected devices, healthcare providers, cloud services, and edge infrastructure relative to the number of devices that are currently considered to be part of an IoMT ecosystem. Authentication methods that work efficiently in smaller installations can be significantly less efficient in larger-scale environments due to increased communication overheads, higher management complexity and decreased performance [19], [26]. Similarly, the heterogeneous nature of the IoMT systems contributes to added complexity. Modern healthcare infrastructures blend together a variety of elements including (but not limited to) implantable devices, wearable sensors, mobile applications, edge gateways, and cloud-based platforms, thus creating environments that often include devices with wide variances in capabilities. Consequently, designing authentication methodologies that function optimally over significant variations in device capabilities is not only difficult but continues to drive research for more adaptable security frameworks [13].

Although post-quantum cryptography (PQC) is emerging as an area of great interest within research, the result of this research has had very limited successful application for authentication in IoMT [19]. The majority of quantum-compliant algorithms will consume more computing resources and will have greater communication overhead than traditional cryptographic methods creating an impediment to the development and implementation of viable solutions that could be implemented with limited resources on devices used for healthcare. Therefore, identifying lightweight implementations of PQC suitable for IoMT will be an important research opportunity.

Several evolving technologies will help facilitate solving the challenges discussed above. For example, many researchers have begun using artificial intelligence to enhance authentication methodologies by employing techniques such as behavioral analysis, anomalous behavior detection and context-sensitive decision making. Other emerging authentication techniques (e.g., adaptive authentication) are investigating additional factors such as whether the device being authenticated has attributes similar to the one being authenticated as well as evaluating operational conditions prior to using more stringent security measures. Both of these types of authentication methodologies will help achieve a balance between high security and minimal use of resources.

Another area of ongoing research that is promising in healthcare is leveraging Zero Trust principles. Rather than authenticate based upon a predefined set of trust-given relationships, Zero Trust architectures are based upon the continuous validation of all users, devices and services that communicate with each other. With this approach, it should be possible to increase resiliency against insider threats, compromised devices and unauthorized access attempts [3].

Finally, federated learning can facilitate the development of privacy-preserving authentication frameworks. Federated learning can allow for collaborative model training without the transmission of sensitive medical/health records to central locations thereby allowing the utilization of intelligent security services, while minimizing the privacy concerns associated with traditional machine learning methods. Combining federated learning with an authentication mechanism will lead to much more secure and privacy-preserving healthcare ecosystems.

Overall, the issues identified in the current literature demonstrate that there is a critical need for authentication mechanisms that are secure and that can also adapt, can scale, and can support highly heterogeneous healthcare environments. Attempting to solve these issues will ultimately play a major role in shaping the IoMT systems of the future.

8. CONCLUSION

The Internet of Medical Things (IoMT) is rapidly expanding and presents new opportunities to provide improved health care services through such areas as patient monitoring, remote health care, and intelligent medical systems. However, with the increased number of devices that are **interconnected with** one another **comes** the concern for the security of those devices; thus, authentication of IoMT devices becomes a critical requirement in protecting health data and ensuring trusted communications among IoMT devices.

This paper, reviews the existing authentication mechanisms published in the literature regarding IoMT systems and their analysis using a capabilities-aware approach. The studies reviewed were categorized beyond just the type of cryptography used for authentication into categories based on the resource limitations of the devices intended to utilize the authentication mechanism. This classification demonstrated how the capabilities of IoMT devices directly impact the selection of authentication mechanisms and their effectiveness.

As demonstrated in the results, lightweight authentication techniques such as hash-based and PUF-based authentication are still the best choice for use with highly-constrained devices, while ECC-based and lightweight mutual authentication schemes are an appropriate middle-ground between secure and efficient method to authenticate wearable and smart sensing devices. In resource-rich environments, stronger authentication solutions such as PKI, blockchain, or hybrid mechanisms may be used to meet the rigorous security requirements of these advanced communications and large-scale health care.

The analysis further demonstrated that there is no single authentication mechanism that will satisfy every IoMT environment. Due to the vast differences between devices (e.g., capabilities, energy available, computational resources, and security needs), an appropriate authentication strategy will differ among all IoMT devices. Therefore, when selecting an authentication mechanism, the selection will be based on both security and also the operational characteristics of the health care environment.

Through this review, it is clear that the importance of aligning authentication design to device capabilities in heterogeneous IoMT systems cannot be overstated. As health care technology continues to evolve, developing authentication frameworks that are adaptable, scalable, and resource-aware will become a major focus of future research.

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

There is no funding for this work.

REFERENCES

[1] 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.
[2] S. M. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.
[3] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, Singapore: IEEE, Oct. 2017, pp. 112–120. doi: 10.1109/LCN.Workshops.2017.72.
[4] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS".
[5] 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.
[6] 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.
[7] A. Merchant, V. Panchami, S. Justine, and S. Eswaran, "An efficient lightweight authentication scheme for smart healthcare in IoMT applications," *Discov. Comput.*, vol. 28, no. 1, p. 261, Nov. 2025, doi: 10.1007/s10791-025-09779-9.
[8] M. Tanveer, S. A. Chelloug, M. Alabdulhafith, and A. A. A. El-Latif, "Lightweight authentication protocol for connected medical IoT through privacy-preserving access," *Egypt. Inform. J.*, vol. 26, p. 100474, Jun. 2024, doi: 10.1016/j.eij.2024.100474.
[9] A. S. Rajasekaran, A. Maria, M. Rajagopal, and J. Lorincz, "Blockchain Enabled Anonymous Privacy-Preserving Authentication Scheme for Internet of Health Things," *Sensors*, vol. 23, no. 1, p. 240, Dec. 2022, doi: 10.3390/s23010240.
[10] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.
[11] H. Geng, Ed., "Front Matter," in *Internet of Things and Data Analytics Handbook*, 1st ed., Wiley, 2017. doi: 10.1002/9781119173601.fmatter.
[12] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," *IETE Tech. Rev.*, vol. 39, no. 4, pp. 775–788, Jul. 2022, doi: 10.1080/02564602.2021.1927863.
[13] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic, "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018, doi: 10.1109/JIOT.2018.2849014.

[14] S. E. El-deep, A. A. Abohany, K. M. Sallam, and A. A. A. El-Mageed, "A comprehensive survey on impact of applying various technologies on the internet of medical things," *Artif. Intell. Rev.*, vol. 58, no. 3, p. 86, Jan. 2025, doi: 10.1007/s10462-024-11063-z.
[15] M. K. Patra, A. Kumari, B. Sahoo, and A. K. Turuk, "Smart Healthcare System Using Cloud-Integrated Internet of Medical Things:," in *Advances in Medical Technologies and Clinical Practice*, R. Queirós, B. Cunha, and X. Fonseca, Eds., IGI Global, 2022, pp. 60–83. doi: 10.4018/978-1-6684-5260-8.ch004.
[16] P. Matthew *et al.*, "A Review of the State of the Art for the Internet of Medical Things," *Sci*, vol. 7, no. 2, p. 36, Mar. 2025, doi: 10.3390/sci7020036.
[17] M. A. G. Hazber *et al.*, "Securing IoMT-Based Healthcare Systems with Meta-Heuristic Quantum Cryptography and Honeybee Optimization," Dec. 12, 2024, *In Review*. doi: 10.21203/rs.3.rs-5447617/v1.
[18] P. Verma, R. Tiwari, and W.-C. Hong, "Secure Authentication in IoT Based Healthcare Management Environment Using Integrated Fog Computing Enabled Blockchain System," in *Image Based Computing for Food and Health Analytics: Requirements, Challenges, Solutions and Practices*, R. Tiwari, D. Koundal, and S. Upadhyay, Eds., Cham: Springer International Publishing, 2023, pp. 137–146. doi: 10.1007/978-3-031-22959-6_8.
[19] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," *IEEE Access*, vol. 9, pp. 4466–4489, 2021, doi: 10.1109/ACCESS.2020.3047895.
[20] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.
[21] T.-Y. Wu, Q. Meng, S. Kumari, and P. Zhang, "Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments," *Sensors*, vol. 22, no. 10, p. 3858, May 2022, doi: 10.3390/s22103858.
[22] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," *Sensors*, vol. 22, no. 19, p. 7433, Sep. 2022, doi: 10.3390/s22197433.
[23] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sens. J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016, doi: 10.1109/JSEN.2015.2502401.
[24] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016, doi: 10.1016/j.comnet.2016.01.009.
[25] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018, doi: 10.1109/JIOT.2017.2780232.
[26] 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.
[27] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016, doi: 10.1109/ACCESS.2015.2503432.
[28] A. H. Koblitz, N. Koblitz, and A. Menezes, "Elliptic curve cryptography: The serpentine course of a paradigm shift," *J. Number Theory*, vol. 131, no. 5, pp. 781–814, May 2011, doi: 10.1016/j.jnt.2009.01.006.
[29] S. Das and S. Namasudra, "Lightweight and efficient PRIVACY-PRESERVING mutual authentication scheme to secure INTERNET OF THINGS -based smart healthcare," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 11, p. e4716, Nov. 2023, doi: 10.1002/ett.4716.
[30] W. Stallings, *Cryptography and network security: principles and practice*, 4th ed. Upper Saddle River, N.J: Pearson/Prentice Hall, 2006.
[31] B. Alotaibi and M. Alotaibi, "Hybrid Deep Learning Framework for Continuous User Authentication Based on Smartphone Sensors," *Sensors*, vol. 25, no. 9, p. 2817, Apr. 2025, doi: 10.3390/s25092817.

BIOGRAPHIES OF AUTHORS

Fatima.G.Abdullah received the B.Sc. degree in Computer Engineering from the Iraqia University, Baghdad, Iraq, in 2017. Since 2017, she has been working with the Laboratories Division, College of Engineering, Iraqia University. She has also gained professional experience through temporary appointments at Al-Mustansiriyah University and Basra University for Oil and Gas, serving within the University Presidency. She is currently affiliated with the Laboratories Division, College of Engineering, Iraqi University. Her academic and professional interests include computer engineering, cybersecurity, and advanced computing technologies.
Email: fatimah.g@aliraqia.edu.iq

Tayseer S. Atia is a professor at the department of computer engineering, Al-Iraqia
University, Iraq, where she has been a faculty member since 2012. From 2013-2014 she
was the head of the computer engineering department. From 2014-2015 she was the dean's
assistant for scientific affairs. Tayseer graduated with a first-class B.Sc. degree in
computer science in 2004 and a M.Sc. in data security in 2007 from the University of
Technology, Iraq. She completed her Ph.D. in computer science from Al Mosul University, Iraq. Her research interests are data security and artificial intelligence,
especially computational intelligence techniques. She can be contacted
Email:tayseer.salman@aliraqia.edu.iq