International Journal of Information Security (2024) 23:51–80
https://doi.org/10.1007/s10207-023-00748-1

SPECIAL ISSUE PAPER

A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs)

Osama Bassam J. Rabie[1,2] · Shitharth Selvarajan[3,4] · Tawfiq Hasanin[1] · Gouse Baig Mohammed[5] · Abddulrhman M. Alshareef[1] · Mueen Uddin[6]

Accepted: 10 August 2023 / Published online: 20 November 2023

Abstract

The dynamic connectivity and functionality of sensors has revolutionized remote monitoring applications thanks to the combination of IoT and wireless sensor networks (WSNs). Wearable wireless medical sensor nodes allow continuous monitoring by amassing physiological data, which is very useful in healthcare applications. These text data are then sent to doctors via IoT devices so they can make an accurate diagnosis as soon as possible. However, the transmission of medical text data is extremely vulnerable to security and privacy assaults due to the open nature of the underlying communication medium. Therefore, a certificate-less aggregation-based signature system has been proposed as a solution to the issue by using elliptic curve public key cryptography (ECC) which allows for a highly effective technique. The cost of computing has been reduced by 93% due to the incorporation of aggregation technology. The communication cost is 400 bits which is a significant reduction when compared with its counterparts. The results of the security analysis show that the scheme is robust against forging, tampering, and man-in-the-middle attacks. The primary innovation is that the time required for signature verification can be reduced by using point addition and aggregation. In addition, it does away with the reliance on a centralized medical server in order to do verification. By taking a distributed approach, it is able to fully preserve user privacy, proving its superiority.

Keywords Healthcare-based wearable wireless medical sensor nodes (HWMSNs) · Certificate-less aggregate signature (CLAS) · Full privacy preservation · Distributed batch authentication · Elliptic curve discrete logarithm problem (ECDLP)

1 Introduction

Internet of Things (IoT) has revolutionized the technology by connecting physical objects (either virtually or directly) which made communications to happen in a smarter way [1]. The most aspect of this invention is to provide access capabilities remotely in ad hoc manner via the Internet. This has revolutionized the remote monitoring applications to be accessible in real time. The core component of the IoT architecture is the wireless sensor networks [2]. Internet of Things has gained a lot of attraction among researchers since the past decade. Remote monitoring and constant care can be made feasible under critical and unfavorable conditions with the help of wireless sensors with Internet connectivity [3]. The combination of medicine and wireless sensor devices connected via Internet of Things has made a new form of technology called healthcare wearable wireless medical sensor networks (HWMSNs). Internet of Things plays a very vital role in case of remote monitoring via wireless

✉ Shitharth Selvarajan
s.selvarajan@leedsbeckett.ac.uk

Osama Bassam J. Rabie
Obrabie@kau.edu.sa

[1] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

[2] Cybersecurity Center, King Abdulaziz University, Jeddah, Saudi Arabia

[3] Department of Computer Science, Kebri Dehar University, Kebri Dehar, Ethiopia

[4] School of Built Environment, Engineering and Computing, Leeds Beckett University, Leeds LS1 3HE, UK

[5] Department of Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India

[6] College of Computing and Information Technology, University of Doha for Science and Technology, 24449 Doha, Qatar

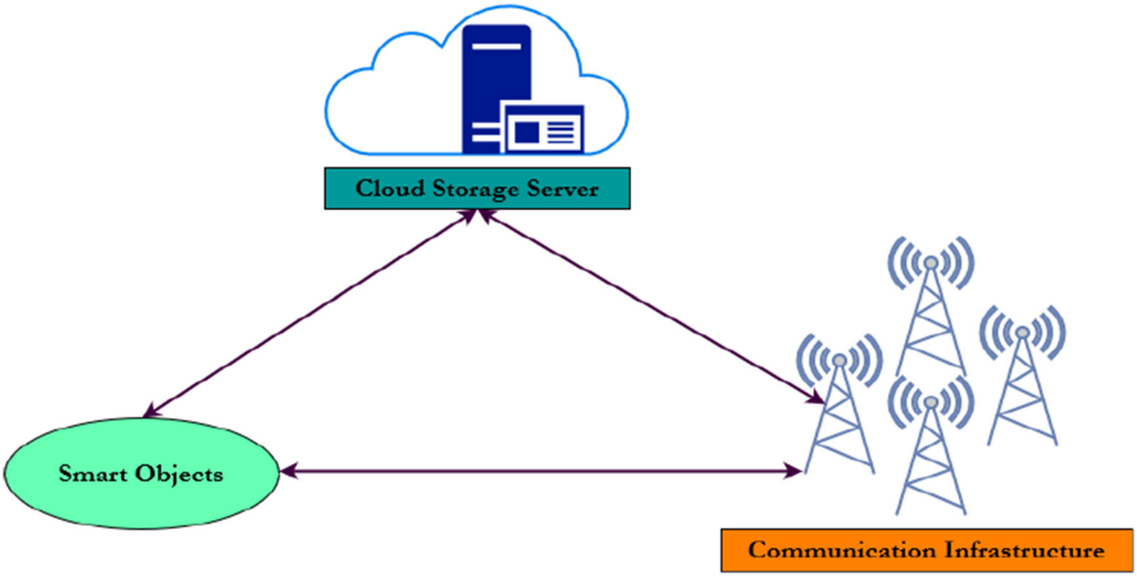

Fig. 1 Basic IoT components in HWMSN

sensor networks in case of medical industry. This invention has improved the medicare facilities to be available 24/7 via various applications relating to patient monitoring, drug management, diagnosis, tracking, etc. Medical professionals, experts and patients are quite often benefitted with even in the physical absence of a patient. IEEE 802.11 (WiFi) and other communication technologies have made possible this connectivity. Because of these capabilities, this technology enables wireless way of tracking, assorting and examining the medical data [4]. IoT consists of a wide variety of structural components broadly categorized into (1) smart objects, (2) storage servers and (3) communication infrastructure [5]. Figure 1 provides a clear cut view of the components of IoT in healthcare-based wearable wireless medical sensor network. The term wireless medical sensor networks (WMSNs) has been framed by the researchers corresponding to engineering, medicine and biotechnology disciplines. Therefore, wireless medical sensor networks consist of a collection of medical sensor nodes (MSNs) which are implanted on the body of a patient that provides constant tracking and accumulation of physiological information (text data) regarding the well-being of the patient health. These text data will be sent to the certified medical experts for further diagnosis [6]. IoT provided an advantage by making the sensors available on the physical devices as wearable sensors which are cheap and cozy. These devices monitor various medical information such as oxygen level (SPO_2), heart rate, blood glucose level, blood pressure rate, levels of pH, etc. A typical healthcare-based wearable wireless medical sensor network consists of the various components, viz. medical sensor networks, zonal node, local medical sensor, central medical sensor, patient, certified medical expert or professional, and Internet connectivity [7]. Medical sensor nodes are usually implanted on the body of the patient which was connected via wireless fidelity (WiFi) Internet connectivity. The medical text data collected get transmitted through the zonal node to a local medical server, and after getting the text data authenticated it will be sent to a central medical server for storage and research analysis insights.

After getting authenticated, the text data will be sent to the certified medical professional for remote diagnosis. Since the medical text data get transmitted via a wide open communication channel, they are highly subjected to security and privacy attacks [11]. Hence, it is much important to ensure the legitimacy and the legality of the transmitted physiological information in case of healthcare-based wearable wireless medical sensor networks (HWMSNs) [8, 9]. If and when an attacker catches the medical information as a man-in-the-middle, it is possible to get modified, impersonated, and then it leads the medical professionals to erroneous diagnosis [10]. Hence medical text data needs to be secured prior to transmission.

Privacy is also an additional issue in case of healthcare wearable wireless medical sensor nodes since the information transmitted is highly personal [12, 13]. A patient's text datum is highly sensitive because any breach or tampering of data may result in faulty treatment with fatal or irrecoverable loss of patient's health or even life. Most often the privacy breaches are often caused by internal privileged abuse, counterfeit access/disclosure for money or other means, improper disposal of unnecessary but sensitive data, loss or theft or the involuntary sharing of data to an unauthorized organization. This often induces physical stress; patients will lose the trust and ultimately result in loss of reputation. Sometimes it may lead to financial threatening or life threatening moments too.

When the medical text data storage gets attacked, then it is impossible for the experts to provide timely solutions. This creates awful, critical or dangerous situations for patients. It is therefore highly essential to achieve data integrity, message authentication, confidentiality, anonymity, forward and backward secrecy, unlinkability and traceability while performing the data collection and transmission [14]. Since the IoT devices utilized are resource-constrained in nature by means of storage, communication and computation resources which is another important challenge. Due to these challenges, traditional cryptographic techniques such as RSA and AES are not conducive since they require high computational resources [15]. Authentication schemes proposed rely on loading the secret keys into the nodes suffers from key compromise attacks which may jeopardize the entire functioning of the network [16].

In order to ensure the security and privacy of the healthcare wearable wireless medical sensor networks, cryptographic methodologies have played a prominent role especially public key cryptography (PKC). Public key cryptography comes up with an exclusive solution termed as digital signatures (DS). A digital signature is a form of cryptography that can be used to ensure the confidentiality, integrity, and authenticity of a transaction [17]. Digital signatures ensure privacy, security, anonymity, confidentiality, message authentication and non-repudiation [18]. Several authentication schemes pertaining to public key cryptography [19, 20], identity-based public key cryptography (ID-PKC), certificate-less public key cryptography (CL-PKC) has been proposed. Public key cryptography produces digital signatures which are subjected to verification prior to transmission. This process of verification involves high computation and communication costs [21]. It also suffers from the overhead of storing and processing of digital certificates [22, 23]. Shamir et al. [24] proposed a solution to the disadvantage of certificate processing referred to as identity-based public key cryptography. However, this technique suffers from key escrow problem. In order to overcome this problem, Al-Riyami et al. [25] proposed a solution referred to as certificate-less cryptography. This technique eliminates both the disadvantages of processing a huge quantity of certificates and key escrow problem. In order to alleviate the computational overhead incurred during verification, Boneh et al. [26] came up with an aggregation technology that facilitates the grouping or batching the signature at a particular time or threshold where these collated signatures are processed in an instance of time, thereby diminishing the huge computation cost of the servers involved. Also when a part of the signature gets aggregated like secret key and not the random primes chosen, then it is called as partial aggregation. Authentication scheme proposed is not conducive for healthcare wearable wireless medical sensor networks. The schemes proposed utilized bilinear pairing technique which increases the computational overhead and are subject to various attacks. Hence the environment challenges the authentication scheme's permeability. This makes the traditional signature schemes are insufficient and inefficient toward healthcare-based wearable wireless medical sensor networks. During verification if the server gets loaded with huge request, then there might be a possibility of denial-of-service attack which increases the cost of verification soaring high. Hence in order to address this problem, an authentication scheme that addresses all the aforementioned challenges has to be designed in order to ensure the security goals of the network.

1.1 Motivation

In healthcare wearable wireless medical sensor networks, the medical sensors are implanted on the patient's body which constantly keeps track of various physiological parameters. The information has to be transmitted through a wide open wireless communication channel which are highly prone to compromise and threatening attacks. Certificate-less aggregate signature schemes proposed also suffers from problems such privacy preservation, security and traceability. Most of the schemes proposed utilize bilinear pairing and map-to-point hash functions which makes it inefficient since it incurs high computational cost. It is the fact that the one-point multiplication using bilinear pairing operation is 20 times slower to that of the elliptic curves [27, 28]. Map-to-point hash function requires high computation power and resources which have a negative impact on the computation, communication and verification costs [29]. The schemes also suffer from the central tendency problem which has to be addressed. Since the medical sensor nodes deals with highly sensitive medical information of the patients, increase in the signature length has a degrading effect during signature verification. The nodes utilized in the healthcare wearable wireless medical sensor network are resource-constrained in nature, and it is necessary to design an authentication scheme that utilizes minimized resource and resistant to various attacks. Thus there is a need to design a full privacy-preserving distributed batch-based aggregate signature authentication scheme that provides efficient authentication, thereby dwindling the computation, communication and verification delays associated during the transmission of text data.

1.2 Major contributions

This work pinnacles the design of a certificate-less signature aggregation scheme to ensure full privacy for healthcare-based wearable wireless medical sensor networks. The major contributions of the proposed work are as follows:

- The proposed authentication scheme employs elliptic curve-based public key cryptography to ensure security

and privacy in a distributed manner for the transmission of medicare text data.
- The proposed data authentication scheme has not used expensive operations like bilinear pairing and map-to-point hash functions which promotes the efficacy of the developed scheme. Instead it used point addition, XOR operation and one-way generic hash functions which alleviate the computational burden incurred during signature verification.
- The scheme employs protection to both the random part and the secret key part of the authenticated cipher text data, thereby achieving full privacy preservation.
- Since the distributed key generation methodology and aggregation technique has been adopted, therefore it alleviates the central tendency over medical servers to perform signature verification. This reduces the computation and communication costs incurred during the signature verification.
- The proposed scheme is resistant to existential signature forgery attacks, man-in-the-middle attacks and other attacks which are proved under the elliptic curve discrete logarithm problem (ECDLP) by means of formal and informal security analysis.

Further the proposed scheme has been compared with the other existing schemes and achieves message authentication, integrity, traceability, anonymity, thereby making it conducive for vehicular communications.

1.2.1 Organization of the paper

The structure of the proposed work has been organized as follows: Sect. 1 defines the introduction. Section 2 elaborates on the related existing data authentication schemes. Section 3 presents the background, including elliptic curve cryptography, adversarial assumption, security model, and system model and design goals. Section 4 details the proposed data authentication scheme. Section 5 presents the formal and the informal security analysis. Section 6 provides the performance analysis of the proposed scheme; finally, Sect. 7 concludes the paper. Table 1 gives list the list of abbreviations used in the proposed scheme.

Table 1 List of abbreviations

Acronym	Description
HWMSN	Healthcare wearable wireless medical sensor network
IoT	Internet of Things
WSN	Wireless sensor network
VANET	Vehicular ad hoc network
ECC	Elliptic curve cryptography
IoV	Internet of vehicle
IEEE	Institute of Electrical and Electronic Engineers
Wi-Fi	Wireless fidelity
WMSN	Wireless medical sensor network
MSN	Medical sensor nodes
SPO_2	Serum Pressure and Oxygen
pH	Potential of hydrogen
PKC	Public key cryptography
RSA	Rivest-Shamir-Adleman
AES	Advanced Encryption Standard
DS	Digital signatures
ID-PKC	Identity-based public key cryptography
CL-PKC	Certificate-less public key cryptography
ECDLP	Elliptic curve discrete logarithm problem
ECDHP	Elliptic curve computational Diffie-Hellman problem
LMS	Local medical server
CMS	Central medical server
ZN	Zonal node
WeMSN	Wearable medical sensor node
CME	Certified medical expert
WBAN	Wireless body area networks
HP	Hard problem
NS	Network Simulator
LTS	Long-term support
RAM	Random access memory
PDR	Packet delivery ratio

2 Related work

Healthcare wearable wireless medical sensor networks (HWMSNs) have attracted a lot of academicians and scientists across the globe. Several contributions have been made in designing an efficient data authentication to cater the needs pertaining to HWMSNs. This section provides a detailed analysis on various works proposed by different researchers.

Castro et al. [30] came up with a first certificate-less aggregate signature data authentication scheme. However, these schemes are inefficient toward security attacks. Most of these schemes have designed based on expensive operations like bilinear pairing and map-to-point hash functions. However, certificate-less aggregate signature schemes are unsusceptible to adopt the highly resource-constrained sensors utilized in wearable wireless medical sensor networks. Vallant et al. [31] came up with a pseudo-identity-based elliptic curve certificate-less cryptography solution which achieved message authentication, anonymity, conditional traceability and revocability. However, the scheme has to be free from the revocation burden on the tracing authority. Shen et al. [32, 33] have developed an authentication scheme for HWMSNs based on the public key infrastructure. The proposed work was based on bilinear pairings and Diffie Hellman assumption. However, it becomes inefficient in handling the wireless traffic during the process of signature verification. Kumar et al. [34] came up with a data authentication scheme designed specifically for HWMSNs. This work involves expensive bilinear pairing operation which is a disadvantage in case of high density of signatures to be verified. Also the energy consumption rate is high that are yet to be addressed. Wu et al. [35] found that the work proposed by [34] is inefficient toward type II attack and proposed an improvement to that scheme. Though the work seems to be effective, it is inefficient since it uses expensive bilinear pairing operations. Also the work suffers from high computation and communication cost that are supposed to be addressed. Liu et al. [36] came up with a batch-based anonymous authentication scheme for m-healthcare crowd sensing applications. Though it concurrently provides anonymity for medical data, it involves huge computation cost since it involves expensive operations like bilinear pairing and map-to-point hash functions. Zhang et al. [37] found that the work proposed by [34] is inefficient and the signature can be forged easily. However, the scheme suffers from high computation cost due to bilinear pairing operation. Xie et al. [38] came up with the solution to the issue faced by [34] and provided a solution for it. Though the proposed work utilizes elliptic curves, it still suffers from the computation cost especially while performing aggregate verification which is not an advantage. Gayathri [39] came up with a certificate-less signature authentication scheme to address the problem of security. However, the verification of signatures and the generation of private keys for the sensor nodes are done solely by the medical server itself. Hence there occurs the problem of central tendency. Also the scheme suffers from a serious design issue that it is not possible for any sensor to pick a random prime to generate a secret key for itself. An external entity prior to deployment has to perform the operation. This poses a serious threat that if any of these sensor nodes are captured, it may lead to adverse situations. Kumar et al. [40] proposed a overview on the certificate-less signatures and certificate-less aggregate signature schemes. The scheme proposed utilized bilinear pairing operation and achieves revocability and traceability. The main drawback is that the scheme suffers from bandwidth consumption.

Zhong et al. [41] proposed a full privacy preservation authentication scheme with full aggregation in VANETs. The scheme utilized pseudonym-based elliptic curve cryptography for achieving security and privacy. Though the scheme achieves efficiency in addressing the bandwidth, computation and storage resources, it still faces problems due to pseudonym management during revocation. Since bilinear pairing operation is used the length of the time incurred to verify also incurs time. Kamil et al. [42] proposed a full privacy preservation authentication schemes that achieves full aggregation. The scheme utilized outproved Zhong et al. [41]'s scheme and is inefficient toward type II attacks. The author proposed a new scheme that proves an improvement over the scheme. The scheme suffers from communication overhead. Kamil et al. [43] came up with an improved certificate-less aggregate signature scheme without bilinear pairing operation. Their scheme utilized elliptic curve cryptography and achieved batch authentication, autonomy and conditional privacy preservation. Their scheme suffers from communication overhead which is a drawback. Zhao et al. [44] came up with a certificate-less aggregate signature scheme for Internet of vehicles. Though the scheme utilizes elliptic curve cryptographic technique, it suffers from the problem of handling pseudonyms. Mei et al. [45] proposed a certificate-less aggregate signature scheme that achieves conditional privacy for Internet of vehicles environment. The scheme utilized bilinear pairing and pseudonyms to achieve conditional traceability. The computation cost is high since it involves four pairing operation. Their scheme is unsuitable for dense scenarios. Xu et al. [46] proposed a certificate-less aggregate signature scheme for vehicular ad hoc networks. Their proposed scheme suffers from high computation and verification costs. Shuai et al. [47] addressed the problem of desynchronization attacks in WBANs by developing a lightweight privacy-preserving data authentication scheme using XoR operation and one way hash functions. The proposed scheme achieves mutual authentication and is resistant toward smart card loss attack, replay attack, privileged insider attack, password guessing attacks. However, the scheme suffers from the problem of communication overhead which increases with the increases in the number of vehicles and signatures. Zhang et al. [48] proposed a lightweight and secure anonymous user authentication protocol for wireless body area networks. The scheme utilized elliptic curve cryptography. Their scheme achieved mutual authentication, data integrity, confidentiality, identity privacy preservation and conditional traceability. However, their scheme suffers from communication overhead which is a major drawback. Ryu et al. [49] have come up with a privacy preservation authentication protocol for wireless body area networks in healthcare applications. Their scheme utilized XoR operations and one-way hash functions which makes it lightweight than the traditional asymmetric cryptographic operations. However, the scheme suffers from communication overhead which is a major drawback. Jegadheesan et al. [50] proposed an efficient privacy-preserving anonymous mutual authentication scheme for wireless body area networks. The scheme utilized bilinear pairing cryptography. The scheme achieves resiliency against bogus message attacks. Their scheme lags in the cost for communication which is a major disadvantage.

Table 2 Drawbacks of various existing authentication schemes

References	Cryptography technique	Authentication method	Benefits	Drawbacks
Shen et al. [32]	Bilinear pairing	Identity-based	Their proposed scheme has been resilient to coalition attacks	Use of bilinear pairing technique increases the computation overhead during verification
Shen et al. [33]	Bilinear pairing	Identity-based	Their scheme achieves integrity, reduce bandwidth consumption and storage in WSNs	Pairing operations results in the increase in the computation overhead
Kumar et al. [34]	Bilinear pairing	Identity-based	Their proposed scheme is resilient against existential forgery on adaptive chosen message and identity attacks	Computation and communication cost has to be reduced due to the use of bilinear pairing
Wu et al. [35]	Bilinear pairing	Identity-based	Their scheme found that the work of Kumar et al. [34] is inefficient against type II attack	Aggregation verification cost is more high than their chosen benchmark scheme
Liu et al. [36]	Bilinear pairing	Identity-based	Their scheme can be able to perform large-scale concurrent data anonymous batch verification for mobile healthcare crowd sensing systems	The scheme is vulnerable to coalition and impersonation attacks
Zhang et al. [37]	Bilinear Pairing	Identity-based	Their scheme can be able to achieve batch authentication, non-repudiation and anonymity. Their scheme out proved that Liu et al. [36]'s scheme is inefficient and are prone to various attacks	Still the improved scheme faces forgery and non-repudiation attacks
Xie et al. [38]	ECC	Certificate-less	Their scheme is resilient to forgery, identity tracing and other security attacks	Computation cost can be reduced further
Gayathri et al. [39]	ECC	Certificate-less	Their scheme provides message authentication, integrity, anonymity, conditional traceability, and revocation	Does not support autonomy and cannot achieve location privacy Also, it cannot resist DoS attack
Kumar et al. [40]	Bilinear pairing	Pseudonym-based	The scheme is secure and does partial aggregation which provides conditional privacy preservation in an effective manner	Computation cost can be reduced further
Zhong et al. [41]	Bilinear pairing	Pseudonym-based	Conditional privacy is achieved	Computation cost can be reduced further
Alhalabi et al. [42]	Bilinear pairing	Pseudonym-based	Their scheme achieves full aggregation and hence privacy preservation is achieved	Computation cost can be reduced further
Kamil et al. [43]	ECC	Identity-based	Their proposed scheme is pairing free and achieves full privacy preservation due to full aggregation	However the scheme is insecure since it is peril to denial-of-service attacks
Zhao et al. [44]	ECC	Pseudonym-based	Their proposed scheme is pairing-free and achieves only partial aggregation	Their proposed scheme is insecure toward side channel and password guessing attacks
Mei et al. [45]	Bilinear pairing	Pseudonym-based	The proposed scheme achieves full aggregation and is secure	The scheme is unsuitable for dense scenarios
Xu et al. [46]	Bilinear pairing	Identity-based	The proposed scheme achieves partial aggregation and is secure	The scheme utilized bilinear pairing method which increases the computation and communication cost

Table 2 (continued)

References	Cryptography technique	Authentication method	Benefits	Drawbacks
Shuai et al. [47]	XOR operation and one-way hash function	Identity-based	Their proposed scheme is resilient toward de-synchronization attacks, forward and backward secrecy in WBANs	The computation cost has to be reduced further
Zhang et al. [48]	ECC	Identity-based	Their scheme is resilient toward replay, insider, impersonation, stolen smart card attacks	The scheme suffers from communication overhead
Ryu et al. [49]	XOR operation and one-way hash function	Identity-based	Their proposed scheme is resilient toward impersonation, password guessing, stolen-verifier table, denial-of-service, identity attacks	The communication cost increases with increase in the number of messages
Jegadheesan et al. [50]	Bilinear pairing	Identity-based	Their scheme achieves anonymous authentication and resistant against bogus message attacks	The communication cost has to be reduced due to the increase in the number of nodes
Shuai et al. [51]	ECC	Identity-based	Their scheme achieves mutual authentication and are resilient toward replay, impersonation and man-in-the-middle attacks	Their scheme suffers from high computation cost which has to be reduced
Shitharth et al. [52]	XOR operation and one-way hash function	Identity-based	Resilient to password guessing attacks, replay, Desynchronization attacks, impersonation, insider modification, smart card stolen attacks, and man-in-the-middle attacks	The communication overhead is high and increases with the increase in the number of nodes in the network
Ji et al. [53]	ECC	Certificate-less	Their scheme achieves batch authentication of multiple clients simultaneously	Signature length increases with increase in the number of nodes
Mandal et al. [54]	ECC	Certificate-less	The proposed scheme achieves anonymity, resistance to key escrow problems, mutual authentication between the sensor nodes attached to patients and the application provider	The proposed scheme has to be tested for big data-based applications in healthcare environments
Chennam et al. [11]	ECC	Certificate-less	Their scheme achieves authentication, efficiency, and confidentiality	However the computation cost is high which increases with the increase in the number of nodes
Chakravorthy et al. [55]	ECC	Ciphertext-policy attribute-based encryption	Their proposed scheme is lightweight in nature and achieves user/attribute revocation	The proposed scheme has to be tested for large scale environments
Nyangaresi et al. [11]	XOR and one-way hash functions	Identity-based	It is also resilient and robust toward e-synchronization, packet replays, man-in-the-middle, privileged insider, impersonation, online and offline password guessing attacks	Their scheme has to be tested for large-scale environments in order to test whether it can achieve the same level of security with less message exchanges

Table 2 (continued)

References	Cryptography technique	Authentication method	Benefits	Drawbacks
Wu et al. [57]	XOR and one-way hash functions	Identity-based	Their proposed scheme achieves mutual authentication and are resilient to insider, offline password guessing, user forgery, sensor capture, gateway forgery, tracking, Desynchronization, attacks	The proposed scheme has to be tested for large scale environments
Jahan et al. [58]	XOR and one-way hash functions	Identity-based	Their scheme covers intra-BAN, inter-BAN, and beyond-BAN transmission in a setting where the patient's mobile phone is semi-trusted	The proposed scheme suffers from high bandwidth consumptions
Iqbal et al. [60]	Homomorphic encryption	Trapdoor based	Achieved desirable security goals and it distinguishes various trapdoors or possibility of leakage profiling	Their proposed scheme increases the computation time which is increased by the increase in the security levels and has to be tested for real-time environments
Almuhaideb et al. [61]	XOR, one-way hash functions	Identity-based	Their scheme is computationally efficient since it uses only hash and XOR functions	Their proposed scheme has to be tested in terms of scalability in real-time environments
Almuhaideb et al. [62]	ECC, XOR and one-way hash functions	Identity-based	Their schemes achieves secrecy, anonymity, revocation, session key disclosure, off-line guessing, impersonation, Stolen controller node Desynchronization attacks	Their scheme incurs computation overhead due to the increase in the length of the signature

Shuai et al. [51] up with a privacy-preserving authentication scheme for wireless body area networks. Their proposed scheme utilized elliptic curve cryptography. The proposed scheme achieves practicability and is suited for multi-server architecture without online third-party intervention. Their proposed scheme achieves forward secrecy, anonymity, untraceability and is resilient toward replay, impersonation and man-in-the-middle attacks. However, the computation cost is high and a drawback. Selvarajan et al. [52] proposed a lightweight group anonymous mutual authentication scheme for wireless body area networks in order to address the issue of forward secrecy in vehicular ad hoc networks. Their proposed authentication scheme utilized XoR operation and one-way hash function to achieve mutual authentication, user anonymity and forward secrecy. Their scheme is resilient toward password guessing attacks, Desynchronization attacks, impersonation, modification, replay, smart card stolen attacks, and insider and man-in-the-middle attacks. However, the scheme suffers from high communication overhead which increases with the increase in the number of nodes in the network. Ji et al. [53] proposed a certificate-less conditional privacy preservation authentication scheme for wireless body area networks. Their proposed scheme utilizes elliptic curve cryptography technique. Their scheme provides mutual authentication, forward secrecy, user anonymity and are resistant toward replay, impersonation, modification, main-in-the-middle, password guessing, insider and stolen smart card attacks. The major drawback is that the communication overhead increases with the increase in the number of nodes. Mandal et al. [54] have come up with a provably secure Certificate-less authentication protocol for wireless body area networks. Their scheme utilized elliptic curve cryptography technique. Their scheme can be able to achieve anonymity, mutual authentication and are resilient to key escrow problems, between the sensor nodes attached to patients and the application provider. Chennam et al. [11] have come up with a group authentication and key distribution mechanism for wireless body area networks. Their proposed scheme utilized elliptic curve cryptography technique. Their scheme achieves authentication, confidentiality and efficiency. However, the computation cost is high which increases with the increase in the number of nodes. Chakravorthy et al. [55] have come up with a ciphertext policy-based attribute encryption technique for wireless body area networks. Their proposed scheme is lightweight in nature and achieves user/attribute revocation. The proposed scheme has to be tested for large scale environments. Nyangaresi et al. [56] proposed a privacy-preserving three-factor authentication protocol for wireless body area network to address the problem of secure forwarding. Their proposed scheme biometric data, smart card and password with fuzzy extractor and one-way hash functions. Their proposed scheme has achieved mutual authentication, forward key secrecy, anonymity, key escrow problem and untraceability. It is also resilient and robust toward e-synchronization, packet replays, man-in-the-middle, privileged insider, impersonation, online and offline password guessing attacks. Their scheme has to be tested for large-scale environments in order to test whether it can achieve the same level of security with less message exchanges. Wu et al. [57] proposed an authentication scheme based on XOR and one-way Hash Functions which makes it lightweight. Their proposed scheme achieves mutual authentication and are resilient to insider, offline password guessing, user forgery, sensor capture, gateway forgery, tracking, de-synchronization attacks. However, the scheme has to be tested for large scale environments. Jahan et al. [58] proposed an end-to-end authentication mechanism for wireless body area networks. Their proposed scheme assumes that the patients' mobile phone is semi-trusted. Their scheme covers intra, inter and beyond body area network transmission. Their scheme is resilient toward masquerading, secret gateway guessing, replay, forward and backward secrecy attacks. However, their scheme has to be tested for big data or large-scale environments. Almuhaideb et al. [59] have come up with a survey on authentication in wireless body area networks. Their proposed work finds many research gaps such as scalability, lack in performance, storage and resource constrined nature. Iqbal et al. [60] have come up with a novel Homomorphic approach for preserving privacy of the patient data in Telemedicine. Their work proceeded by testing and by implementing audio datsets of varying sizes while varying the security parameters. Their proposed approach achieved high amount of security while processing mutiple levels of files. Almuhaideb et al. [61] proposed two secure and efficient WBAN authentication protocols between the sensors and a mobile device/controller. Their proposed work has segregated the scheme into two parts, namely authentication protocol-I for emergency medical reports and the authentication protocol-II for periodic medical reports. The scheme proved its correctness by using BAN logic and achieves mutual authentication, which resists passive and active attacks. However, their proposed protocol has not addressed the feature of scalability. Almuhaideb et al. [62] have come up with a work on inter-BAN authentication protocols for WBAN in a cloud-assisted environment. Their proposed work achieves authentication, forward/backward secrecy, password attacks, revocation, replay, session key disclosure offline-guessing, impersonation attacks, etc. However, their proposed work suffers from high computation cost and communication costs which are supposed to be reduced. Table 2 provides the comparative analysis of the various authentication schemes pertaining to wireless body area networks. From the literature survey, it has been identified that the existing authentication schemes are based on bilinear pairing operation which is a main drawback [32–37, 40–42, 45, 46]. It is true that one-point multiplication of a bilinear pairing operation is 20 times slower than that of the elliptic curve point multiplication operation [11]. Similarly, the exiting schemes utilized identity-based cryptography which suffers from key escrow problem.

Though some of the schemes utilize elliptic curve cryptography [11, 43, 44, 48, 51, 53, 55] which eliminates the central dependency of the medical server or the central server it is still difficult to achieve autonomy and distributed authentication. Few of the existing schemes [11, 47, 49, 52, 56–58] utilize lightweight XoR operations and one-way hash functions it still suffers from computation and communication overhead which decreases the efficiency of the network. In order to provide a trade-off between these requirements, it is essential to design a full privacy-preserving certificate-less aggregate signature-based authentication scheme for healthcare wearable wireless medical sensor networks.

3 Background

This chapter highlights the mathematical suppositions based on elliptic curves, background and the specifications related to healthcare wearable wireless medical sensor networks.

3.1 Elliptic curve cryptography

Public key cryptography has been the predominantly used cryptographic technique for encrypting data. In our proposed scheme, the elliptic curve cryptography has been chosen which plays an alternative role in providing high amount of security with smaller keys comparable to RSA. It works on the basis of developing security based on key pairs for public key encryption by utilizing the concept of elliptic curves. The definition of ECC defined by E as follows: $x^2 = y^3 + ay + b$ mod P over a finite field F_p, where a, b ε F_p. Since the chosen elliptic curve is a non-singular elliptic curve the prime value has been set as $p > 3$, by satisfying the condition $4a^2 + 27b^2 ! = 0$. It is obvious that the set of points (x, y) defined over a finite field forms a cyclic group and the point of Infinity O [27, 28].

3.2 Adversarial assumptions

Elliptic Curve Discrete Logarithm Problem (*ECDLP*): For any given α, $\beta \in F_p$, where $\beta = y\ \alpha$ where $y \in Z_q{}^*$ is a positive integer. It is intransigent to find y from β.

Elliptic Curve Computational Diffie–Hellman Problem (*ECDHP*): For any two abstract points αP, βP $\in F_p$, where $\alpha, \beta \in Z_q{}^*$ which are unknown. It is intransigent to compute the point $\alpha\ \beta\ P$ in G.

3.3 System model

A typical healthcare-based wireless medical sensor network architecture consists of four components, namely WeMSN (wearable medical sensor node), zonal node (ZN), central medical server (CMS), certified medical expert (CME). Figure 2 provides a depiction of the proposed architecture of a typical healthcare-based wearable wireless medical sensor network. Figure 3 provides the layered working model of the proposed methodology. The functionalities of these different entities are as follows: *1.* ***WeMSN:*** These are the wearable medical sensor nodes which are supposed to be installed on the body of the patients. These are nodes that pose smaller computation and storage capability. They are mainly responsible for collecting the medical data like blood pressure, oxygen level, and blood glucose levels via the zonal node (ZN). Before the deployment of the sensor node the certified medical expert professional performs the registration of each node by taking its unique identifier and encrypting it using a positive prime integer which acts as a secret key for each sensor node. This facilitates the security while collecting and transmitting messages to the zonal node. Wearable medical sensor nodes are connected to the zonal nodes with the help of wireless fidelity communication protocol (WiFi-IEEE 802.11) [63]. They cannot be trusted.

2. ZN: These are also the sensor nodes which possess high computation and storage capacity than the wearable medical sensor nodes. They are mainly responsible for aggregating the individual signatures from the wearable mobile sensor nodes by adding the signature of the zonal node and central medical server. By performing the Ex-OR operation, the secret keys are generated which eliminates the central tendency of the medical server. It is assumed that the wearable medical sensor nodes registered or encrypted by the zonal node has been utilized for a particular body of the patient. These nodes also register with the central medical server and receive its corresponding public parameters before initialization. They can be partially trusted.

3. Central medical server (CMS): Since it is a gross processing unit, it is capable of performing huge computation and storage capability of 46 TB oracle solid state drive [72]. It can be partially trusted and is responsible for generating the system parameters necessary for the functioning of the system.

4. Local medical server (LMS): Since this is a stand-alone gross processing unit, it is also capable of performing huge computation, storage and processing capabilities. The local server is partially trusted and registers itself with the central medical server during initialization. It is mainly responsible to perform signature verification during the transmission of text data. It performs verification after the signatures are aggregated via the zonal node.

5. Certified medical expert (CME) Professional: These are responsible for having a direct contact with the patient and the body of the patients. They are the doctors, nurses and the medicare professionals who receive data via the central medical server installed in a particular medicare unit. They are assumed to be partially or semi-trusted. Similarly the patients are partially trusted.

3.4 Threat model

The inferences to ensure security for healthcare-based wearable wireless medical sensor network have been made via [39]. Our proposed full privacy-preserving certificate-less aggregate signature data authentication scheme involves two types of attackers defined as *type I attacker ξ_1 and type II attacker ξ_2. Let $\xi_1$be the malicious user and ξ_2 be the malicious local medical server which generates the partial secret keys.*

Type I Adversary: *ξ_1 being the malicious user cannot poses access control to the central medical server where it is possible for him to take access to modify the public access privileges with any desirable quantity.*

Type II Adversary:*$\xi_2$be the malicious local medical server has access over the central medical server but cannot be able to modify the public keys of any sensor node.*

The security model has been chosen from [31] that act as a benchmark for our proposed data authentication scheme. The security model has been developed via the game over the challenger C and an attacker thereby performs malevolent behavior where ξ ε (ξ_1, ξ_2). An attacker can have complete access permission over the transmission channel where the other components can reply. No way direct communication is possible. An adversary can deploy replay, modification, alteration delaying, interleaving, and deletion of messages in the architecture.

4 Proposed authentication scheme

This section details the proposed methodology of a full privacy-preserving data authentication scheme and its security proofs via ECDLP supposition. The proposed full privacy-preserving data authentication scheme composed of eight different algorithms. Each of the algorithms will be executed by different components, namely *WeMSN (wearable medical sensor node), zonal node (ZN), central medical server (CMS), local medical server (LMS), certified medical expert (CME).* The proposed scheme consists of eight modules. Each module works based on algorithms, namely (1)*system initialization,* (2) *deployment,* (3) *distributed key generation,* (4) *signature generation*, (5) *aggregation, and* (6) *aggregation verification.* Figure 4 represents the working methodology of the proposed data authentication scheme.

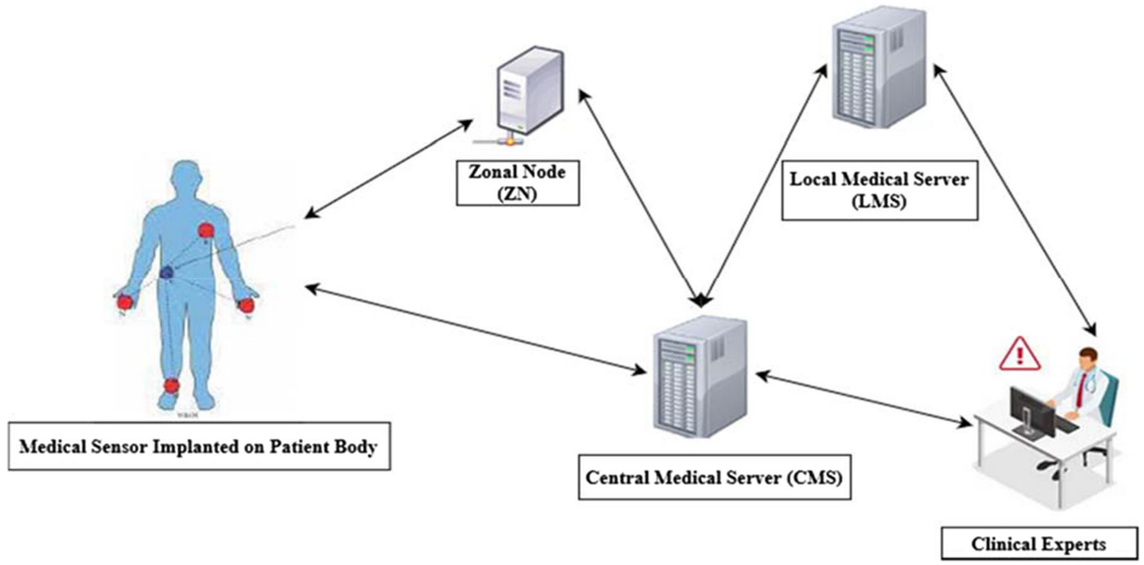
Zonal Node (ZN)
Local Medical Server (LMS)
Medical Sensor Implanted on Patient Body
Central Medical Server (CMS)
Clinical Experts

Fig. 2 Architecture of a healthcare-based wearable wireless medical sensor network

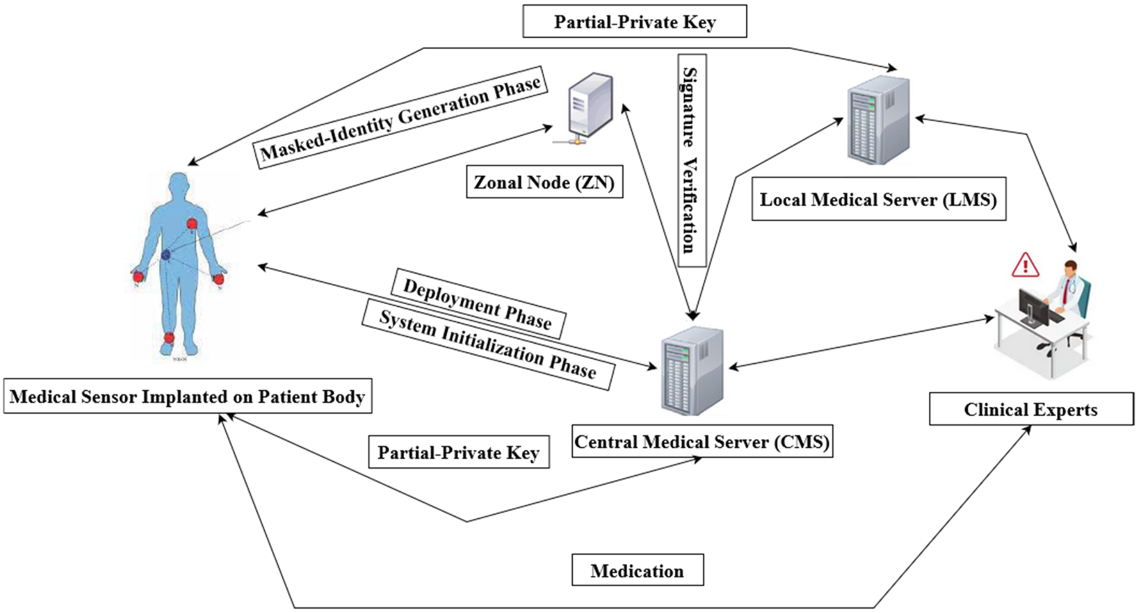
Partial-Private Key
Masked-Identity Generation Phase
Signature Verification
Zonal Node (ZN)
Local Medical Server (LMS)
Deployment Phase
System Initialization Phase
Medical Sensor Implanted on Patient Body
Central Medical Server (CMS)
Clinical Experts
Partial-Private Key
Medication

Fig. 3 Layered Working model of the proposed data authentication scheme

The notations utilized for the design of the proposed data authentication scheme are elaborated in Table 3.

4.1 System initialization

In this phase, the central medical server (CMS), local medical server (LMS), and zonal node provide the certificate parameters which are responsible for the system to perform its functionality. Algorithm 1 provides the steps supposed to be ensued.

5 Algorithm 1: System Initialization

Input: Variables for security, Prime Integers

Output: Creation of Public Variables

Step 1: Let μ be the security parameter; the central medical server (CMS) selects two large primes r and s where the elliptic curve has been defined by the equation

$$x^2 = y^3 + ay + b \mod P; \quad \forall a, \ b \varepsilon F_p \tag{1}$$

Step 2: The central medical server selects a random integer $\psi \ \varepsilon \ Z_q{}^*$ as a master private/secret key

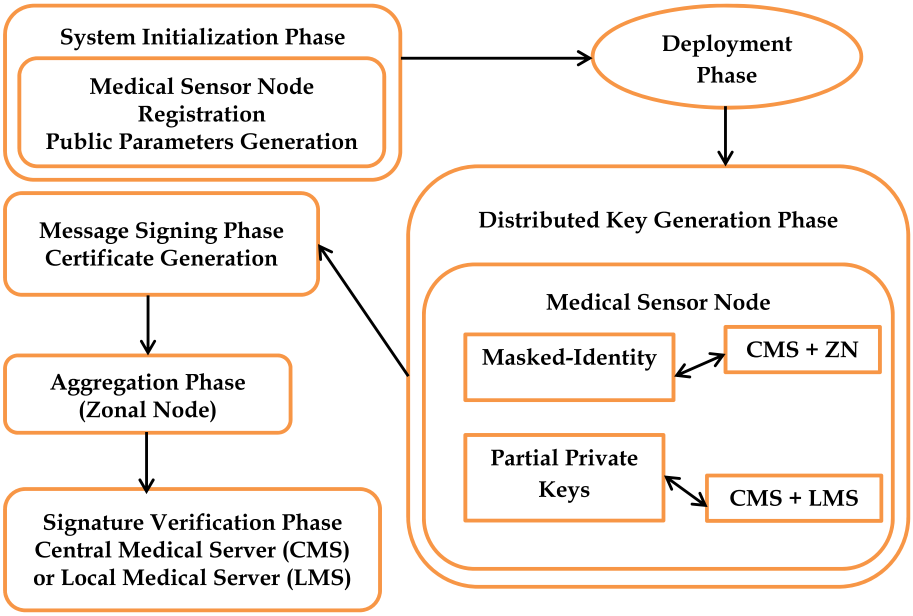
System Initialization Phase
Medical Sensor Node Registration
Public Parameters Generation
Deployment Phase
Distributed Key Generation Phase
Medical Sensor Node
Masked-Identity
CMS + ZN
Partial Private Keys
CMS + LMS
Message Signing Phase
Certificate Generation
Aggregation Phase
(Zonal Node)
Signature Verification Phase
Central Medical Server (CMS)
or Local Medical Server (LMS)

Fig. 4 Working methodology of the proposed data authentication scheme

Step 3: Computes $C_{\text{pub}} = \psi\ P$ as the system public key

Step 4: Central medical server creates the necessary public parameters as CMS = $\{\psi, C_{\text{pub}}\}$

Step 5: Similarly the local medical creates its master private/secret key. It selects $\Omega\ \varepsilon\ \ Z_q{}^*$ as a secret key and computes $L_{\text{pub}} = \Omega P$ as its public key

Step 6: It produces the public parameters as LMS = $\{\Omega, L_{\text{pub}}\}$

Step 7: Zonal node first authenticates itself with the central medical server by selecting a random integer $\lambda\ \varepsilon\ Z_q{}^*$ as its secret key.

Step 8: Computes $T_{\text{pub}} = \lambda$ P as the public key

Step 9: Zonal node produces the system parameters as $ZN = \{\lambda,\ T_{\text{pub}}\}$

Step 10: The central medical server chooses one way hash functions as

$$h_0 : G \to Z_q^*;\ h_1 : \{0,\ 1\}^* \to Z_q^*;\ h_2 : \{0,\ 1\}^* \to Z_q^*;\ h_3 : \{0,\ 1\}^* \to Z_q^*$$

Step 11: The systems public parameters generated are given by Eq. (2) as follows:

$$\text{Params} = \{P,\ r,\ s,\ E,\ G,\ C_{\text{pub}},\ L_{\text{pub}},\ T_{\text{pub}},\ h_0,\ h_1,\ h_2,\ h_3\} \quad (2)$$

Step 12: Similarly the Clinical Medical Experts registers themselves with the central medical server which assigns a private key as a password combination of their name, mobile number and date-of-birth which makes it unique and are as follows:

$$\text{CE}_i \xrightarrow{\text{Name, Mob No, DoB}} \text{CMS}$$

$$\text{CMS} \xrightarrow{\text{Password}_i} \text{CE}_i$$

$$\text{CEPassword}_i = \{\text{CEP}_1, \text{CEP}_2, \ldots, \text{CEP}_n\}$$

Step 13: After generating the private key which is a password it then sends it to the local medical server as a copy in order to generate a One-time password to be sent for further verification which is generated randomly as a combination of letters and number making it as unique.

$$\text{CMS} \xrightarrow{\sum_{i=1}^{n} \text{CEPassword}_i} \text{LMS}$$

$$\text{LMS} \xrightarrow{\text{Fn(OTP)}} \{\text{OTP}_1, \text{OTP}_2, \ldots, \text{OTP}_n\}$$

$$\text{LMS} \xrightarrow{\text{OTP}_i} \text{CE}_i$$

Step 14: Similarly each patient/care taker will be granted a password and an OTP for authentication so that they can read/download the prescription by entering it.

5.1 Deployment phase

In this phase, before deployment each of the medical sensor nodes it will be installed with the corresponding masked identity so that the conditional privacy preservation can be achieved. When a conflict occurs, the local medical server can be able to revoke or identify the original identity of the medical sensor node. Algorithm 2 provides the procedure to be ensued for the deployment phase.

Algorithm 2: Deployment Phase

Input: Public and private identity of a medical sensor node

Table 3 Notations utilized in our scheme

Symbols params	Explanation parameters
E_q	Elliptic curve $x^3 + ay + b$ (mod$P$)
r, s	Prime numbers
F_p	Finite field of prime numbers
G	Cyclic group generated by a point P on a non-singular elliptic curve E
P $Z_q{}^*$	Generator of $E(F_q)$ Prime field of integers
$\{\psi, C_{\mathrm{pub}}\}$	Central medical server (CMS) public key and master key
$\{\Omega, L_{\mathrm{pub}}\}$	Local medical server (LMS) public and master key
$\{\lambda, Z_{\mathrm{pub}}\}$	Zonal node public and master key
h_0, h_1, h_2, h_3	One-way hash functions
$\mathrm{MSN}_i, \mathrm{MSN}_{\mathrm{ID}_I}$	ith medical sensor node; original identity of a medical sensor node
$\mathrm{QMSN}_{\mathrm{ID}_i}$ Q	Pseudo-identity of a medical sensor node i Public key of the medical sensor node
t_i	Timestamp
M_i	Message i
PPK_i PPK_j, PPK_k $\overline{\overline{Q_l}}$, $\overline{\overline{Q_m}}$	Partial private key i Partial private keys of CMS and LMS before appending Pseudo-identity of CMS and LMS before appending
$\overline{\overline{Q_i}}$	Pseudo identity after appending
SKMSN_i	Full private key of the Medical Sensor Node i
$\mathrm{SMSN}_{\mathrm{PPK}_i}$ ξ_1, ξ_2 δ $\mathcal{Z}_i$	Public key of the medical sensor node i Malevolent user, Malevolent LMS or CMS Secret key of the medical sensor node Message signature
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

Output: Masked identity

Step 1: Let the number of medical sensor nodes be defined as

$$\sum_{i=1}^{n} \mathrm{MSN}_i = \{\mathrm{MSN}_1, \mathrm{MSN}_2, \mathrm{MSN}_3, \ldots, \mathrm{MSN}_n\}$$

Step 2: The original identity of the medical sensor nodes are given by

$$\sum_{i=1}^{n} \mathrm{MSN}_{\mathrm{ID}_\mathrm{I}} = \left\{\mathrm{MSN}_{\mathrm{ID}_1}, \mathrm{MSN}_{\mathrm{ID}_2}, \ldots, \mathrm{MSN}_{\mathrm{ID}_n}\right\}$$

Step 3: The local medical Server chooses an abstract integer δ ε $Z_q{}^*$ for each medical sensor node and computes $Q_i = \delta\ P$ as the public key.

Step 4: The public and the private parameters for a particular medical sensor node can be given as $\left\{\mathrm{MSN}_{\mathrm{ID}_I},\ Q_i\right\}$.

Step 5: These parameters are then sent to the central medical server for the masked identity generation

Step 6: The central medical server after checking its original identity iff $\{\mathrm{MSN}_{\mathrm{ID}_\mathrm{I}},\ Q_i\}$ is true; then compute $\overline{Q}_i = \left\{\mathrm{MSN}_{\mathrm{ID}_I} \oplus h_0\left\{\psi\, Q_i||t_i||C_{\mathrm{pub}}\right\}\right\}$; t_i implies the validity period of the masked identity.

Step 7: Central Medical Server after generating the masked identity the deployment team performs the installation of the masked identity as follows

$$\mathrm{QMSN}_{\mathrm{ID}_\mathrm{I}} = \{Q_i||\overline{Q}_i||t_i\};\ \forall_i$$

Step 8: In case of any conflicts the local medical server computes the original identity of the medical sensor node given by Eq. (3). The central medical server after performing the masking it will send the data to the local medical server so that the revocation or tracing back happens.

$$\mathrm{MSN}_{\mathrm{ID}_I} = \left\{\overline{Q}_i \oplus h_0\left\{\psi||t_i||C_{\mathrm{pub}}\right\}\right\} \tag{3}$$

5.2 Distributed key generation phase

The private keys are generated by the zonal node and the local medical server simultaneously in a distributed fashion partially. They are appended together at the zonal node in a secured manner since it acts as an aggregator. The masked identity and the partial private keys for a corresponding medical sensor node is then installed on the corresponding node. Algorithm 3 provides the procedure to be ensued for the Distributed Key Generation Phase.

Algorithm 3.1: Partial private key generation

Input: Random number, masked identity of a medical sensor node

Output: Partial private Keys

Step 1: After receiving the masked identity from the central medical server, the local medical server selects a random number φ ε $Z_q{}^*$ and computes $\overline{\overline{Q_l}} = \varphi\ P$ as the public key of local medical server.

Step 2: The part of the partial private key $\mathrm{PPK}_j\,P\ = \varphi \oplus h_2\left\{\mathrm{QMSN}_{\mathrm{ID}_I}||\overline{\overline{Q_l}}\right\}L_{\mathrm{pub}};\quad \forall_j$.

Step 3: The local medical server then sends the masked identity and the partial private key to the zonal node deployment phase as $\left\{\overline{\overline{Q_l}},\ \mathrm{PPK}_j\right\}$.

Step 4: Similarly the central medical server after producing the masked identity it selects an abstract number γ ε

${Z_q}^*$ and computes $\overline{\overline{Q_m}} = \gamma\ P$ as the public key and produces the part of the partial private key as $\text{PPK}_k P = \gamma \oplus h_3 \left\{ QMSN_{ID_I} || \overline{\overline{Q_m}} \right\} C_{\text{pub}}; \quad \forall_k.$

Step 5: The central medical server then sends the masked identity and the partial private key to the zonal node deployment phase as $\left\{ \overline{\overline{Q_m}}, \text{PPK}_k \right\}$.

Step 6: The partial private keys produced are then sent to the aggregator and produces a single entity ensued by Eq. (4)

$$\text{PPK}_i = \text{PPK}_k + \text{PPK}_j\ \forall_j,\ \forall_k \varepsilon \forall_i \tag{4}$$

Step 7: Similarly the masked identities are aggregated together and stored as a single entity as ensued by Eq. (5)

$$\overline{\overline{Q_i}} = \overline{\overline{Q_l}} \oplus \overline{\overline{Q_m}}; \quad \forall_l, \forall_m \varepsilon \forall_i \tag{5}$$

Step 8: Each of the medical sensor node contains

$$\text{MS}_i \leftarrow \left\{ \overline{\overline{Q_i}}, \text{PPK}_i \right\} \tag{6}$$

Under this phase full privacy preservation has been ensured since it is impossible even if the attacker attempts to gain anyone of the partial private keys. Each medical sensor node takes it secret key which was already generated by the local medical sensor node $\delta\ \varepsilon\ {Z_q}^*$ and produces the public key.

Algorithm 3.2: Secret Key Generation

Input: Partial private keys and masked identity of a medical sensor node

Output: Secret key of a medical sensor node

Step 1: The public key of the sensor node is $\text{SMSN}_{\text{PPK}_i} = \delta_i P$ and sends it to the zonal node.

Step 2: The full private key of the medical sensor node

$$\text{SKMSN}_i = \{\delta_i, \text{PPK}_i\} \tag{7}$$

5.3 Signature Generation Phase

This algorithm ensures the authenticity and the integrity of the generated medical data generated from the sensor nodes. Each sensor nodes after sensing performs signing via the steps mentioned in Algorithm 4.

Algorithm 4: Message signature generation

Input*:* Masked identity, time stamp, secret keys and message

Output: Message signature

Step 1: In order to produce a message signature now the medical sensor node has the message $M_i \varepsilon \{0,1\}^*$, it uses its masked identity $\overline{\overline{Q_i}}$, the secret key SKMSN_i, the public parameters, timestamp t_i

Step 2: The sensor node contains secret keys which was installed selects an abstract number $\theta_i \varepsilon\ {Z_q}^*$ and computes $\text{Л}_i = \theta_i$ which further generates $X_i = h_4\{M_i // \text{QMSN}_{\text{ID}_I} // \bar{\bar{Q}}_i // \text{SMSN}_{\text{PPK}_i} // \text{Л}_i // t_i\}$

Step 3: Further to secure this, it performs $\overline{X_i} = h_4 \cdot \theta_i \oplus \text{SKMSN}_i \mod p$

Step 4: Therefore the message signature can be generated as

$$\text{Շ}_i = \{\text{Л}_i, \bar{X}_\iota\} \tag{8}$$

where τ_i is the generated message signature

Step 5: The generated message signature is then sent to the aggregator (zonal node) for aggregation in batch-wise fashion.

5.4 Aggregation phase

The aggregation is carried out by the zonal node which was proposed by Boneh et al. [3]. This helps us to diminish the computation and the communication cost involved. Batch aggregation has been performed. Each zonal node performs the process of aggregation and outputs the aggregated signature to the local medical server for verification process which then sends the messages to the clinical experts for further diagnosis or treatment and a copy of it is encrypted and uploaded to the central medical server. The steps involved in Algorithm 5 are as follows:

Algorithm 5: Aggregation

Input: Message Signatures Շ_i

Output: Aggregated Signature Շ_i

Step 1: The aggregation has been performed as ensued which consists of medical sensor nodes $\{\text{MSN}_1, \text{MSN}_2, \text{MSN}_3, \ldots, \text{MSN}_n\}$ along with their masked identities $\left\{\text{QMSN}_{\text{ID}_1}, \text{QMSN}_{\text{ID}_2}, \ldots, \text{QMSN}_{\text{ID}_n}\right\}$ and the public keys $\{\text{SMSN}_{\text{PPK}_1}, \text{SMSN}_{\text{PPK}_2}, \ldots, \text{SMSN}_{\text{PPK}_n}\}$ and the message signature pairs as $\{M_i, t_i, \text{Շ}_i\}$:$\{\{M_1, t_1, \text{Շ}_1\}, \{\text{M}_2, \text{t}_2, \text{Շ}_2\}, \ldots\ldots., \{M_n, t_n, \text{Շ}_n\}$.

Step 2: The zonal node computes

$$\sum_{i=1}^{n} \overline{X_i}$$

Step 3: Finally, the aggregator after performing aggregation outputs the certificate-less signature pairs given by Eq. (9) as

$$\text{Շ} = \{\{\text{Л}_1, \overline{X_1}\}, \{\text{Л}_2, \overline{X_1}\}, \ldots\ldots\ldots., \text{Л}_n, \overline{X_n}\}\} \text{--------}\mathit{(10)} \tag{9}$$

5.5 Aggregate Signature Verification

The generated aggregate message signature pairs are then checked for the timestamp, and if it is alive, then it is accepted for verification by the local medical server. Because once the timestamp gets expired, thereby may be a possibility of attacks. In order to avoid that the signature pair batches with expired timestamps are deleted. It is assumed that the revocation list of certificate signature pairs are stored and maintained at the each corresponding entities of healthcare-based wearable wireless medical sensor networks. The steps involved in the verification process are given in Algorithm 6.

Algorithm 6: Aggregate signature verification

Input: Aggregate signature pairs

Output: Accept or Reject

Step 1: Iff (timestamps of both masked identity ≤ the sensor node) then

$$\begin{aligned}
&\text{Compute } \overset{\equiv}{\mathrm{F}}_i = h_3\ \{\mathrm{QMSN}_{\mathrm{ID}_I} || \overset{\equiv}{Q}_i\} \\
&\text{Compute } F_i = h_4\{M_i || \mathrm{QMSN}_{\mathrm{ID}_I} || \overset{\equiv}{Q}_i || \mathrm{SMSN}_{\mathrm{PPK}_i}\ || \text{ЛJ}_i || t_i\}; \quad \forall_i \\
&\text{Validate } \bar{X}_\iota \cdot P = F_i\ \text{ЛJ}_i \oplus \mathrm{SMSN}_{\mathrm{PPK}_i} \\
&\qquad\qquad \oplus\ \mathrm{QMSN}_{\mathrm{ID}_I} \oplus \overset{\equiv}{F}_i .\ C_{\mathrm{pub}}
\end{aligned} \tag{10}$$

Step 2: Each local medical server performs the verification via

$$\begin{aligned}
\bar{X}\ P = &\ \textstyle\sum_{i=1}^{n} F_i\ \text{ЛJ}_i + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} \\
&+ \textstyle\sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_I} + \sum_{i=1}^{n} \overset{\equiv}{F}_i\ C_{\mathrm{pub}}
\end{aligned} \tag{11}$$

Step 3: Compute the batch of the signature pairs as follows:

$$\begin{aligned}
\bar{X}\ P = &\textstyle\sum_{i=1}^{n} F_i\ \text{ЛJ}_i + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} \\
&+ \textstyle\sum_{i=1}^{n} \{\mathrm{QMSN}_{\mathrm{ID}_j} \oplus \mathrm{QMSN}_{\mathrm{ID}_k}\} + \sum_{i=1}^{n} \overset{\equiv}{F}_i\ C_{\mathrm{pub}} \\
= &\textstyle\sum_{i=1}^{n} F_i\ \text{ЛJ}_i + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} \\
&+ \textstyle\sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_j} \oplus \sum_{i=1}^{n} \mathrm{QMSN}_{ID_k} + \sum_{i=1}^{n} \overset{\equiv}{F}_i\ T_{\mathrm{pub}}
\end{aligned} \tag{12}$$

Step 4: Proof of the Lemma has been as follows:

$$\begin{aligned}
\bar{X} \cdot P &= \sum_{i=1}^{n} \{F_i \theta_i + \mathrm{SKMSN}_i\} \cdot P \\
&= \sum_{i=1}^{n} F_i \theta_i P + \sum_{i=1}^{n} \mathrm{SKMSN}_i P \\
&= \sum_{i=1}^{n} F_i \theta_i P + \sum_{i=1}^{n} \{\delta_i \oplus \mathrm{PPK}_i\} P \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_i + \sum_{i=1}^{n} \delta_i P + \sum_{i=1}^{n} \mathrm{PPK}_i P \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_i + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} \\
&\quad + \sum_{i=1}^{n} \mathrm{PPK}_k P + \sum_{i=1}^{n} \mathrm{PPK}_j P \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_\mathrm{i} + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} + \sum_{i=1}^{n} \gamma \oplus h_3 \left\{\mathrm{QMSN}_{\mathrm{ID}_I} \parallel \overline{\overline{Q_m}}\right\} \\
&\quad + \sum_{i=1}^{n} \varphi \oplus h_2 \left\{\mathrm{QMSN}_{\mathrm{ID}_I} \parallel \overline{\overline{Q_l}}\right\} \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_\mathrm{i} + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} + \sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_l} \\
&\quad + \sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_m} + \sum_{i=1}^{n} \left\{h_2\left(\varphi \oplus \overline{\overline{Q_l}}\right)\right\} + \sum_{i=1}^{n} h_3\left(\gamma \oplus \overline{\overline{Q_m}}\right) \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_\mathrm{i} + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} + \sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_l} \\
&\quad + \sum_{i=1}^{n} \mathrm{QMSN}_{ID_m} + \sum_{i=1}^{n} \overline{\overline{Q_l}} + \sum_{i=1}^{n} \overline{\overline{Q_m}} \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_\mathrm{i} + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} \\
&\quad + \sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_l} + \sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_m} + \sum_{i=1}^{n} \overline{\overline{Q_i}} \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_\mathrm{i} + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} + \sum_{i=1}^{n} \mathrm{QMSN}_{\mathrm{ID}_i} + \sum_{i=1}^{n} \overline{\overline{Q_i}} \\
&= \sum_{i=1}^{n} F_i\ \text{ЛJ}_\mathrm{i} + \sum_{i=1}^{n} \mathrm{SMSN}_{\mathrm{PPK}_i} + \sum_{i=1}^{n} \overline{\overline{F_i}}\ C_{\mathrm{pub}}
\end{aligned} \tag{13}$$

5.5.1 Clinical expert and treatment

The clinical experts having access to the local medical server will access the local database based on the periodic and emergency reports received based on a batch-wise first-come-first-serve (FCFS) basis. Each clinical expert gets authorized by the central medical server and the local medical server and they will be given a security credential in the form of a OTP other than the private key. Even if any of the medical professional or the clinical expert tries to manipulate the private key, it is impossible to get access to the local medical database since they need the OTP. If the web page or the database remains inactive for more than two or three minutes, it will automatically lock along with the expiration of the session. If the clinical expert tries to issue a medication, then an additional OTP is required which has to match with the password and the session OTP. Hence even if an insider or the patient tries to manipulate, it is not possible. The steps involved in this process are as follows:

Algorithm 7: **Clinical Examination and Treatment**

Input: Credentials of the Clinical Expert (Private Key) & One-Time Password (OTP)

Output: Local Medical Database Accept or Reject

Step 1: Clinical Medical Expert first enters the password registered with the central medical server.

$$\mathrm{CE}_{\mathbf{i}} \xrightarrow{\mathrm{Password_i}} \mathrm{LMS}$$

Step 2: After the password gets authenticated the central medical server sends the same data to the local medical server which then generates an OTP which is unique to each clinical expert having access to the particular database of the patient.

$$\mathrm{LMS} \xrightarrow{\mathrm{Password_i}} \mathrm{CMS}$$

Step 3: The local medical server after checking the correctness of the entered password it generates a One-time Password and is sent to clinical expert for prescribing the medication with a time frame. If and when the OTP is not entered within the time frame it will expire and the process gets repeated again.

$$\mathrm{LMS} \xrightarrow{\mathrm{OTP_i}} \mathrm{CE}_{\mathbf{i}}||\Delta \mathrm{T}_{\mathbf{i}}$$

Step 4: Before prescribing the medication, the clinical expert checks the timestamp of the message signature of the batch and if it is alive or fresh, then he will decrypt it by using the private key assigned to him by the central medical server during registration.

$$\mathrm{CE_i} \xrightarrow{\mathrm{Decryption/Verification}} \Delta \mathrm{T_i} \times \mathrm{CE_{pvk}}$$

Step 5: After prescribing the medication in order to upload or to send the data to the patient, another OTP will be generated and is sent to the clinical expert mobile number.

$$\mathrm{CE_i} \xrightarrow{\mathrm{RequestOTP}} \mathrm{LMS}$$

$$\mathrm{LMS} \xrightarrow{\mathrm{OTP_i}} \mathrm{CE}_{\mathbf{i}}||\Delta \mathrm{T}_{\mathbf{i}}$$

Step 6: On the patient/Care-taker end, if he/she does not enter the required password and the OTP given during the time of registration in the hospital, it is impossible to receive or to read/ download the medication.

6 Security analysis

The section highlights the security analysis carried out for the proposed full privacy-preserving data authentication scheme. The validation has been performed via both the formal and informal security analysis. Security proofs are arrived for the proposed certificate-less aggregate signature scheme by utilizing two types of attacking assumptions ($A_1$and A_2). To demonstrate the efficiency in providing security and privacy aspects Random oracle Model is utilized.

Divarication Axiom [64]**:** Let ξ be a probabilistic polynomial time Turing machine whose input only consists of public data. It is denoted that U and ∩ the number of queries that A can ask to the random oracle and the number of queries that 𝕁 can ask to the signer. Assume that, within a time bound T, A produces, with probability $\mathcal{E} \geq 10\ (\mathrm{U}\ +\ 1)\ (\mathrm{U}\ +\ \cap)/2^k$, a valid signature $(\mathbb{J}_{1,}\overline{X_1}, \theta_1, \overline{X_2}\ )$. If the triples $(\overline{X_1},\ \theta_1,\ \overline{X_2})$ can be simulated without knowing the secret key, with an indistinguishable distribution probability, then there is another machine that has control over the machine obtained from 𝕁 replacing interaction with the signer by simulation and produces two valid signatures $(\mathbb{J}_{1,}\overline{X_1}, \theta_1, \overline{X_2}\ )$ and $(\mathbb{J}_{1,}\overline{X_1}, \acute{\theta}_1, \overline{\acute{X}_2}\ )$ such that $\theta ! = \theta\ \prime$ in the expected time $T' \geq 120{,}686\ \cap T/\ \mathcal{E}$..

6.1 Formal security analysis

Under the assumption of the security requirement, we strive to prove that the proposed scheme is efficient and secure against forgery of signatures upon adaptively chosen message attacks by utilizing the random oracle model. We then proceed to prove further our proposed scheme is secure.

Theorem 1 *The proposed certificate-less aggregate signature scheme is unforgeable upon adaptive chosen message under hard ECDLP supposition.*

Axiom 1 *Based on the random oracle model (ROR), an invader* ξ_1*at a probability-based polynomial time can forge a certificate-less aggregate signature by a security attack designed by Game I after making* U_{h_i}*queries to a* *random oracles where h_i $\forall i$ where $i = 1, 2, 3$.* $\mathrm{U}_{C_{\mathrm{rev}}}$*queries to the oracle for create-sensor node;*$\mathrm{U}_{\mathrm{PPK}_i}$*queries to the oracle of partial private key;*$\mathrm{U}_{\mathrm{SKMSN}_i}$*queries to the oracle of secret key;* $\mathrm{U}_{\mathrm{SIG}}$*queries to the oracle of signing. It the invader* ξ_1*can be able to forge a original signature in polynomial time, then there is a challenger* ß$_1$ *who solves ECDLP within time*$T < 120686$ ∩$T/$ $\mathcal{E}$,, iff $\mathcal{E} \geq 10$ $(\mathrm{U}_{\mathrm{SIG}} + 1)$ $(\mathrm{U}_{h_1} + \mathrm{U}_{h_2} + \mathrm{U}_{C_{\mathrm{rev}}} + \mathrm{U}_{\mathrm{PPK}_i} + \mathrm{U}_{\mathrm{SKMSN}_i} + \mathrm{U}_{\mathrm{SIG}})/$ U..

Proof By the Assumption from ECDLP, Let p_1 and p_2 be the two points on the elliptic curve $E_q|F_q$; *where* $p_2 = x\ p_1$; and an invader ξ_1 can produce a message $\{\mathrm{QMSN}_{\mathrm{ID}_I}||\bar{\bar{Q}}_i||\mathrm{SMSN}_{\mathrm{PPK}_i}||M_i||t_i||$ꓙ$_{\mathrm{i}}\}$. Therefore a game is being built between the invader ξ_1 and a challenger ß$_1$, where ß$_1$ possess capabilities to run ξ_1 to solve ECDLP as a sub-procedure with a trivial probability.

Setup: The challenger ß$_1$, selects a master key α and calculates the public key with $C_{\mathrm{pub}} = \psi\ P$ and sends the system parameters pms $\{P, p, q, E, G, C_{\mathrm{pub}}, L_{\mathrm{pub}}, Z_{\mathrm{pub}}, h_0, h_1, h_2, h_3\}$ *to* ξ_1.

H*$_2$ *Query*:** When ξ_1 uses the query H_2 with the parameter $(\mathrm{QMSN}_{\mathrm{ID}_I}, \overline{\overline{Q_l}})$, ß$_1$ checks whether the tuple L_{h_2} is already in the hash list L_{h_2} or not. If so, ß$_1$ sends $\aleph_{h_2} = H_2(\mathrm{QMSN}_{\mathrm{ID}_I}, \overline{\overline{Q_l}})$ to ξ_1. If else, ß$_1$ selects a random $\aleph_{h_2} \varepsilon Z_q{}^*$ and appends it to $(\mathrm{QMSN}_{\mathrm{ID}_I}, \overline{\overline{Q_l}}, \aleph_{h_2})$ into the hash list $\aleph_{h_2}$. In the end ß$_1$ transmits$\aleph_{h_2} = H_2(\mathrm{QMSN}_{\mathrm{ID}_I}, \overline{\overline{Q_l}}) to \xi_1$. ***H*$_3$ *Query: When ξ_1 uses the query H_3 with the parameter $(M_i, \mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i},$ ꓙ$_i, T_i)$, ß$_1$ checks a tuple $(M_i, \mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i},$ ꓙ$_i, T_i, \aleph_{h_2})$ in order to examine whether the input is kept previously in the hash list $\aleph_{h_2}$. If so ß$_1$ sends $\aleph_{h_3} = H_3$ $(M_i, \mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i},$ ꓙ$_i, T_i)$ to ξ_1. Else, ß$_1$ selects a random $\aleph_{h_3}$ ε $Z_q{}^*$ and appends it to $(M_i, \mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i},$ ꓙ$_i, T_i, \aleph_{h_3})$ into the hash list$\aleph_{h_3}$. In the end, transmits $(M_i, \mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i},$ ꓙ$_i, T_i, \aleph_{h_3})$ to ξ_1.

Partial Private Query: When ξ_1 utilizes a partial private query on a masked identity $\mathrm{QMSN}_{\mathrm{ID}_I}$, ß$_1$ calculates $\overline{\overline{Q_l}}$, $\overline{\overline{Q_m}}$ of both the central medical server and the local medical server by choosing φ, γ ε $Z_q{}^*$ as the random number or integers and examines whether the tuple $(\overline{\overline{Q_i}}, \mathrm{PPK}_i)$ is present in the hash list $\aleph_{h_2}$. If, ß$_1$ finds that it has obtained a failed output and solution for the query. Else, ß$_1$ finds the private key $(\mathrm{PPK}_i = \mathrm{PPK}_k + \mathrm{PPK}_j;\ \forall_j,\ \forall_k \varepsilon \forall_i;)\ \psi \bmod U$ and then the value of PPK_i is sent to ξ_1.

[*Note*: It is impossible to obtain the partial private key PPK_i by ξ_1 by using $\mathrm{QMSN}_{\mathrm{ID}_I}$. Even if he invokes the query it is not possible to find the partial private key ξ_1 has to get access into the partial private keys of both CMS and LMS which is not feasible within a polynomial-time.]

Create-Sensor Node Query: Let us assume the invader requests for a masked identity $\mathrm{QMSN}_{\mathrm{ID}_I}$.
If the list contains $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$ then ß$_1$ examines $\mathrm{SMSN}_{\mathrm{PPK}_i}$ if $\mathrm{SMSN}_{\mathrm{PPK}_i} = \bot$. Iff $\mathrm{SMSN}_{\mathrm{PPK}_i}! = \bot$ then ß$_1$ sends $\mathrm{SMSN}_{\mathrm{PPK}_i}$ to ξ_1. Else ß$_1$ selects a random value ∇_i ε $Z_q{}^*$ then finds $\mathrm{SMSN}_{\mathrm{PPK}_i} = \nabla_i$ P and sets $\mathrm{SKMSN}_i = \nabla_i$. Now ß$_1$ transmits $\mathrm{SMSN}_{\mathrm{PPK}_i}$ to ξ_1 performs updation by updating the values in the list $L(\mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$.
If the list cannot include $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$ then ß$_1$ sets $\mathrm{SMSN}_{\mathrm{PPK}_i} = \bot$ and selects a random value $\nabla_i \varepsilon Z_q{}^*$ and finds $\mathrm{SMSN}_{\mathrm{PPK}_i} = \nabla_i$ P and sets $\mathrm{SKMSN}_i = \nabla_i$. Now ß$_1$ transmits $\mathrm{SMSN}_{\mathrm{PPK}_i}$ to ξ_1 performs adding the values in the list $L(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$.

Secret-Key Query: Let us assume the invader requests for a secret key.
If the list contains $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$ then ß$_1$ examines SKMSN_i, if $\mathrm{SKMSN}_i = \bot$. Iff $\mathrm{SKMSN}_i = \bot$, then ß$_1$ sends it SKMSN_i to ξ_1. Else, ß$_1$ by utilizing create-node query it generate $\mathrm{SMSN}_{\mathrm{PPK}_i} = \mathrm{SMSN}_{\mathrm{PPK}_i}$. Then ß$_1$ transmits $\mathrm{SMSN}_{\mathrm{PPK}_i}$ to ξ_1, and perform updation to the list L as $(\mathrm{SMSN}_{\mathrm{PPK}_{\mathrm{i}}}, \mathrm{SKMSN}_{\mathrm{i}})$.
If the list cannot include $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$, then ß$_1$ performs a create node query and sends SKMSN_i to ξ_1 and appends $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, \mathrm{SKMSN}_i)$, to the list L.

Sign Query: When ξ_1 executes the sign query on the message M_i, ß$_1$ checks if the tuple $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i} \aleph_{\mathrm{h}_2})$ is in the list $\aleph_{\mathrm{h}_2}$. Iff not ß$_1$ gets $\aleph_{\mathrm{h}_2}$ from the tuple and selects two random numbers Ψ_{i}, F_{i} and finds ꓙ$_{\mathrm{i}} = \theta_i\ P$ and $\overline{\mathrm{X}_{\mathrm{i}}} = \mathrm{F}_{\mathrm{i}}$ P and Ƹ$_{\mathrm{i}} = \{$ꓙ$_{\mathrm{i}}, \bar{X}_{\mathrm{l}}\}$ transmits it to ξ_1 and appends it to $(\mathrm{QMSN}_{\mathrm{ID}_I}, \mathrm{SMSN}_{\mathrm{PPK}_i}, M_i, T_i,$ ꓙ$_{\mathrm{i}}, \aleph_{h_3})$ list L.

With respect to the bifurcation axiom, ß$_1$ has the ability to obtain two different legal signatures $\tau_{\mathrm{i}} = \{$ꓙ$_{\mathrm{i}}, \bar{\mathrm{X}}_{\mathrm{l}}\}$ and $\acute{\tau}_{\mathrm{l}} = \{$ꓙ́$_{\mathrm{l}}, \acute{\bar{\mathrm{X}}}_{\mathrm{l}}\}$ in a polynomial time, where $\overline{X_i} = F_i \cdot \theta_i \oplus \mathrm{SKMSN}_i \mod p$ and $\acute{Z}_i = \acute{H}_i \cdot \theta_i \oplus \mathrm{SKMSN}_i \mod p$. Because by calculating

$$\frac{\acute{F}_i \overline{X_i} - F_i \acute{X}_i}{\acute{F}_i - F_i} = \frac{\acute{F}_i\left(\mathrm{SMSN}_{\mathrm{PPK}_i} \oplus\ \mathrm{QMSN}_{\mathrm{ID}_I} \oplus \overline{\overline{F_i}}\right) - F_i\left(\left(\mathrm{SMSN}_{\mathrm{PPK}_i} \oplus\ \mathrm{QMSN}_{\mathrm{ID}_I} \oplus \overline{\overline{F_i}}\right)\right)}{\acute{F}_i - F_i}$$

$$= \frac{\acute{F_i}\left(\mathrm{SMSN}_{\mathrm{PPK}_i}\right) \oplus \acute{F_i}\ \mathrm{QMSN}_{\mathrm{ID}_I} \oplus \overline{\overline{F_i}}\,\acute{F_i} - F_i\,\mathrm{SMSN}_{\mathrm{PPK}_i} \oplus F_i\ \mathrm{QMSN}_{\mathrm{ID}_I} \oplus \overline{\overline{F_i}}\,F_i}{\acute{F_i} - F_i} = \mathrm{SMSN}_{\mathrm{PPK}_i}$$

for $\mathcal{E} \geq 10(\mathrm{U}_{SIG} + 1)\ (\mathrm{U}\ _{h_1} + \mathrm{U}\ _{h_2} + \mathrm{U}_{C_{\mathrm{rev}}} + \mathrm{U}_{\mathrm{PPK}_i} + \ \mathrm{U}_{\mathrm{SKMSN}_i} + \mathrm{U}_{\mathrm{SIG}})/\ \mathrm{U}$,, ß$_1$ can solve the ECDLP within a time less than 120,686ȵ$T/\mathcal{E}$.. But, this is an absolute contradict when compared with the hardness and the intractability of ECDLP. Hence it is proved that the proposed scheme is efficient to resist forgery under chosen message attacks.

Theorem 2 *If and when the scheme is resistant to chosen message attacks, then it is effective towards existential forgery by means of aggregation chosen.*

Proof Let us assume that the forger ξ_2 can crack the proposed data authentication scheme. Assuming that the challenger, ß$_2$ utilize the capability of ξ_2 to solve the ECDLP. Now the challenger ß$_2$ interacts with ξ_2 and performs the following:

Setup: The challenger ß$_2$ chooses a random master key ψ ε $Z_q{}^*$ and calculates the public key with $C_{\mathrm{pub}} = \psi\ P$ and initializes the oracle. When the game starts with a query by ß$_2$, ξ_2 makes a list L (QMSN$_{\mathrm{ID}_i}$, SMSN$_{\mathrm{PPK}_i}$, PPK$_j$, $\overline{\overline{Q_l}}$) or (QMSN$_{\mathrm{ID}_i}$, SMSN$_{\mathrm{PPK}_i}$, PPK$_k$, $\overline{\overline{Q_m}}$) and gives answer to ß$_2$ query as follows:

***H*$_2$ Query:** Whenever a masked -identity is presented to an oracle H_2, ß$_2$ first throws a coin c_i ε {0,1}in order to generate the probability. c_i gives 0 when the probability is ε and gives 1 when the probability is 1 – ε. Therefore ß$_2$ selects ξ_i ε $Z_q{}^*$ at random. If c_i gives 0; then $\overline{\overline{P_l}} = \xi_i\ P$ and when gives 1 then ß$_2$ gives $\overline{\overline{P_l}} = \xi_i\ P$. In both cases ß$_2$ inserts a tuple (QMSN$_{\mathrm{ID}_i}$, ξ_i, c_i, $\overline{\overline{Q_l}}$) or (QMSN$_{\mathrm{ID}_i}$,Ƨ$_i$, c_i, $\overline{\overline{Q_m}}$) into the list $L_{h_2} \rightarrow$ (QMSN$_{\mathrm{ID}_i}$, ξ_i, c_i, $\overline{\overline{Q_l}}$) or $L_{h_2} \rightarrow$ {QMSN$_{\mathrm{ID}_i}$,Ƨ$_i$, c_i, $\overline{\overline{Q_m}}$}.. A tracking has to be observed on its response.

When ß$_2$ produces the masked identities of n medical sensor nodes from the list $L_{\mathrm{QMSN}_{\mathrm{ID}_i}}{}^* = \{\mathrm{QMSN}_{\mathrm{ID}_i}*\}$; $\forall_i$; the public keys $L_{pk_i}{}^* = \{\mathrm{PPK}_i*\}$; $\forall_i$; which correlate to every individual identity that are anonymous, Messages $L_M{}^* = \{M_i*\}$; $\forall_i$ as well as certificate-less aggregate signatures Ƨ$_\mathrm{i}$ = {Л$_i$, $\overline{X_\iota}$}*; $\forall_i$.; $\forall_i$.

When ß$_2$ identifies the particular nth tuple (QMSN$_{\mathrm{ID}_i}$, ξ_i, c_i,$\overline{\overline{Q_l}}$) from L_{h_2} with $c_k = 1$ and c_j=1;$\forall_i$. But the tuples are (QMSN$_{\mathrm{ID}_i}*$, PPK$_i*$, M_i*) is not yet transmitted to the oracle. Else ß$_2$ is unsuccessful and stops proceeding further. Iff ß$_2$ succeeds, PPK$_j.P = \varphi \oplus h_2$ {QMSN$_{\mathrm{ID}_i}||\overline{\overline{Q_l}}$}.$C_{\mathrm{pub}}$; $\overline{Z_i} = \xi_i$PPK$_j$ $\forall_j$!=$\forall_k$ and hence the aggregate signature$\overline{X_i}.P = \sum_{i=1}^{n}\{F_i\theta_i + \mathrm{SKMSN}_i\}.P$. Further, ß$_2$ finds the particular tuples (QMSN$_{\mathrm{ID}_i}*$, SMSN$_{\mathrm{PPK}_i}*$, SKMSN$_i*$,Λ_i*, $\xi_{2i}*$) and (QMSN$_{\mathrm{ID}_i}*$, $\overline{\overline{Q_l}}*$, Л$_i*$, SKMSN$_i*$) from the lists L_{h_2} andL_{h_3}. If and when ß$_2$ sets $\overline{X_i}*$=ξ_i,ψ, $\overline{X_i}*P = \xi_i C_{\mathrm{pub}}$=$\xi_i$.

Finally when ß$_2$ sets $\acute{X}_i* = \overline{X_i}* - \sum_{i=1, i!=k}^{n} \overline{X_i}*$ which by means Л$_i * = \theta_\mathrm{i} *$P; so $\acute{X}_i^* = \mathrm{PPK}_j^* - \sum_{i=1}^{n} \theta_i^* \xi_{2i}^*$. ß$_2$ chooses $F_k *$ ε$Z_q{}^*$ randomly and then computes Л$_i' * = (F_k' *)^{-1} \sum_{i=1}^{n}$ Л$_i * \xi_{2i} *$.. Therefore ß$_2$ sets the hash value as $F_k * = H_3$ ($M_i *$, QMSN$_{\mathrm{ID}_i} *$, SKMSN$_i *$, Л$_i *$) and SKMSN$_i$= $\sum_{i=1}^{n}$ SKMSN$_i*$. If the tuple H_3 (M_i*, QMSN$_{\mathrm{ID}_i}*$, SKMSN$_i*$, Λ_i*) is found in the list L_{h_3}, then ß$_2$ will make a try until it does not happen. Therefore, According to the verification, the proposed certificate-less aggregate signature scheme can be forged:

$$\sum_{i=1}^{n}\{F_i\theta_i + \mathrm{SKMSN}_i\}P$$

$$= \text{Л}_i * P + \textstyle\sum_{i=1}^{n} \mathrm{SKMSN}_i * F_k * P$$

$$= \text{Л}_i * \theta_i * P + \textstyle\sum_{i=1}^{n} \mathrm{SKMSN}_i * F_k * P$$

$$= \acute{X}_\iota * P$$

Hence the obtained result is a contradiction to the ECDLP assumption made. Thus the proposed scheme is resistant to forgery attacks.

6.2 BAN Logic

This section verifies the correctness of the proposed authentication scheme by providing an analysis using the Burrows–Abadi–Needham (BAN) logic [71]. It is apparent that our proposed scheme has achieved the required security goals. The primitives of the BAN logic are as follows:

$$P_1 : \text{Message-Dispatch Rule} : \frac{R| \equiv R \leftrightarrow S,\ R \triangleleft (X)_k}{R| \equiv S| \sim Y}$$

$$P_2 : \text{Nonce} - \text{Verification Rule} : \frac{R| \equiv \#(Y),\ R| \equiv S| \sim Y}{R| \equiv S| \equiv Y}$$

$$P_3 : \text{Jurisdiction Rule} : \frac{R| \equiv S \Rightarrow Y,\ R| \equiv S| \Rightarrow Y}{R| \equiv Y}$$

$$P_4 : \text{Freshness} - \text{Conjuncatenation Rule} : \frac{R| \equiv \#(Y)}{R| \equiv \#(Y,\ Z)}$$

$$P_5 : \text{Session} - \text{Key Rule} : \frac{R|\equiv \#Y,\ R|\equiv S|\equiv Y}{R|\equiv R \overset{k}{\underset{\leftrightarrow}{}} S}$$

In order to prove the correctness of the proposed authentication scheme, the following objectives are to be proved and are as follows:

Obj 1: CMS: C_{pub}, $\text{QMSN}_{\text{ID}_l}$, CE_{pvk}
Obj 2: LMS: $\overline{\overline{Q}}_i$, PPK_i, OTP_i
Obj 3: $ZN|\equiv F_i$, SKMSN_i
Obj 4: $\text{CE}| \equiv F_i, JJ_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \overline{\overline{F}}_i, C_{\text{pub}}, \text{Password}_i, \text{OTP}_i$
Obj 5: $MSN| \equiv\ M_i, \text{QMSN}_{\text{ID}_I}, \text{SMSN}_{\text{PPK}_i}, \overline{\overline{Q}}_i, JJ_i, t_i$
Obj 6: $\text{CMS}|\equiv \text{Password}_i$, OTP_i, t_i
Obj 7: $\text{LMS}|\equiv \text{Password}_i$, OTP_i, t_i

The messages exchanged between the medical sensor nodes, local medical server, central medical server and the zonal node can be formulated as follows:

$$M_1 : \text{MSN} \to \text{LMS}\left\{\text{MSN}_{\text{ID}_l},\ Q_i\right\}$$

$$M_2 : \text{CMS} \to \text{MSN}\left\{\text{QMSN}_{\text{ID}_I},\ Q_i,\ \overline{Q}_i,\ C_{\text{pub}},\ t_i\right\}$$

$$M_3 : \text{LMS} \to \text{MSN}\{\overline{\overline{Q}}_i,\ \text{QMSN}_{\text{ID}_I},\ L_{\text{pub}}\}$$

$$M_4 : \text{LMS} \to \text{ZN}\left\{\overline{\overline{Q}}_k,\ \text{PPK}_j\right\}$$

$$M_5 : \text{CMS} \to \text{ZN}\left\{\overline{\overline{Q}}_m,\ \text{PPK}_k\right\}$$

$$M_6 : \text{ZN} \to \text{MSN}\left\{\overline{\overline{Q}}_i,\ \text{PPK}_i\right\}$$

$$M_7 : ZN \to \text{CE}\left\{JJ_i, \text{SKMSN}_i\right\}$$

$$M_8 : \text{CMS} \to \text{CE}\left\{\text{Password}_i,\ \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}}\right\}$$

$$M_9 : \text{LMS} \to \text{CE}\left\{\text{OTP}_i,\ \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}}\right\}$$

The pre-requisites for the formal proof verification are as follows:

$$A_1 : \text{MSN}|\equiv \text{MSN} \xrightarrow{\text{MSN}_{\text{ID}_I},\, Q_i} \text{CMS}$$

$$A_2 : \text{MSN}|\equiv \#\Delta T_i$$

$$A_2 : \text{MSN}|\equiv \text{CMS} \Rightarrow \text{MSN}_{\text{ID}_I},\ \psi,\ Q_i,\ C_{\text{pub}},\ \Delta T_{\boldsymbol{i}}$$

$$A_4 : \text{CMS}|\equiv \#\Delta T_i$$

$$A_5 : \text{CMS}|\equiv MSN \Rightarrow Q_i,\ \overline{Q}_i,\ \Delta T_{\boldsymbol{i}}$$

$$A_6 : \text{LMS}|\equiv \#\Delta T_i$$

$$A_7 : LMS|\equiv ZN \Rightarrow \text{PPK}_j,\ \overline{\overline{Q}}_i,\ L_{\text{pub}}$$

$$A_8 : LMS|\equiv ZN \Rightarrow \text{PPK}_i,\ \overline{\overline{Q}}_i$$

$$A_9 : \text{CMS}|\equiv ZN \Rightarrow \text{PPK}_m,\ \overline{\overline{Q}}_m,\ C_{\text{pub}}$$

$$A_{10} : ZN|\equiv MSN \Rightarrow \text{PPK}_i,\ \overline{\overline{Q}}_i$$

$$A_{11} : ZN|\equiv MSN \Rightarrow C_{\text{pub}},\ L_{\text{pub}},\ T_{\text{pub}}$$

$$A_{12}: \text{CE}| \equiv \text{CMS} \Rightarrow F_i, JJ_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \overline{\overline{F}}_i, C_{\text{pub}}, \text{Password}_i, \text{CE}_{pvk}, \Delta T_{\boldsymbol{i}}$$

$$A_{13} : \text{CE}|\equiv \Delta T_{\boldsymbol{i}}$$

$$A_{14} : \text{CE}|\equiv ZN \Rightarrow C_{\text{pub}},\ L_{\text{pub}},\ T_{\text{pub}},\ \Delta T_{\boldsymbol{i}}$$

$$A_{15}: \text{CMS}| \equiv \text{LMS}$$
$$\Rightarrow F_i, JJ_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \overline{\overline{F}}_i, C_{\text{pub}}, \text{Password}_i, \text{CE}_{\text{pvk}}, \Delta T_{\boldsymbol{i}}$$

$$A_{16} : \text{CMS}|\equiv \text{CE} \Rightarrow,\ \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}}$$

$$A_{17} : LMS|\equiv \text{CE} \Rightarrow,\ \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}}$$

$$A_{18}: \text{LMS}| \equiv \text{CE}$$
$$\Rightarrow F_i, JJ_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \overline{\overline{F}}_i, C_{\text{pub}}, \text{OTP}_i, \text{CE}_{\text{pvk}}, \Delta T_{\boldsymbol{i}}$$

According to these formulations and logical proposition of BAN logic the formal correctness proof of the proposed scheme are as follows:

By message 3, the following statement can be obtained:

$$S_1 : ZN \lhd \left\{L_{\text{pub}},\ T_{\text{pub}},\ \text{QMSN}_{\text{ID}_I}\right\}_{\text{MSN}_{\text{ID}_I},\, Q_i,\, \overline{Q}_i,\, \Delta T_{\boldsymbol{i}},\, C_{\text{pub}}}$$

According to S_1, A_1 and Obj 1, we have,

$$S_2 : ZN| \equiv \text{MSN}| \sim Q_i, \bar{Q}_i, \Delta T_{\boldsymbol{i}}, \text{Л}_i, \text{SMSN}_{\text{PPK}_i}$$

According to S_2, A_2 and Obj 2 and Obj 4, we have,

$$S_3 : ZN| \equiv \text{MSN}| \equiv Q_i, \bar{Q}_i, \Delta T_{\boldsymbol{i}}, \text{Л}_i, \text{SMSN}_{\text{PPK}_i}$$

According to S_3, A_3, and Obj 3, we have

$$S_4 : ZN| \equiv \text{MSN}| \equiv Q_i, \bar{Q}_i, \Delta T_{\boldsymbol{i}}, \text{Л}_i, \text{SMSN}_{\text{PPK}_i} \qquad \text{(Obj 3)}$$

By message 1, the following statement is obtained:

$$S_5 : \text{CMS}|\lhd \text{MSN}| \sim \text{QMSN}_{\text{ID}_I},\ Q_i,\ \overline{Q}_i,\ \Delta T_{\boldsymbol{i}},\ C_{\text{pub}}$$

According to S_5, A_5, Obj 2 and Obj 4, we have

$$S_6 : \text{CMS}|\equiv \text{MSN}|\equiv \text{QMSN}_{\text{ID}_I},\ Q_i,\ \overline{Q}_i,\ \Delta T_{\boldsymbol{i}},\ C_{\text{pub}}$$

According to S_6, A_5 and Obj 3, we have

$$S_7 : \text{CMS}|\equiv \text{MSN}| \equiv \text{QMSN}_{\text{ID}_I},\ Q_i,\ \overline{Q}_i,\ \Delta T_{\boldsymbol{i}},\ C_{\text{pub}} \qquad \text{(Obj 1)}$$

By message 2, the following statement can be obtained:

$$S_8 : \text{LMS}|\lhd \text{MSN}| \sim Q_i,\ \text{PPK}_i,\ L_{\text{pub}},\ \text{QMSN}_{\text{ID}_I}$$

According to S_8, A_6, Obj 3 and Obj 4, we have

$$S_9 : \text{LMS}|\equiv \text{MSN}|\equiv Q_i,\ \text{PPK}_i,\ L_{\text{pub}},\ \text{QMSN}_{\text{ID}_\text{I}}$$

According to S_9, A_7, Obj 3, we have

$$S_{10} : \text{LMS}|\equiv \text{MSN}| \equiv Q_i,\ \text{PPK}_i,\ L_{\text{pub}},\ \text{QMSN}_{\text{ID}_I} \quad \text{(Obj 2)}$$

By message 5, the following statement can be obtained:

$$S_{11} : \text{MSN}|\lhd ZN|\text{QMSN}_{\text{ID}_I}, \bar{\bar{Q}}_i, \text{PPK}_i, \text{SMSN}_{\text{PPK}_i}, \Delta T_{\boldsymbol{i}}\ , \text{Л}_i$$

According to S_{11}, A_1, A_2, Obj 2 and Obj 4, we have

$$S_{12} : MSN|\equiv ZN| \sim QMSN_{ID_I}, \bar{\bar{Q}}_i, PPK_i, SMSN_{PPK_i}, \Delta T_{\boldsymbol{i}}\ , \text{Л}_i$$

According to S_{12}, A_3, Obj 1, we have

$$S_{13} : \text{MSN}|\equiv ZN|\text{QMSN}_{\text{ID}_I}, \bar{\bar{Q}}_i, \text{PPK}_i, \text{SMSN}_{\text{PPK}_i}, \Delta T_{\boldsymbol{i}}\ , \text{Л}_i$$

According to S_{13}, A_{11}, Obj 1 and Obj 3, we have

$$S_{14} : \text{MSN}|\equiv ZN|\text{QMSN}_{\text{ID}_I}, \bar{\bar{Q}}_i, \text{PPK}_i, \text{SMSN}_{\text{PPK}_i}, \Delta T_{\boldsymbol{i}}\ , \text{Л}_i \qquad \text{(Obj 5)}$$

By message 4, the following statements can be obtained:

$$S_{15} : \text{CE}| \lhd ZN|F_i, \text{Л}_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \bar{\bar{\bar{F}}}_i, C_{\text{pub}}$$

According to S_{15}, A_{11}, A_{10}, Obj 2 and Obj 4, we have

$$S_{16} : \text{CE}| \equiv ZN| \sim F_i, \text{Л}_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \bar{\bar{\bar{F}}}_i, C_{\text{pub}}$$

According to S_{16}, A_{12}, A_{13} and Obj 3, we have

$$S_{17} : \text{CE}| \equiv ZN| \equiv F_i, \text{Л}_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \bar{\bar{\bar{F}}}_i, C_{\text{pub}}$$

According to S_{17}, A_{14} and Obj 1, we have

$$S_{18} : \text{CE}| \equiv ZN| \equiv F_i, \text{Л}_i, \text{SMSN}_{\text{PPK}_i}, \text{QMSN}_{\text{ID}_I}, \bar{\bar{\bar{F}}}_i, C_{\text{pub}} \quad \text{(Obj 4)}$$

By message 6, the following statement can be obtained:

$$S_{19} : \text{CMS}|\lhd \text{CE}|\text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}},\ \text{Password}_i$$

According to S_{19}, A_{15}, A_{16}, Obj 2 and Obj 4, we have

$$S_{19} : \text{CMS}|\equiv \text{CE}| \sim \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}},\ \text{Password}_i$$

According to S_{19}, A_{16}, and Obj 3, we have

$$S_{20} : \text{CMS}|\equiv \text{CE}| \equiv \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}}, \quad \text{Password}_i \qquad \text{(Obj 6)}$$

By message 6, the following statement can be obtained:

$$S_{21} : \text{LMS}|\lhd \text{CE}|\text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}},\ \text{OTP}_i$$

According to S_{21}, A_{15}, A_{17}, Obj 2 and Obj 4, we have

$$S_{22} : \text{LMS}|\lhd \text{CE}| \sim \text{CE}_{\text{pvk}},\ \Delta T_{\boldsymbol{i}},\ \text{OTP}_i$$

According to S_{22}, A_{18}, A_{17}, and Obj 3, we have

$$S_{23} : \text{LMS}|\lhd \text{CE}| \equiv \text{CE}_{\text{pvk}}, \quad \Delta T_{\boldsymbol{i}},\ \text{OTP}_i \qquad \text{(Obj 7)}$$

From the above performed analysis, it is apparent that the proposed full privacy-preserving distributed batch-based certificate-less signature authentication scheme for health-care wearable wireless medical sensor networks has achieved all the necessary security objectives (Obj 1–7) and performs efficient batch-wise authentication in a secured way.

6.3 Informal security analysis

Informal security analysis has been carried out in order to assure that the proposed full privacy-preserving data authentication scheme is efficient in relative to message legitimacy and legality, Non-repudiation, anonymity, traceability, unlinkability and resistance to attacks.

Data Integrity and Authentication: Whenever the data get legally signed, it is meant to be authenticated. To assure the integrity of the data the verifier has to verify the timestamp $X_i = h_4\{M_i||\text{QMSN}_{\text{ID}_I}||\bar{\bar{Q}}_i||\text{SMSN}_{\text{PPK}_i}||\text{ЛJ}_i||t_i\}$ and verifies $\overline{X_i} = h_4{\cdot}\theta_i \oplus \text{SKMSN}_i \bmod p$ which is highly intractable.

Anonymity Since the original identity of the sensor node is encrypted by the central server and the local server it is highly impossible for the attacker to determine which entity possess that. It is also not possible to gain access even if the attacker gets the data.

Traceability In our proposed scheme the sensor nodes cannot be traced since the pseudo-identities are generated by two various entities in a distributed fashion. Only in case of conflicts the central medical sever or the local medical server with the authorization of the CMS can be traced toward its real identity.

Unlinkability Message signature generated from a medical sensor node $X_i = h_4\{M_i//\text{QMSN}_{\text{ID}_I}//\bar{\bar{Q}}_i//\text{SMSN}_{\text{PPK}_i}//\text{ЛJ}_i//t_i\}$ contains the random component for pseudo-identity generation this can't be related with the real identity since they are encrypted via the secret keys. Hence one signature cannot be linked in any way to that of the others.

6.4 Resistance to attacks

(i) Replay Attacks: This kind of attack is possible only when an attacker can be able to capture the message that has been already sent. Even the attacker can be able to compensate the timestamp it is highly impossible since it engulf full aggregation including the random part of the signature being generated according to the equation $\overline{X_i} = h_4 \cdot F_i\theta_i \oplus \text{SKMSN}_i \bmod p$.

(ii) Modification Attacks: According to the equation $X_i = h_4\{M_i//\text{QMSN}_{\text{ID}_I}//\bar{\bar{Q}}_i//\text{SMSN}_{\text{PPK}_i}//\text{ЛJ}_i//t_i\}$ is a generated signature with which contains an anonymous signature part $(\text{QMSN}_{ID_I}, \text{ЛJ}_i)$ that needs the simultaneous keys from the central, local and zonal node. Hence it is not possible for an invader to perform modification attacks since they are strongly coupled.

(iii) Impersonation and masquerading Attacks: In order to perform an impersonation attack an attacker has to gain an access privilege of the public entities like central medical server's secret key for the system even if he has access to the public parameters which is highly impossible. Even if local medical server or the zonal node gets attacked, it is impossible to gain access since the private keys are partially made and in a distributed fashion. The major possibility of impersonation can happen either at the patient end or at the clinical expert end. If an invader impersonates himself as a doctor and even if he knows or cracks the password, it is impossible to obtain the one-time password required to gain access to view the system. Supposing that even if he attempts to gain access; it is impossible for him to send the fake prescription or to steal the data because again it requires a one-time password which is difficult to crack. The major advantage of our proposed scheme is that only an authorized person knows the private key required to generate the OTP. Hence it is a two-way door authentication mechanism which is difficult to crack. If more than one attempt the corresponding entry will be blocked or locked. Similarly of a patient tries to steal the text data, it is not possible to steal the data since he needs a One-time password to access it. The limitation is set as only one try is allowed. The second try needs a verification from an information analyst professional who will be sitting at the central or local medical server.

(iv) Stolen verifier table attacks: Since the design of the scheme doesn't maintain any explicit catalog it is not possible for any invader to perform stolen verifier attack.

(v) Key escrow attack: The attacker cannot be able to find even the masked identity of the medical sensor node since they are registered and generated by the central or local medical server which is once more encrypted via the secret key of the zonal node with the help of one-way hash functions. This makes it more efficient to gain access to the individual sensor nodes.

(vi) Man-in-the-Middle Attacks: Assuming that any invader stays in the communication channel between. For example, when the invader stays in between the medical sensor node and the zonal node he cannot gain access to the secret key of the sensor node since it was not generated by it. Even if the invader stays in between the zonal node and the local server, it is impossible to gain access without knowing the secret key of the zonal node and the local server combined. Even though, if the invader gains access to both the keys it is not possible to gain the access privileges of the central storage server.

(vii) Denial-of-service attacks: Since batch-wise aggregation is followed it reduces half of the computation time needed for signature verification. Therefore, it can be able to overcome the overhead incurred in single signature verification which makes the verifier to be more available along with its resources.

(viii) Coalition-Resistant Attacks: It is not possible for any invader to generate a legal message signature due to the usage of coalition resisting one way hash functions.

Table 4 Performance rate of various cryptographic functions

Function	T_{BPF}	$T_{\text{\_MUL}}$	$T_{\text{\_BPAO}}$	$T_{\text{\_MPTH}}$	$T_{\text{\_E-M}}$	$T_{\text{\_Oh}}$
Execution-time (ms)	3.61	1.63	1	1	2.74	1

Table 5 Execution analogy of the traditional data authentication schemes

Methodology	Hard problem (HP)	Pairing operation	Aggregation type	Peril/safe
Shen et al. [33]	CDHP	Bilinear pairing	Partial	Peril
Shuai et al. [47]	HP	Non-bilinear pairing	Partial	Peril
Zhang et al. [48]	ECDLP	Non-bilinear pairing	Partial	Safe
Ryu et al. [49]	HP	Non-bilinear pairing	Full	Safe
Peng et al. [52]	HP	Non-bilinear pairing	Full	Peril
Proposed	ECDLP	Non-bilinear pairing	Full	Safe

Table 6 ECC-based group field range

Method	Curve	Pairing	Cyclic group	$\|P\|$	$[G\}$	Group field range
Bilinear-pairing	$\overline{E}$: $x^2 = y^3 + y \bmod \widehat{p}$	$\widehat{e}$: $G_1 \times G_2 \rightarrow G_T$	$G_1(P)$	64 Bytes	$q = 20$ bytes	$\|G_1\| =$ 128 bytes
Elliptic curve	$\overline{E}$: $x^2 = y^3 + ay + b \bmod p$	No	$G(P)$	20 Bytes	$q = 20$ bytes	$\|G\| =$ 40 bytes

7 Performance analysis

This section analyzes the performance of the proposed full privacy-preserving data authentication scheme in terms of communication and computation costs. The analysis has been performed for the chosen parameters in terms of message signing, single signature and aggregate Signature verification. The proposed scheme has been compared with the schemes like [11, 33, 47–49, 52]. Evaluation method has been adapted from [65, 66]. The proposed scheme utilizes Intel i8 Neon processor, 3.20 GHz clock speed, 4 GB memory under windows 8 operating system environment using MIRACL C++ cryptographic library [67]. Under bilinear pairing Tate pairing is used over the super singular elliptic curves with a security parameter of length 80 bits. Bilinear pairing operation can be defined by the form $\widehat{e}$: $G_1 \times G_2 \rightarrow G_T$, where G defines the group operation. Our proposed scheme utilizes elliptic curve cryptography which is a Koblitz curve defined by the form $x^2 = y^3 + ay + b \bmod P$; $\forall\, a, b\ \varepsilon\ F_p$ over a finite field where the random prime p is set to 160 bits. The cryptographic operations are listed in Table 4. Table 5 provides the execution analogy of the traditional data authentication schemes. From these tables, it is evident that the schemes are insecure and vulnerable to attacks. The notations utilized in Table 4 can be defined as ensued: T_{BPF}—execution time required for the bilinear pairing operation $\widehat{e}\,(R, S)$ where R, S ε G_1; $T_{\text{\_MUL}}$—specifies the execution time required to perform scalar multiplication such that x.P; $T_{\text{\_BPAO}}$—specify the execution time required for performing point operation in a bilinear pairing operation such that $P = R + S$ where R, P, $S\ \varepsilon\ G_1$; $T_{\text{\_MPTH}}$—specify the execution time required to perform map-to-point hash operation such that $\widehat{e}\,(R, S)$ where R, $S\ \varepsilon\ G_1$; $T_{\text{\_E-M}}$-specifies the execution time required for performing the multiplication operation via a scalar such that x.P defined over an elliptic curve where $R\ \varepsilon\ G$ and $x\ \varepsilon\ Z_q{}^*$; $T_{\text{\_E-A}}$-specify the execution time required for performing the point addition operation over an elliptic curve group such that $P = R + S$ where R, P, $S\ \varepsilon G_1$; $T_{\_oh}$- specify the execution time required for performing the one-way hash operation. Table 6 provides the ECC-based group field range.

7.1 Cost of computation

According to the design of our proposed scheme, the computation cost can be evaluated at different entities, viz. medical sensor node, zonal node, local medical server or central medical server. Performance analysis has been conducted under two different strategies with the benchmarks in the field. From Table 6, the bilinear pairing-based data authentication proposed by shen et al. [33] involves three bilinear scalar multiplication operations, one bilinear point addition operation and one map-to-point hash operation approximating to 9.54 ms. It takes three bilinear scalar multiplication operations and two map-to-point hash operations for single message verification. In case of aggregation, it takes n bilinear pairing operation, one bilinear scalar multiplication

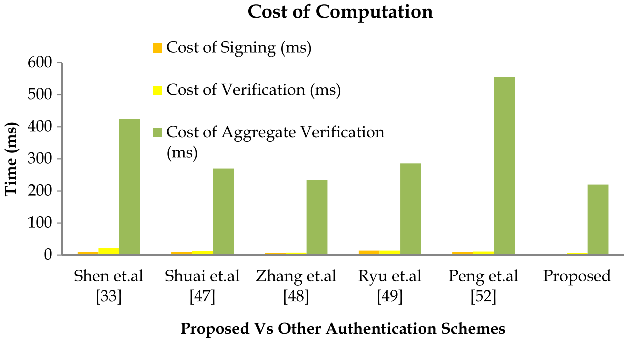

Fig. 5 Graph for computation cost

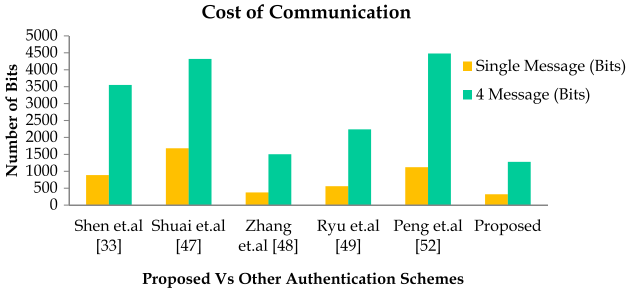

Fig. 6 Graph for communication cost

operation and n-1 bilinear point addition operation approximating 21.44 ms per 100 messages. In case of aggregation signature verification process, it takes n bilinear pairing operation, one bilinear scalar multiplication operation and n-1 bilinear point addition operation approximating to 424 ms per 100 messages. For other chosen benchmarks [11, 47–49, 52] the cost of computation for message signing takes approximately 10.107 ms, 5.853 ms, 14.123 ms, and 10.107 ms.

For single signature verification the computation cost approximates to 13.476 ms, 7.483 ms, 14.123 ms, and 11.23 ms. For aggregation the computation costs of the benchmarks approximates to 30.321 ms, 7.87 ms, 14.123 ms, and 11.23 ms per 100 messages. For our proposed scheme the computation cost for message signing approximates to one binary scalar multiplication operations, five binary point addition operations and one hash operation approximating to 3.753 ms. In case of single signature verification the cost of computation for our proposed scheme involves three binary scalar multiplication operation, one binary point addition operations and one hash operation approximating to 7.013 ms. In case of aggregation operation the cost of computation involves three n times of binary scalar multiplication operation, n times of binary point addition operations and n hash operation approximating to 7.013 ms per 100 messages. In case of aggregate signature verification process, the computation cost involves three 3n times of binary scalar multiplication operation, n times of binary point addition operations and n hash operation approximating to 7.013 ms per 100 messages. Figure 5 represents the graph comparison of the proposed scheme to that of the selected benchmarks. From the graph it is evident that our proposed has been efficient in dwindling the cost when compared with its counterparts. The major novelty of the proposed scheme is the use of aggregation and point addition which does not cause delay in verification and also reduces overhead in the Zonal node by employing elliptic curve cryptography (ECC). In the proposed scheme, the aggregation is performed in the Zonal Node**.** On the reception of the messages along with their time stamps are received by the Zonal Node. Initially the messages are analyzed first for the validity period and if it there then it accepts the message for verification. On successful verification of timestamps, the proposed scheme creates a batch of signatures within the range of time t by using the aggregate function. Once the batch gets created, the Zonal Node verifies the signatures. In batch verification method, the multiple signatures can be verified at a time instead of verifying them one by one. By doing so the length of the aggregated signature during verification is considerably reduced and it has significant impact on improving the overhead on computation, communication efficiency and storage (Fig. 6).

7.2 Cost of communication

The data aggregator (Zonal Node) sends the aggregated signature either to the local or the central medical server for verification. It is much desired that this transmission should possess less cost. To perform the analysis the parameter of security has been chosen to 64 bits. The calculation starts by selecting an element length of G_1 as 128 bytes and G as 40 bytes. Similarly for $Z_q{}^*$, the range is 20 bytes, hash function-20 bytes and times stamps-4 bytes. The ranges chosen are utilized for both the bilinear pairing and it is evident from Table 8 that our proposed scheme requires only 520 bits, thereby achieving full aggregation and is secure and efficient when compared with its counterparts. The cost for communication has to be proceeded except the message. For our proposed scheme, it involves three times of pairing and one addition and one hash operation equating to 3*40 + 20 + 20 = 160 bytes*8 = 1280 bits.

Similarly for Shen et al. [33], the communication cost involves three times of scalar binary pairing multiplication operation and one binary pairing operation and one addition operation accounting to 3*128 + 40 + 20 = 444 bytes = 3552 bits. For other Shuai et al. [47], it involves 27 times of hash operation accounting to 27*20 = 540 bytes = 4320 bits. For Zhang et al. [48] the communication cost involves one binary pairing operation and two times of scalar multiplication operation and one hash operation accounting to 128 + 2*20 + 20 = 188 bytes = 1504 bits. For Ryu et al.

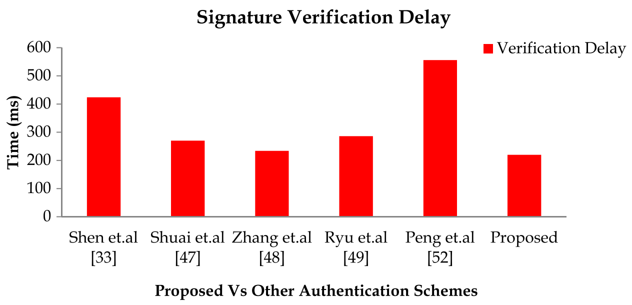

Fig. 7 Graph for the verification delay of the proposed scheme

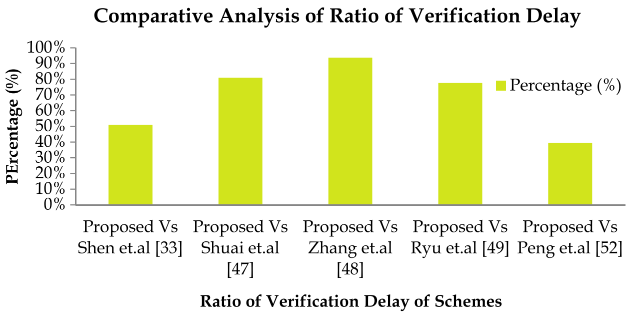

Fig. 8 Comparison graph for the ratio of verification delay of the proposed vs other schemes

[49] the communication cost involves 14 times of hash operation accounting to 14*20 = 280 bytes = 2240 bits. For Peng et al. [52] communication cost involves 23 times of hash operation accounting to 23*20 = 560bytes = 4480 bits. From the analysis carried out Shen et al. [33] chose bilinear pairing operation which increases the encrypted text length. The schemes [47, 49, 52] involves the use of XoR operation and one-way hash function which diminish the communication cost to a considerable extent, whereas it is not secure since it does not involve any secure mechanism to selects the secret keys. Similarly, the scheme [48] involves the use of elliptic curve cryptography which has the similar impact as that of our proposed scheme. Hence it is evident that our proposed scheme is efficient than that of its counterparts.

7.3 Verification delay

It is apparent that the verification of message signature is directly subjected to the availability of central medical server or the local medical server. In case of healthcare-based wearable wireless medical sensor networks the zonal node creates an aggregated batch of message signatures for every 100 messages. It is evident from the table that the proposed scheme exhibits a verification delay for every 1000 messages approximated to 7.013 ms. Hence our proposed scheme is efficient when compared with its counter benchmarks like [11, 47–49, 52] takes 424 ms, 30.321 ms, 7.87 ms, 14.123 ms, 25.829 ms, and 7.013 ms respectively. Figure 7 depicts the verification delay of the proposed scheme. Figure 8 represents the comparison graph for the ratio of improvement in terms of signature verification exhibited by the traditional schemes with respect to the proposed scheme. It is found that our scheme takes less cost of about 1280 bits for every single message transmission and 400 bits for every n aggregated message where the cost of communication gets decreased by significant improvement.

7.4 Experimentation

This section explains about the experimental simulation in order to assess the performance of the full privacy distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless body area networks. For our proposed scheme the simulation setup has been carried out by using network simulator (NS-3) tool. The simulation has been carried out on a laptop machine with Ubuntu Linux-based operating system of version 18.04 LTS on an intel i3-core processor with 8 GB RAM. Table 7 provides details on the parameters used for the simulation. Experimental analysis focused mainly on throughput and end-to-end delay which has a direct impact on the number of messages exchanged inside the network. Table 8 provides details on the settings of the network utilized.

Table 7 Experimental setup parameters

Parameter	Specification
Operating system	Ubuntu Linux 18.04 LTS
Area	400 * 200 m^2
Simulation time	1200 s
Bandwidth	2 Mbps
Communication protocol	IEEE 802.11p, 2.4 GHz WiFi

Table 8 Network setup

Scenario	Medical experts	Patients	Sensors
1	1	1	1–10
2	1	3	1–10
3	3	3	10

The network setup has been constructed under three varying network scenarios which consist of varying set of medical experts, patients and sensors installed in order to measure the performance of the proposed scheme. The proposed scheme has utilized a few values mentioned in [68] order to perform the execution. The setup has been made in such a way that the network consists of a user who sends packets for every five seconds with messages of varying bit size ranging from 320,

Table 9 Execution analogy of the proposed scheme vs other chosen schemes

Methodology	Signing cost (i)	Verification cost (ii)	Aggregation cost (per 100 messages) (iii)	Aggregate verification cost (per 100 messages) (iv)	Total cost (ms)	Performance increment (%)
Shen et al. [33]	$3\ T_{\_\mathrm{BPSM}} + T_{\_\mathrm{BPAO}} + T_{\_\mathrm{MPT}_H} \approx$ 9.54 ms	$3T_{\mathrm{BPF}} + 2T_{\_\mathrm{MPT}_H} \approx$ 21.44 ms	$3n\ T_{\mathrm{BPF}} + T_{\_\mathrm{BPSM}} + (n-1)T_{\_\mathrm{BPAO}} \approx 424$ ms	$3n\ T_{\mathrm{BPF}} + T_{\_\mathrm{BPSM}} + (n-1)T_{\_\mathrm{BPAO}} \approx 424$ ms	847	83
Shuai et al. [47]	$9\ T_{\_\mathrm{Oh}} \approx 10.107$ ms	$12\ T_{\_\mathrm{Oh}} \approx 13.476$ ms	$6n\ T_{\_\mathrm{Oh}} \approx 6.738$ ms	$27\ nT_{\_\mathrm{Oh}} \approx 30.321$ ms	30.321	23
Zhang et al. [48]	$T_{\mathrm{BPF}} + T_{\_\mathrm{BPSM}} + T_{\_\mathrm{Oh}} \approx$ 5.853 ms	$T_{\mathrm{BPF}} + 2T_{\_\mathrm{BPSM}} + T_{\_\mathrm{Oh}} \approx$ 7.483ms	$nT_{\mathrm{BPF}} + 2nT_{\_\mathrm{BPSM}} + nT_{\_\mathrm{Oh}} \approx$ 7.87 ms	$nT_{\mathrm{BPF}} + 2nT_{\_\mathrm{BPSM}} + nT_{\_\mathrm{Oh}} \approx$ 7.87 ms	7.87	89
Ryu et al. [49]	$14\ T_{\_\mathrm{Oh}} \approx 14.123$ ms	$14\ T_{\_\mathrm{Oh}} \approx 14.123$ ms	$14\ nT_{\_\mathrm{Oh}} \approx 14.123$ ms	$14\ nT_{\_\mathrm{Oh}} \approx 14.123$ ms	14.123	50
Peng et al. [52]	$9\ T_{\_\mathrm{Oh}} \approx 10.107$ ms	$10\ T_{\_\mathrm{Oh}} \approx 11.23$ ms	$4\mathrm{n}\ T_{\_\mathrm{Oh}} \approx 4.492$ ms	$23\ nT_{\_\mathrm{Oh}} \approx 25.829$ ms	25.829	27
Proposed	$T_{\_\mathrm{EC-SM}} + T_{\_\mathrm{EC-A}} + T_{\_\mathrm{oh}} \approx$ 3.753 ms	$3\ T_{\_\mathrm{EC-SM}} + T_{\_\mathrm{EC-A}} + T_{\_\mathrm{oh}} \approx 7.013$ ms	$3\mathrm{n}\ T_{\_\mathrm{EC-SM}} + n\ T_{\_\mathrm{EC-A}} + n\ T_{\_\mathrm{oh}} \approx 7.013$ ms	$(3n)T_{\_\mathrm{EC-SM}} + (n)\ T_{\_\mathrm{EC-A}} + (n)\ T_{\_\mathrm{oh}} \approx 7.013$ ms	7.013	–

Table 10 Analogy of cost of communication

Methodology	Communication cost (bits)
Shen et al. [33]	1024
Shuai et al. [47]	574
Zhang et al. [48]	1524
Ryu et al. [49]	3872
Peng et al. [52]	1656
Proposed	520

440, 520, and 680 bits. Table 9 provides execution analogy of the proposed scheme Vs other chosen schemes. Table 10 gives analogy of cost of communication.

(i) Packet delivery ratio (PDR)
Packet delivery ratio can be defined the number of messages received to that of the sent. It is utilized to assess the performance aspects of the network. From Fig. 9 it is evident that the packet delivery ratio increase with decrease in the number of nodes and vice versa. When the scenario becomes dense is frequent where congestion might occur. Table 11 comparison of the security features of the proposed Vs other schemes. Also, when the distance between the nodes is far, the packet may get lost. Hence the graph grows and then falls. Packet delivery ratio can be calculated by using Eq. (14) as follows:

$$\text{Packet Delivery Ratio}(\%) = \frac{\text{Number of packets received}}{\text{Number of packet sent}} * 100 \tag{14}$$

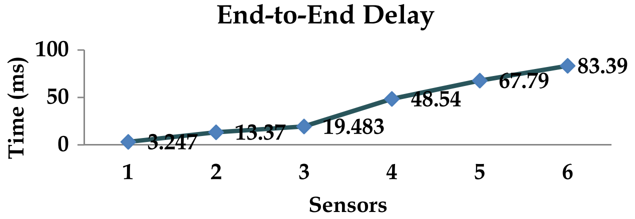

Fig. 11 End-to-end delay for our proposed scheme

(ii) Throughput
Throughput can be defined as the number of messages or packets transmitted per second. It is measured in terms of bits per second (bps). It can be calculated by using Eq. (15). The proposed scheme possesses no varying since the number of sensors and data exchanged are quite lower. Throughput becomes high in case of dense environments. Figure 10 presents the overview of throughput exhibited by our proposed scheme.

$$\text{Throughput (bps)} = \frac{\sum_{i=1}^{n} \text{Packets received}|T_i}{\text{Time Taken}} \tag{15}$$

(iii) End-to-end delay
End-to-End delay can be defined as the average time taken by the transmitted packets from the source to that of the destination. From Fig. 11, it is evident that as the distance between the sensors decreases the end-to-end delay gets higher and vice versa. Throughput can be

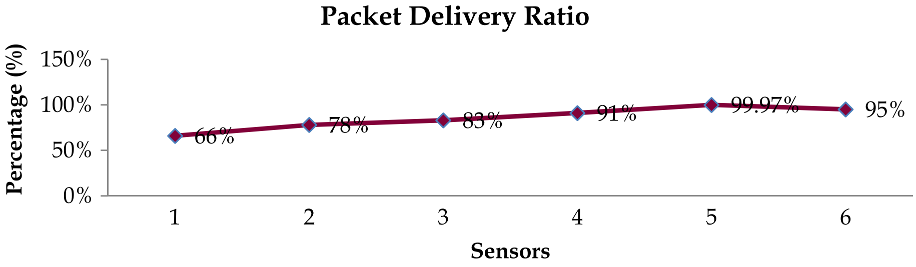

Fig. 9 Packet delivery ratio of our proposed scheme

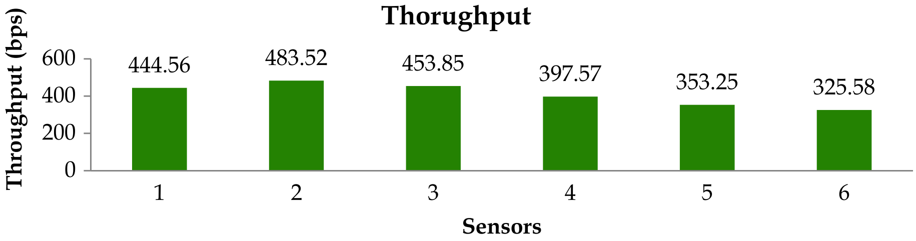

Fig. 10 Throughput for our proposed scheme

Table 11 Comparison of the security features of the proposed vs other schemes

Security feature	Shen et al. [33]	Shuai et al. [47]	Zhang et al. [48]	Ryu et al. [49]	Peng et al. [52]	Proposed
Integrity	✓	✓	✓	✓	☒	✓
Authentication	✓	✓	✓	✓	✓	✓
Anonymity	✓	✓	✓	✓	✓	✓
Traceability	✓	✓	✓	☒	☒	✓
Revocability	✓	☒	☒	☒	☒	☒
Unlinkability	✓	☒	✓	✓	✓	✓
Key Escrow	☒	☒	☒	☒	☒	✓
Impersonation	✓	✓	✓	✓	✓	✓
Modification	☒	☒	☒	✓	✓	✓
Masquerading	☒	☒	☒	☒	✓	✓
Replay	✓	✓	✓	✓	✓	✓
Man-in-the-Middle	☒	✓	✓	✓	✓	✓
Denial-of-Service	☒	☒	☒	✓	☒	✓

defined by Eq. (16) as follows:

$$\text{End - to - end Delay} = \sum_{i=1}^{n} \frac{\text{Packets transmitted } \{\text{Destination} - \text{Source}\}}{N} \tag{17}$$

8 Conclusion and future work

In this paper, a full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks has been presented. Data once generated by the medical sensors implanted on the patient body are supposed to be authenticated prior to transmission. Privacy of the patient health information is an additional requirement that has to be addressed. The schemes proposed based on bilinear pairing, elliptic curves and XoR operations are highly susceptible to a wide variety of security and privacy attacks such as computation, communication overhead, increase in the length of the signature and insecure without any secret generating mechanism. Hence in order to provide a better trade-off between these requirements the proposed scheme is more efficient. It is evident that the proposed system exhibits only less communication, computation costs. It is also true that majority of the schemes do not support autonomy, location privacy and distribution which gives a lead to the design of our proposed scheme. Our proposed scheme outperforms the chosen benchmarks in terms of computation and communication costs and is resilient toward a variety of attacks. The proposed scheme is lightweight since it uses one way generic hash function and elliptic curve cryptography and achieves full privacy preservation in distributed batch-based verification.

Artificial intelligence-based security and privacy-based methods provides a viable solution by predicting the diagnosis of the patients [69]. Prediction is also possible and disease can be detected at an early stage. This technology will erase the burden of the clinical medical expert in detecting the diseases and preventing it from next door infection [43]. Also use of blockchain will facilitate more security and privacy by providing the immutability to the data [70]. Scalability and authentication for image medical data are also a concern which is supposed to be addressed in our future work.

Acknowledgements Not applicable.

Author's contributions OBJR and TH contributed to data curation and methodology; SS and GBM contributed to writing original draft; supervision; project administration; conceptualization; and overall review and editing. AMA and MU contributed to validation; visualization; and resources. All authors reviewed the final manuscript.

Funding This project was funded by the Deanship of Scientific Research (DR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia has funded this project, under Grant No. (RG-9-611-43). The authors, therefore, acknowledge with thanks DSR for technical and financial support.

Data availability The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Declarations

Conflict of interests The authors declare that they have no competing interests.

References

1. Wail Nourildean, S., Mohammed Salih, A.: Internet of things based wireless sensor network—WiFi coexistence in medical applications. In: 2022 8th International Engineering Conference on Sustainable Technology and Development (IEC), pp. 1–6 (2022). https://doi.org/10.1109/IEC54822.2022.9807574
2. Shakeri, M., Sadeghi-Niaraki, A., Choi, S.M., Riazul Islam, S.M.: Performance analysis of IoT-based health and environment WSN deployment. Sensors (Switzerland) **20**(5923), 1–22 (2020)
3. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw.. Netw. **54**(15), 2787–2805 (2010)
4. Wagh, S.S., More, A., Kharote, P.R.: Performance evaluation of IEEE 802.15.4 protocol under coexistence of WiFi 802.11b. Procedia Comput. Sci. **57**, 745–751 (2015). https://doi.org/10.1016/j.procs.2015.07.467
5. Fotouhi, H., Cauevic, A., Lundqvist, K., Björkman, M.: Communication and security in health monitoring systems—a review. In: IEEE 40th Annual Computer Software and Applications Conference (COMPSAC) pp. 545–554 (2016)
6. Yuce, M.R., Ng, S.W.P., Myo, N.L., Khan, J.Y., Liu, W.: Wireless body sensor network using medical implant band. J. Med. Syst. **31**(6), 467–474 (2007)
7. Saeed, M.E.S., Liu, Q.-Y., Tian, G.Y., Gao, B., Li, F.: Remote authentication schemes for wireless body area networks based on the Internet of Things. IEEE Internet Things J. **5**(6), 4926–4944 (2018)
8. Crosby, G.V., Ghosh, T., Murimi, R., Chin, C.A.: Wireless body area networks for healthcare: a survey. Int. J. Ad Hoc Sensor Ubiquitous Comput. **3**(3), 1–26 (2012)
9. Khadidos, A.O., Shitharth, S., Khadidos, A.O., Sangeetha, K., Alyoubi, K.H.: Healthcare Data security using IoT sensors based on random hashing mechanism. J. Sens. vol. 2022, Article ID 8457116, 17, 2022. https://doi.org/10.1155/2022/8457116
10. Chaudhry, S.A., Mahmood, K., Naqvi, H., Khan, M.K.: An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. J. Med. Syst. **39**(11), 1–12 (2015)
11. Chennam, K.K., Aluvalu, R., Shitharth, S.: An authentication model with high security for cloud database. In: Architectural Wireless Networks Solutions and Security Issues, Lecture Notes in Network and Systems, Springer, Berlin, vol. 196(1), pp. 13–26 (2021). https://doi.org/10.1007/978-981-16-0386-0_2
12. Singla, R., Kaur, N., Koundal, D., Bharadwaj, A.: Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. Wireless Pers. Commun.Commun. **122**(2), 1767–1806 (2022)
13. Zandesh, Z., Ghazisaeedi, M., Devarakonda, M.V., Haghighi: Legal framework for health cloud: A systematic review. Int. J. Med. Informatics **132**, 103953 (2019)
14. Altamimi, A.M.: Security and privacy issues in eHealthcare systems: Towards trusted services. Int. J. Adv. Comput. Sci. Appl.Comput. Sci. Appl. **7**(9), 229–236 (2016)
15. Sarkar, A., Chatterjee, S.R., Chakraborty, M.: Role of cryptography in network security. In: The" Essence" of Network Security: An End-to-End Panorama, pp. 103–143. Springer, Singapore (2021)
16. Wu, L., Du, X., Guizani, M., Mohamed, A.: Access control schemes for implantable medical devices: A survey. IEEE Internet Things J. **4**(5), 1272–1283 (2017)
17. Kumar, P., Kumari, S., Sharma, V., Li, X., Sangaiah, A.K., Islam, S.H.: Secure CLS and CL-AS schemes designed for VANETs. J. Supercomput.Supercomput. (2018). https://doi.org/10.1007/s11227-018-2312-y
18. Raya, M., Hubaux, J.P.: The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 11–21. Alexandria, VA, USA (2005)
19. Divakaran, J., Prashanth, S.K., Mohammad, G.B., Shitharth, Mohanty, S.N., Arvind, C., Srihari, K., Abdullah, R.Y., Sundramurthy, V.P., Shitharth, S., et al.: Improved handover authentication in fifth-generation communication networks using fuzzy evolutionary optimisation with nano core elements in mobile healthcare applications. J. Healthc. Eng. Hindawi (2022). https://doi.org/10.1155/2022/2500377
20. Lu, R., Lin, X., Zhu, H., Ho, P., Shen, X.: ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: IEEE INFOCOM 2008—the 27th Conference on Computer Communications, Phoenix, AZ, USA (2008). https://doi.org/10.1109/INFOCOM.2008.179
21. Ogundoyin, S.O.: An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks. Int. J. Comput. Appl. Comput. Appl. (2018). https://doi.org/10.1080/1206212X.2018.1477320
22. Ismail, S., Tahat, N.M.F., Ahmad, R.R.: A new digital signature scheme based on factoring and discrete logarithms. J. Math. Stat. **4**(4), 222–225 (2008)
23. Lin, Q., Li, J., Huang, Z., Chen, W., Shen, J.: A short linearly homomorphic proxy signature scheme. IEEE Access **6**, 12966–12972 (2018)
24. Shamir, A.: Identity-based cryptosystem and signatures schemes. In: Blakley, G.R., Chaum, D. (eds.) Advances in cryptology. CRYPTO 1984. LNCS 196, pp. 47–53. Springer, Berlin (1984)
25. Al-Riyami, S.S., Paterson K.G.: Certificate-less public key cryptography. In: Proceedings of the International Conference on theory and Application of Cryptology and Information Security, pp. 452–473, Springer, Taipei, Taiwan, November 2003
26. Shitharth, S., Manoharan, H., Khadidos, A.O., Shankar, A., Maple, C., Khadidos, A.O., Mumtaz, S.: Improved security for multimedia data visualization using hierarchical clustering algorithm. ACM Trans Multimedia Comput. Commun. Appl. Just (2023). https://doi.org/10.1145/3610296
27. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. Comput. **48**(177), 203–209 (1987)
28. Miller, V.: Use of elliptic curves in cryptography. In: Proceedings in Advances in Cryptology (Crypto), pp. 417–426 (1985)
29. Ali, I., Chen, Y., Ullah, N., Kumar, R., He, W.: An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. IEEE Trans. Veh. Technol. Veh. Technol. **70**(2), 1278–1291 (2021)
30. Castro, R., Dahab, R.: Efficient certificate-less signatures suitable for aggregation. IACR Cryptology 2007. https://eprint.iacr.org/2007/454.pdf
31. Vallent, T.F., Hanyurwimfura, D., Mikeka, C.: Efficient certificate-less aggregate signature scheme with conditional privacy–preservation for vehicular ad hoc networks enhanced smart grid system. Sensors **21**, 2900 (2021). https://doi.org/10.3390/s21092900

32. Shen, L., Ma, J., Liu, X., Miao, M.: A provably secure aggregate signature scheme for healthcare wireless sensor networks. J. Med. Syst. **40**(11), 244 (2016)
33. Shen, L., Ma, J., Liu, X., Wei, F., Miao, M.: A secure and efficient ID based aggregate signature scheme for wireless sensor networks. IEEE Intern. Things J. **4**(2), 546–554 (2017)
34. Kumar, P., Kumari, S., Sharma, V., Sangaiah, A.K., Wei, J., Li, X.: A certificate-less aggregate signature scheme for healthcare wireless sensor network". Sustain. Comput. Inf. Syst. **18**, 80–89 (2018). https://doi.org/10.1016/j.suscom.2017.09.002
35. Wu, L., Xu, Z., He, D., Wang, X.: New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment. Secur. Commun. Netw., vol. 2018, Apr. 2018, Art. no. 2595273
36. Liu, J., Cao, H., Li, Q., Cai, F., Du, X., Guizani, M.: A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. IEEE Internet Things J. **6**(2), 1321–1330 (2019). https://doi.org/10.1109/JIOT.2018.2828463
37. Zhang, Y., Shu, J., Liu, X., Li, J., Zheng, D.: Security analysis of a large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. IEEE Intern. Things J. **6**(1), 1287–1290 (2019)
38. Xie, Y., Li, X., Zhang, S., Li, Y.: iCLAS: an improved certificateless aggregate signature scheme for healthcare wireless sensor networks. IEEE Access **7**, 15170–15182 (2019). https://doi.org/10.1109/ACCESS.2019.2894895
39. Gayathri, N.B., Thumbur, G., Rajesh Kumar, P., Rahman, M.Z.U., Reddy, P.V., Lay-Ekuakille, A.: Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks. IEEE Internet Things J. **6**(5), 9064–9075 (2019). https://doi.org/10.1109/JIOT.2019.2927089
40. Kumar, P., Kumari, S., Sharma, V., Li, X., Kumar, S.A., Islam, S.K.H.: Secure CLA and CL-AS schemes designed for VANETs. J. Supercomput. Supercomput. **75**, 3076–3098 (2019). https://doi.org/10.1007/s11227-018-2312-y
41. Zhong, H., Han, S., Cui, J., Zhang, J., Xu, Y.: Privacy-preserving authentication scheme with full aggregation in VANET. Inf. Sci. **476**, 211–221 (2019)
42. Alhalabi, W., Al-Rasheed, A., Manoharan, H., Alabdulkareem, E., Alduailij, M., Alduailij, M., Selvarajan, S.: Distinctive measurement scheme for security and privacy in internet of things applications using machine learning algorithms. Electronics **12**, 747 (2023). https://doi.org/10.3390/electronics12030747
43. Kamil, I.A., Ogundoyin, S.O.: An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. J. Inf. Secur. Appl. **44**, 184–200 (2019)
44. Zhao, Y., Hou, Y., Wang, L., Kumari, S., Khan, M.K., Xiong, H.: An efficient certificateless aggregate signature scheme for the Internet of Vehicles. Trans. Emerg. Telecommun. Technol. **31**, 1–20 (2020). https://doi.org/10.1002/ett.3708
45. Mei, Q., Xiong, H., Chen, J., Yanng, M., Kumari, S., Khan, M.K.: Efficient certificateless aggregate signature with conditional privacy preservation in IoV. IEEE Syst. J. Early. Accessed 25 Feb 2020 https://doi.org/10.1109/JSYST.2020.2966526
46. Xu, Z., He, D., Kumar, N., Choo, K.-K.R.: Efficient certificateless aggregate signature scheme for performing secure routing in VANETs. Security Commun. Netw., vol. 2020, Feb. 2020, Art. No. 5276813
47. Shuai, M., Xiong, L., Wang, C., Yu, N.: Lightweight and privacy-preserving authentication scheme with the resilience of desynchronisation attacks for WBANs. IET Inf. Secur. Secur. **14**(4), 380–390 (2020). https://doi.org/10.1049/iet-ifs.2019.0491
48. Zhang, J., Zhang, Q., Li, Z., Lu, X., Gan, Y.: A lightweight and secure anonymous user authentication protocol for wireless body area networks. Secur. Commun. Netw. 2021, Article ID 4939589, (2021). https://doi.org/10.1155/2021/4939589.
49. Ryu, H., Kim, H.: Privacy-preserving authentication protocol for wireless body area networks in healthcare applications. Healthcare **9**, 1114 (2021). https://doi.org/10.3390/healthcare9091114
50. Jegadeesan, S., Azees, M., Ramesh Babu, N., Subramaniam, U., Almakhles, J.D.: EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access **8**, 48576–48586 (2020). https://doi.org/10.1109/ACCESS.2020.2977968
51. Shuai, M., Liu, B., Yu, N., Xiong, L., Wang, C.: Efficient and privacy-preserving authentication scheme for wireless body area networks. J. Inf. Secur. Appl. **52**, 102499, ISSN 2214-2126. (2020) https://doi.org/10.1016/j.jisa.2020.102499
52. Selvarajan, S., Srivastava, G., Khadidos, A.O., Khadidos, A.O., Baza, M., Alsheri, A., Chun-Wei Lin. J.: An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J. Cloud Comput. 12–38 (2023)
53. Ji, S., Gui, Z., Zhou, T., Yan, H., Shen, J.: An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services. IEEE Access **6**, 69603–69611 (2018). https://doi.org/10.1109/ACCESS.2018.2880898
54. Mandal, S.: Provably secure certificateless protocol for wireless body area network. Wirel. Netw. **29**, 1421–1438 (2023). https://doi.org/10.1007/s11276-022-03205-4
55. Chakravorthy, G.B., Vardhan, R.A., Shetty, K.K., Mahesh, K., Shitharth, S.: Handling Tactful data in cloud using pkg encryption technique. In: 4th Smart City Symposium, pp. 338–343 (2021) https://doi.org/10.1049/icp.2022.0366
56. Nyangaresi, V.O.: Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks. Ad Hoc Netw. **142**, 103117. ISSN 1570-8705 (2023) https://doi.org/10.1016/j.adhoc.2023.103117
57. Wu, F., Li, X., Sangaiah, A.K., Xu, L., Kumari, S., Wu, L., Shen, J.: A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Fut. Gener. Comput. Syst. **82**, 727–737, ISSN 0167-739X (2018) https://doi.org/10.1016/j.future.2017.08.042
58. Jahan, M., Zohra, F.T., Parvez, Md. K., Kabir, U., Al Radi, A.M., Kabir, S.: An end-to-end authentication mechanism for wireless body area networks, Smart Health, 2023, 100413, ISSN 2352-6483, https://doi.org/10.1016/j.smhl.2023.100413
59. Almuhaideb, A.M., Alqudaihi, K.S.: Authentication in wireless body area network: taxonomy and open challenges. J. Intern. Things JIOT **3**(4), 159–184 (2021)
60. Iqbal, Y., Tahir, S., Tahir, H., Khan, F., Saeed, S., Almuhaideb, A.M., Syed, A.M.: A novel homomorphic approach for preserving privacy of patient data in telemedicine. Sensors **22**, 4432 (2022). https://doi.org/10.3390/s22124432
61. Almuhaideb, A.M., Alghamdi, H.A.: Secure and efficient WBAN authentication protocols for intra-BAN Tier. J. Sens. Actuator Netw.Netw. **11**, 44 (2022). https://doi.org/10.3390/jsan11030044
62. Almuhaideb, A.M., Alghamdi, H.A.: Design of inter-BAN authentication protocols for WBAN in a cloud-assisted environment. Big Data Cogn. Comput. **6**, 124 (2022). https://doi.org/10.3390/bdcc6040124
63. Kshirsagar, P.R., Manoharan, H., Alterazi, H.A., Alhebaishi, N., Rabie, O.B.J., Shitharth, S.: Construal attacks on wireless data storage applications and unraveling using machine learning algorithm. J. Sens. vol 2022, Article ID 8457116, 17 pages, 2022. https://doi.org/10.1155/2022/9386989
64. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptol. Cryptol. **13**(3), 361–396 (2000)
65. Khan, M.A., Ullah, I., Alsharif, M.H., Alghtani, A.H., Aly, A.A., Chen, C.-M.: An efficient certificate-based aggregate signature scheme for internet of drones. Secur. Commun. Netw. vol. 2022, Article ID 9718580. https://doi.org/10.1155/2022/9718580

66. Khadidos, A.O., Shitharth, S., Manoharan, H., Yafoz, A., Khadidos, A.O., Alyoubi, K.H.: An intelligent security framework based on collaborative mutual authentication model for smart city networks. In: IEEE Access (2022) https://doi.org/10.1109/ACCESS.2022.3197672
67. Shamus Software Ltd. MIRACL Library. Accessed: Jan. 2019. [Online]. Available: http://www.shamus.ie/index.php?page=home
68. Tian, L., Deronne, S., Latré, S., Famaey, J.: Implementation and validation of an IEEE 802.11 ah module for ns-3. In: Proceedings of the Workshop on Ns-3, ACM, 2016, pp. 49–56
69. Selvarajan, S., Mouratidis, H.: A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Sci. Rep. **13**(1), 7107 (2023). https://doi.org/10.1038/s41598-023-34354-x
70. Mirza, O.M., Mujlid, H., Manoharan, H., et al.: Mathematical framework for wearable devices in the internet of things using deep learning. In: Diagnostics, MDPI (2022). https://doi.org/10.3390/diagnostics12112750
71. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proc. R. Soc. Lond. A Math. Phys. Sci. Lond. A Math. Phys. Sci. **426**, 233–271 (1989)
72. https://www.oracle.com/a/ocom/docs/engineered-systems/database-appliance/oda-x9-2-ha-datasheet.pdf

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.