electronics

Article

Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT

B. D. Deebak and Seong Oun Hwang *

Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea
* Correspondence: sohwang@gachon.ac.kr

Abstract: The social Internet of Medical Things (S-IoMT) highly demands dependable and non-invasive device identification and authentication and makes data services more prevalent in a reliable learning system. In real time, healthcare systems consistently acquire, analyze, and transform a few operational intelligence into actionable forms through digitization to capture the sensitive information of the patient. Since the S-IoMT tries to distribute health-related services using IoT devices and wireless technologies, protecting the privacy of data and security of the device is so crucial in any eHealth system. To fulfill the design objectives of eHealth, smart sensing technologies use built-in features of social networking services. Despite being more convenient in its potential use, a significant concern is a security preventing potential threats and infringement. Thus, this paper presents a lightweight two-factor authentication framework (L2FAK) with privacy-preserving functionality, which uses a mobile sink for smart eHealth. Formal and informal analyses prove that the proposed L2FAK can resist cyberattacks such as session stealing, message modification, and denial of service, guaranteeing device protection and data integrity. The learning analysis verifies the features of the physical layer using federated learning layered authentication (FLLA) to learn the data characteristics by exploring the learning framework of neural networks. In the evaluation, the core scenario is implemented on the TensorFlow Federated framework to examine FLLA and other relevant mechanisms on two correlated datasets, namely, MNIST and FashionMNIST. The analytical results show that the proposed FLLA can analyze the protection of privacy features effectively in order to guarantee an accuracy ≈89.83% to 93.41% better than other mechanisms. Lastly, a real-time testbed demonstrates the significance of the proposed L2FAK in achieving better quality metrics, such as transmission efficiency and overhead ratio than other state-of-the-art approaches.

Keywords: Internet of Medical Things; eHealth; two-factor authentication; federated learning; learning analysis; device protection; transmission efficiency

check for updates

Citation: Deebak, B.D.; Hwang, S.O. Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT. *Electronics* **2023**, *12*, 1250. https://doi.org/10.3390/electronics12051250

Academic Editors: Lixin Wang, Jianhua Yang, Sukjin Lee and Qiang Ye

Received: 21 December 2022
Revised: 2 March 2023
Accepted: 3 March 2023
Published: 5 March 2023

1. Introduction

The recent advances in algorithms and hardware have led to massive computation and memory costs for the development of user authentication models using various multimodal AI. Commercial devices including infotainment systems adopt machine learning-based authentication features to unlatch the system process or to provide a few user-specific services, namely, recommendation, notification, and configuration adjustment. The features of the authentication protocol rely on a decision-making problem that uses a set of testing inputs to accept or reject based on its similarity measurement to train the user inputs [1]. The similarity measurement is often assessed using an embedded spacing to predict the testing input referring to learning models with the local computing data. The authentication models utilize a variety of computing data to learn the security characteristics of the physical layer [2]. The raw inputs and embedded spacing address the issues of privacy sensitivity to analyze the modeling characteristics of application systems and test the adversarial settings to protect data privacy over the inference-time attack [3].

Most distributed services use telecommunication technologies and IoT devices to store and analyze the physiological or behavioral characteristics of digital applications. The behavioral characteristics including irises, palm prints, and fingerprints extract the layered features of the computing devices using spatial correlation (i.e., channel impulse response and state information) to authenticate users and computing devices. The health insurance portability and accountability act (HIPAA) was developed by the United States to protect the sensitive information of the patient and provide the accessing rules to authorize system information [4]. The computing system demands service authentication and access control to authorize user credentials aligned with the records available on the server. The loss of data protection allows intruders to acquire sensitive information via unauthorized access to arise cybersecurity risks and gain access to confidential data via malicious IoT applications [5]. Moreover, inappropriate security practices cannot endorse a network policy without adequate controls to evaluate the shared security model across the physical and virtualized infrastructure.

As a result, security infrastructure integrates cloud computing, mobile communication, and artificial intelligence to create an innovative IoT application that successfully transfers different kinds of real-time data between the computing devices to operate the industrial process to a larger extent [6]. The massive amount of computing data generated by IoT devices necessitates more efficient data collection and processing to conduct proper development processes and adopt technological paradigms such as transfer learning and mobile computing to manage edge intelligence controlled by industrial applications. Industrial applications converge with edge networks to meet a basic constraint of strong computation in order to evaluate a large set of real-time data. In other words, the modeling process uses an edge cache to boost the performance of IoT-based networks which develop a trustworthy platform based on physical-layer data extracted from user behavior to design a secure authentication [7]. The context-aware authentication leverages biometric or physical-layer features to protect massive private data and leverage the use of machine learning to achieve reliable communication in a smart environment.

In the smart environment, a new computing paradigm, the so-called massive IoT, has evolved as a leveraging technology for the growth of digital transformation such as smart cities, automation, grids, and eHealth. The leveraging technologies revolutionize the significance of smart computing to offer a real-time awareness of the application systems. Connected edge devices can be tightly coupled with unconnected smart objects to offer data sharing, device coordination, and resource utilization [8]. An IoT environment consists of distributed sensors and actuators to gather environmental information via dedicated wireless channels. It may even route sensitive information via trusted gateways to improve the performance of computing resources. According to a report by International Data Corporation, the IoT is expected to connect 41 billion devices by 2025 [9]. It can generate massive amounts of sensitive data totaling approximately 79.4 zettabytes to utilize resources effectively. As a result, a two-fold development strategy is applied to achieve device integrity and security efficiency. Since each IoT device has limited computational capabilities, securing user credentials is still a challenging task in protecting transmitted data against threats such as unlawful eavesdropping, unauthorized access, and data tampering [10].

In real time, malicious attackers attempt to insert, delete, and modify the sensitive data of legitimate users. Therefore, a proper authentication technique is preferred to improve the security efficiency of IoT frameworks. Moon et al. [11] outlined the essential factors of an authentication mechanism to claim device integrity and application security. Saqib et al. [12] devised a secure mutual authentication framework to improve the security features of IoT environments. In addition, security features such as availability, integrity, and confidentiality are quietly surveilled to resist potential attacks with less computation and communication overhead. To improve system efficiencies, researchers apply artificial intelligence in developing various distributed IoT applications. Most distributed IoT applications use metaheuristic approaches to optimize resource utilization. Heuristic algorithms employ a proven genetic process to design an intelligent framework that applies cryptographic algorithms to improve searching efficiency. Most IoT devices apply cryptographic algorithms to offer seamless connectivity when accessing cloud-based computing resources and communication services [13].

The cloud-based computing services employ machine and deep learning algorithms to extract hidden patterns to maintain a large amount of IoT data in smart healthcare [14]. Healthcare can discover the hidden pattern using graph analytics to relate the connection between the data points and organize the associated rules to manage learning databases based on predictive modeling. The modeling applies the distributed learning algorithms via a centralized database to train the computing data using context-aware rules to improve the decision-making process [15]. However, the centralized database addresses various challenging issues such as increased latency, single point of failure, and security deficiencies leveraged by a dynamic environment. In this environment, the learning database is centrally located to generate the rules based on distributed learning to train the computing data stored in a diverse location. The machine and deep learning algorithms access the computing data across diverse locations to train the learning rules and increase the overall efficiency of the healthcare system using distributed ML [16]. Traditional machine and deep learning algorithms persist with the issue of device privacy. As a result, the algorithm cannot generalize the performance of modeling with a large amount of sensitive data to secure a deep-rooted infrastructure with advanced healthcare applications [17].

The performance modeling utilizes federated learning to train the sensing data located across diverse devices such as wearable health monitors, security systems, and logistic tracking [18]. The IoT device uses federated learning to compute or learn the generated source using scalable machine learning to improve prediction accuracy with guaranteed system latency. The personalized applications simplify the access control of the computing systems to protect user credentials using static authentication [19]. However, static authentication is susceptible to a key impersonation attack, which allows a computing device to impersonate as an illegal entity to authenticate the service access. Therefore, healthcare applications prefer distributed machine learning, so-called federated learning, to analyze the key features of the authentication protocol [20]. The application system is designed with the components of a digitized network such as control, communication, and sensing to manage the computing tasks with the social Internet of Medical Things (Social IoMT). The social IoMT distributes the application features of resource management to establish secure communication with medical devices.

1.1. Technological Advancements

Healthcare application uses a machine learning algorithm to offer a promising solution to relate the key features of the authentication protocol [21]. The features utilize a few significant tools of the learning algorithm to handle data extraction more reliably and train the extraction pattern to correlate the data points to perform cross-validation. The knowledge database constructs a protective mechanism to automate the pattern discovery to prepare a decision or prediction case that leverages the physical layer features to authenticate smart IoT devices. Moreover, smart IoT includes wireless channel characteristics such as channel state information and medical access control to analyze the physical layer features and adapt context-aware authentication within a network based on the dynamic features to improve system security [22]. The deployment of context-aware applications introduces the edge computing paradigm as a promising solution to meet the requirements of real-time services. The application service processes the raw data locally with data mining or aggregation to distribute the model gradients. The centralized server utilizes a gradient descent algorithm to preserve the privacy of localized data over different transmission stages to achieve the functionality of distributed encryption [23].

The utilization of distributed communication technologies offers seamless integration across 5G networks and IoT to discover business opportunities with edge computing [24]. Edge computing utilizes a core technology of IoT to manage the essential parts of interconnected networks. The integration of heterogeneous IoT inherits the properties of next-generation networks to meet the requirements of a communication environment such as low latency, massive connectivity, and high flow data rates [25]. However, the coexistence of multi-access techniques cannot protect network access as the time-based authentication increases its degree of network failures due to inadequate distributed machine learning models. Therefore, the emerging paradigms employ key technologies of current IoT systems to present an effective decentralized system using distributed machine learning. The learning system associates with an edge-enabled IoT network to optimize the training model and aggregate the unique identifier of the network using blockchain technology to ensure decentralization and immutability [26]. Moreover, the edge-based IoT converges with intelligence modeling to utilize three basic elements of blockchain technology including graph structure, tree, and chain.

Most application services such as healthcare, transportation, entertainment, etc., rely on a cloud-centric machine learning model to leverage the usage of smart sensing within the physical environment [27]. The application service initiates a few predefined actions to transform the physical properties into measurable signals through different sensing units. In particular, network intelligence and its advent technologies greatly expand a few machine perceptions such as image processing, pattern recognition, and computer vision to deal with detection, recognition, and navigation [9]. However, advanced networking and digital processing technologies demand an expansion of decentralization to support the growth of the modern Internet and to promote data localization and end-device portability. The key roles of the computing layers are as follows:

Cloud [Data] Center has a powerful solution to offer an intelligent infrastructure that handles huge amounts of computing services, namely, sharing, accessing, and processing the data via a well-protected data center.

Learning [Data] Center applies a decentralized machine model across edge computing systems or devices to formulate a suitable optimization problem that infers the shared knowledge of the computing devices.

Mobile [Data] Center has a technological infrastructure to provide comprehensive delivery of data packets with better visualization of information via a dedicated mobile application [28].

Communication modules such as network control and storage can interconnect with device paradigms to improve the quality of network performance. As a result, IoT devices can invoke a cloud computing model to handle a massive amount of data. A three-tier architecture, including mobile, learning, and cloud explores key features of decentralized ecosystems such as visualization, data analytics, and processing. Each ecosystem has its backbone network to access the core features of the end IoT device and to support the interconnection of baseband units using a cloud server. The IoT device integrates an edge computing paradigm to address key challenges, such as network latency, processing costs, and load balancing. Layered mechanisms, such as cloud-to-fog and fog-to-cloud processes, handle the requests of IoT devices to support mobility [29]. Parameters such as communication protocols, network types, and services offered are configured with a mobile sink to leverage the scope of network convergence. Devices such as wireless routers and machine-to-machine gateways can act as fog computing nodes to store and process data locally via dedicated cloudlets. The capabilities of cloud computing deploy intermediate nodes, which may allow end computing devices to offload network resources such as bandwidth usage and response time over the cloudlets.

A centralized cloud entity monitors the activities of geo-distributed fog servers, and a decentralized network platform between end computing devices and cloud data offers better content delivery and data analytics using a learning center [30], as shown in Figure 1. In addition, the learning center coexists with a suitable security framework to examine the core features of the computing systems which can be actively transmitted via a public network to achieve technical benefits such as privacy preservation and scalability [31].

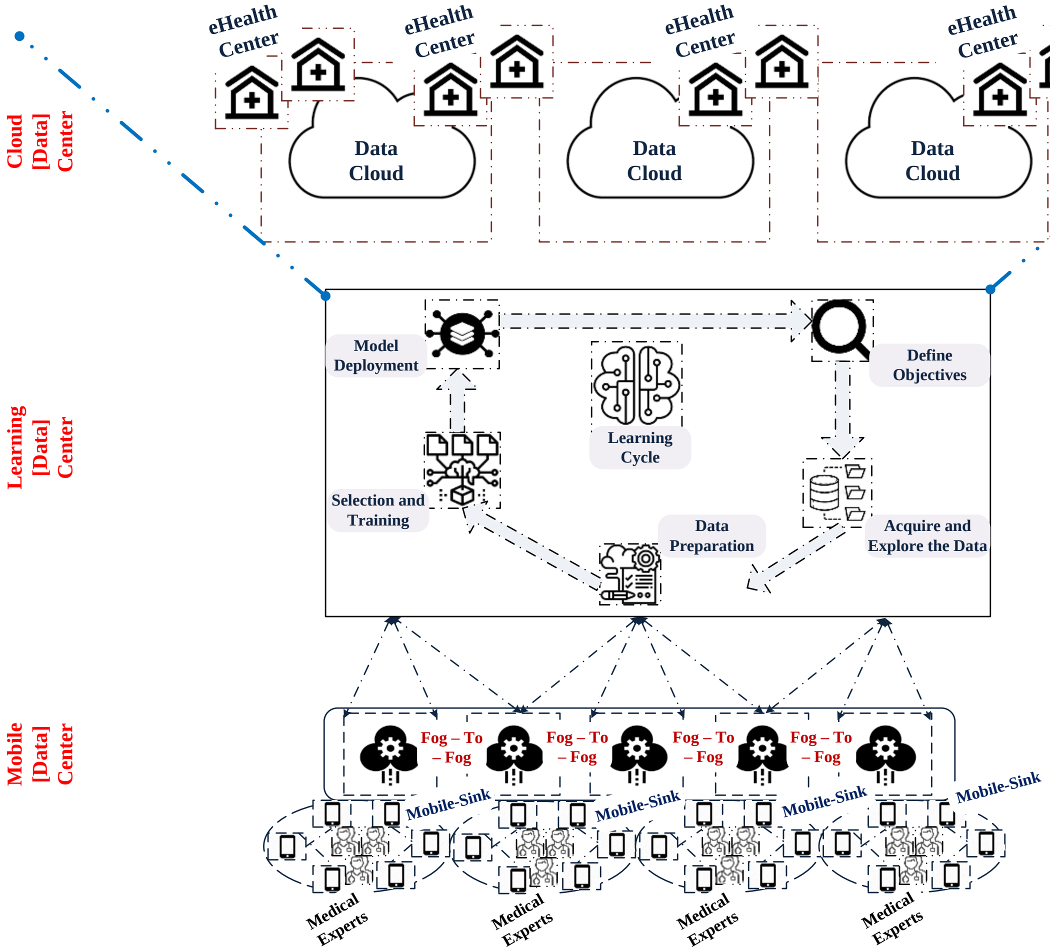


Figure 1. A Data Cloud-Centric Architecture of eHealth System Using Federated Learning Approach.

1.2. Motivation

In real time, fog computing services evolve a scenario of IoT-Cloud architecture which decentralizes the significant features, such as data processing, access control, application security, and network analytics to guarantee data integrity and security [32]. The emerging computing service enables end-user authentication to secure communication over adversarial networking devices. The enabled network gains information access to train the user modeling to learn different characteristics of user-specific services. The IoT-Cloud application uses legacy infrastructures to analyze real-time data which operates intelligent gateways to handle privacy-sensitive information of sustainable architectures [33]. In practice, the users of sustainable architecture exploit direct network access to eliminate the constraint of identity management. As a result, the architecture uses fog and cloud computing as complementary approaches to operating the connected layer with edge networks to minimize the quality issues related to cyber security and transmission latency [34]. Depending on the availability of edge-IoT devices, the generated data are transmitted to the related edge server.

To expand the storage limit horizontally and satisfy the quality requirements including delay and mobility, the network infrastructure prefers fog computing. However, fog computing cannot test any input data based on its similarity to learn the characteristics of data. Moreover, the computing paradigm cannot locate the user data centrally to train any predictive modeling due to the privacy sensitivity of any statistical database [35]. The user applications demand privacy protection to test or train any adversarial model to determine the leakage of embedding space and examine the security vulnerabilities using an authentication model. Thus, distributed machine learning, known as federated learning, is chosen to train the predictive modeling with the sensitive data of IoT devices.

This model repeatedly communicates its weights and gradients between the dedicated server and the IoT devices to maximize the predictive correlation. In federated learning, the training models enable data sharing without user preference to access the aggregated models using input–output pairs. In most cases, the input–output pairs can obtain a better user interaction to learn different data characteristics with mobile AI applications.

The application of next-generation networks interconnects with IoT devices to form intelligent networking and provide a seamless data connection to achieve better data transmission and storage [36]. Intelligent networking has the potential features such as identity, data privacy, security, and connectivity to solve the problem of data collection in a distributed machine learning technology. This technology has an extensive observation to provide technical support to secure data sharing in distributed healthcare systems. Most computing systems utilize distributed machine learning to reduce the computation complexity of a centralized database and preserve the privacy of the data owner evaluated by aggregation strategies [37]. To offer better reliability with data sharing, the modeling strategy correlates the random binary output with embedding vectors. The data protection with user privacy makes the computing device to train and upload the local model with its respective weights and gradients to the centralized server. In general, federated learning guarantees device privacy to the local data [38]. However, local training has a possibility of data leakage while the modeling parameters are uploaded into untrusted servers.

The untrusted servers utilize the modeling weights and gradients to recover the actual local data in order to observe its network structure. The initial parameter and its training labels may vary over time using adversarial techniques to disclose the private information of the social IoMT device [39]. Modern IoT demands a promising approach to examine the behavior of the computing devices based on the extraction of user profiling patterns to verify the modalities with smart medical devices. Advances in IoMT and social networks communicate with high-end computing devices to establish social links in order to process authentication requests [40]. The continuous interactions within an environment deal with supportive infrastructure to exploit the sensitive features of the information system such as identity and pattern. To overcome the security issues associated with authentication protocol, the execution trade-off considers a robust optimization approach. The optimization approach consumes less computation and communication cost to meet the desired constraints of real-time applications and expedites the process of authentication to detect malicious behavior with minimum power consumption [41].

This strategy motivates researchers to design a robust lightweight authentication with unpredictable pseudonym updates which rely on hashing and XOR operation to offer high anonymity in the social IoMT [42]. The development of computing paradigms interconnects with medical devices and healthcare providers to offer remote consultation and patient monitoring with minimum computation overload in healthcare systems. Of late, various authentication schemes have been designed using elliptic-curve cryptography (ECC) for cloud-centric eHealth systems. Jian et al. [43] designed a cloud-assisted authentication scheme using ECC to secure communication between the users and the cloud server. Yang et al. [44] utilized a secure hash function and elliptic-curve operator to design a robust authentication protocol between wearable devices and cloud servers to achieve proper mutual authentication with minimum computation cost. Izza et al. [45] devised a hybrid authentication protocol based on ECC and lightweight operations to encrypt the data features of wearable medical devices. This mechanism uses symmetric encryption to perform various computing tasks with minimum energy consumption in order to guarantee end-to-end delivery of packet transmission with reduced packet loss.

Most healthcare system applies lightweight cryptography including hash functions and XOR operation to guarantee better transmission efficiency. Alzahrani et al. [46] designed a lightweight authentication scheme for a wearable body area network that uses a hash function and XOR operation to update the device identities locally. Chunka et al. [47] constructed a hash-based authentication scheme to operate the system parameters at the end of session establishment. Wei et al. [48] devised a two-factor authentication protocol with device anonymity for a cloud computing environment. Regrettably, this scheme cannot resist a few security vulnerabilities such as user and gateway masquerading. To address security issues, this paper formulates a lightweight two-factor authentication framework (L2FAK) with the functionality of privacy preservation, which utilizes a mobile sink for smart eHealth.

1.3. Contribution

The associated technologies interconnect the computing devices with unique identities to transfer sensitive data without human intervention. The development of the S-IoMT applications handles the data traffic using the communication channel to prepare a comparative study of different network-based countermeasures including security requirements and authentication protocols. Healthcare systems operate wearable devices to collect and transmit sensitive data periodically. As a result, in healthcare, the remote monitoring system using the S-IoMT applies decentralized verification and authentication to achieve data security with secure transmission. To meet the essential requirements of the S-IoMT including session key agreement and credible mutual authentication, this paper designs a lightweight two-factor authentication framework (L2FAK). For practical uses of the S-IoMT, the proposed L2FAK includes secure data storage and transmission when facing a privileged-insider attack. The study analysis showed that the existing lightweight authentication frameworks using IoMT [49] do not have any specific strategy such as a machine learning algorithm to protect the system features; therefore, the public and private keys of the sensing units cannot be well preserved to ensure device security. The major contributions of the proposed L2FAK are as follows.

1. Use a two-factor strategy with privacy-preserving and federated learning to block potential threats such as privileged-insider and denial-of-service attacks through an authentic-ware system [15] and to analyze the data features effectively without any centralized server access.
2. Apply a secure averaging function and Boolean and Numerical (BN) responses according to source attributes of the data to update secret keys locally and to transfer the weighted parameters and their relevant gradients.
3. Design federated learning layered authentication (FLLA) which proactively manages the shared data in any social network to analyze two different datasets using the poisoning attacks. The extensive analysis utilizes the privacy features of FLLA to resist malicious behavior and guarantee better robustness and credibility.
4. Explore the layer attributes of a communication channel to extract the authentication features and enable the classification system to train the authentication process based on controlled parameters with a high-level physical layer [16].
5. A practical testbed using Raspberry Pi 3 and Arduino examines quality metrics such as transmission efficiency and overhead ratio.

1.4. Paper Organization

The remaining sections of the paper are organized as follows. Section 2 briefly describes the security efficiencies of existing authentication frameworks against threats, such as forgery, password guessing, user tracking, and perfect secrecy, to highlight the challenges of a resource-constrained IoT. Section 3 presents a smart healthcare system model that addresses two key challenges: computation and communication. Section 4 presents the phases of the proposed L2FAK and FLLA, and Section 5 discusses informal and formal security using RoR and learning analysis, offering computational analysis and reliable authentication. Section 6 presents the performance analysis using a real-time testbed, and Section 7 concludes this research work.

2. Related Works

This section discusses the issues of security frameworks, artificial intelligence, and federated learning to analyze a few crucial factors such as access rights, security, privacy, heterogeneous network, etc. Of late, the security frameworks have utilized an edge-adaptive federated learning approach for various peer-to-peer computing services. In the past decade, various system functionalities such as resource efficiency, perfect secrecy, anonymity, mutual authentication, nontraceability, revocability, and resiliency have been considered for the improvement of healthcare sectors. In the design of any secure authentication scheme, key properties such as session key agreement and mutual authentication are chiefly concerned with strengthening network performance. In recent studies, various security and privacy issues have been addressed [11–14] for significant solutions in terms of security and performance. One study revealed that cloud-centric architectures in the literature have not had enough work highlighting security and privacy issues.

Adbussami et al. [50] developed a provable lightweight authentication framework to preserve the privacy of healthcare systems. This framework uses a dedicated network architecture to explore the functional requirements of the edge computing paradigm in order to protect the privacy of the medical service provider. Kim et al. [51] constructed a lightweight authentication with anonymity preservation to protect the healthcare system against replay attacks. The anonymity preservation uses biometric-based authentication to ensure the key freshness of the message requests while integrating the gateway with medical sensors for any clinical decision. Praveen et al. [52] utilized a bioacoustics signal to design a robust secure lightweight authentication to meet the security requirements of IoMT applications including integrity, authenticity, security, and privacy. This strategy applies the Chinese Remainder Technique (CRT) to generate a group key via a protective network to validate the performance of application systems in terms of computation and communication overhead.

Chen et al. [53] intended to improve the lightweight authentication framework which uses low-power wearable sensors to analyze the key requirements of medical systems. Moreover, the lightweight framework applies biometric authentication to verify the key freshness of the message requests via a dedicated gateway. Nair et al. [54] applied a federated learning framework to construct a lightweight authentication with privacy preservation. This model adopts a strategy of big-data analytics to analyze the functionalities of multi-tier system architecture with load reduction. Gupta et al. [55] designed context-aware data authentication and access control to resist quantum attacks. The comprehensive analysis proved that context-aware authentication meets the network requirements of the IoMT networks such as anonymity, mutual authentication, and quantum security. Chatterjee et al. [56] employed a ring signature-based authentication to validate the collaborative environment of the medical system. This scheme exploits quality assessment criteria to resist the network attacks such as man-in-the-middle, denial-of-service, and privileged insider to maintain data confidentiality and integrity.

Deebak and Al-Turjman [57] formulated a single sign-on mechanism using Chebyshev chaotic map to analyze the computing services of the distributed network. This model uses a strategy of unary access control to meet the service level agreements of medical IoT systems. Dharminder et al. [58] developed an efficient authentication framework based on a Chebyshev chaotic map to protect the management systems against security vulnerabilities such as key impersonation and the privileged-insider attack. This modeling framework uses key verifiers to examine the requirements of digital systems. Dsouza et al. [59] proposed a policy-based security framework to control the flow of data transmission with multiple application domains to provide a high level of security. This framework initialized attribute-based authentication to acquire the essential criteria such as computing resources and services. The main objective is to execute computing services involving storing and processing sensitive information [60]. Shivraj et al. [61] designed a two-factor authentication using elliptic-curve cryptography (ECC) which utilizes fewer key sizes, a reliable infrastructure, and a robust testbed to analyze the core features of smart cities. However, this authentication scheme cannot be more genuine to examine the key elements of the three-tier architecture of fog computing architectures, namely, pre-processing, storage, and security.

Lu et al. [62] intended to develop a lightweight, privacy-preserving scheme to perform data aggregation in a fog computing environment. In this scheme, three basic techniques (the Chinese remainder problem, one-way hashing, and the Paillier cryptosystem) were applied to prevent data injection attacks at the edge of the network. Examination results demonstrated that this scheme can mitigate computation and communication costs to meet the standard constraints of a fog computing environment. Kumar and Gandhi [63] utilized data transport layer security to address vulnerability to denial-of-service (DoS) attacks. Their method uses a constrained application protocol to optimize deployment with a high number of computing devices. Ibrahim [64] designed a proper mutual authentication framework to explore the key functionalities of a master secret key. This scheme uses smart cards and intelligent devices to verify the identities of users who transmit sensitive data over public channels. Unfortunately, this scheme cannot achieve better device compatibility and user anonymity or lessen signal interference, to block unauthorized entities.

Amor et al. [65] designed a reliable authentication framework using a public-key cryptosystem. It uses pseudonym-based cryptography to maintain user anonymity between computing nodes and fog servers. However, this scheme cannot offer a secret session key agreement to meet the general requirements of a fog computing system. Xu et al. [66], Lee et al. [67], and Yu et al. [68] analyzed two-factor and three-factor authentication for a multi-server architecture. Watters et al. [69] implemented short messaging services to analyze key features of two-factor authentication. Test results revealed that the authentication scheme can only achieve about 76.5% accuracy in analyzing key features such as authentication and anonymity [70]. Amin et al. [71] proved that the security mechanisms of He et al. [72] and Wu et al. [73] directly contact sensors to collect or read medical data. Therefore, their schemes could not restrict offline guessing, intractability, and a privileged-insider attack. Amin et al. presented two-factor authentication specifically designed for wireless medical sensor networks (WMSN) to address those security weaknesses. However, their scheme is still susceptible to offline password guessing. Kumari et al. [74] presented a novel lightweight authentication scheme that constructs a secure session key between real-time entities. Unfortunately, their scheme could not restrict offline password guessing and user traceability.

Farash et al. [75] designed a secure authentication protocol to prevent forgery and password guessing. Cryptanalysis proved that their scheme is still susceptible to user traceability. Wu et al. [76] presented a lightweight, two-factor authentication scheme that blocks threats such as privileged-insider attacks, user nontraceability, session key disclosure, and offline password guessing. Inopportunely, their scheme could not rely on perfect secrecy. Wazid et al. [77] designed a robust authentication scheme that applies a fuzzy extractor to manage biometric mechanisms. However, their scheme fails to prevent attacks such as password guessing, user traceability, breach of anonymity, etc. Above all, most of the existing authentication schemes still find it challenging to offer better security and privacy protection [78]. Gope et al. [79] developed an authentication framework using a one-time physical unclonable function to update the challenge–response pair dynamically to prevent a machine learning attack. Jegadeesan et al. [80] devised a lightweight privacy preservation framework with anonymous authentication to resolve the issue related to response errors. Jiang et al. [81] utilized a one-way hash function and an ideal physical unclonable function to minimize the operational cost between the medical devices and the server. Table 1 summarizes the challenging issues of existing authentication schemes.

Table 1. Security and privacy challenges in existing authentication schemes.

Existing Schemes	Systematic Approach	Pros and Cons	Vulnerable To			
			Forgery	Password Guessing	User Tracking	Perfect Secrecy
He et al. [72], 2015	Cryptography Hash Function	The lightweight functions are applied to minimize the computation cost. However, this scheme cannot have any specific platform to validate the energy consumption of medical sensors.	Yes	Yes	No	No
Kumari and Om [74], 2016	Cryptography Hash Function	Two-factor authentication is utilized to reduce cost efficiencies including computation and communication. However, this protocol cannot resist forgery and password guessing to meet the requirements of wireless medical sensor networks.	Yes	No	Yes	No
Wu et al. [73], 2017	Symmetric Encryption	This scheme uses lightweight two-factor authentication to achieve the property of mutual authentication and key agreement. Despite that, this scheme cannot achieve a property of perfect secrecy to resist a forgery attack.	No	Yes	No	No
Farash et al. [75], 2017	Symmetric Encryption	This scheme uses lightweight authentication with user anonymity to achieve better computation efficiency. In spite of its conditional provable security, this scheme cannot satisfy the design goals such as forgery, password guessing, and perfect secrecy.	No	No	Yes	No
Amin et al. [71], 2018	Cryptography Hash Function	An effective architecture is designed with anonymity-preservation to claim the key features of the mutual authentication framework. Contrarily, this framework cannot resist forgery and password-guessing attacks to achieve a property of perfect secrecy.	No	No	Yes	No
Wu et al. [76], 2018	Cryptography Hash Function	This scheme utilizes lightweight authentication to guarantee the security of data transmission between the communication entities. Conversely, this authentication scheme cannot prevent the forgery attack unconditionally to meet the requirement of wireless medical sensor networks.	Partially	Yes	Partially	No

Table 1. *Cont.*

Existing Schemes	Systematic Approach	Pros and Cons	Vulnerable To			
			Forgery	Password Guessing	User Tracking	Perfect Secrecy
Wazid et al. [77], 2019	Cryptography Hash Function	Device authentication and key management are employed to secure the communication of an edge-based IoT environment. Despite that, this key management scheme cannot withstand forgery and password-guessing attacks to authenticate the cloud server mutually.	No	No	Yes	No
Deebak [78], 2020	Cryptography Hash Function	The key management scheme is designed to offer secure data transmission between computing devices. Unfortunately, this management scheme cannot achieve the property of traceability to preserve the privacy of IoT-based technologies.	Yes	Yes	No	Yes
Kalaria et al. [70], 2021	Identity-based elliptic curve cryptography	A fog-based mutual authentication framework is constructed to protect the end device against cyberattacks. However, this framework cannot resist the security vulnerabilities such as forgery and password-guessing to function the fog computing appropriately.	No	No	No	No
Deebak and Al-Turjman [57], 2021	Chebyshev Chaotic-Map-Based Single-User Sign-in	In this scheme, sensor/sensor tag-based authentication is introduced to offer security and privacy. On the contrary, this scheme cannot resist forgery and password-guessing attacks to make it more suitable for telecare medical information systems.	No	No	No	No
Dharminder et al. [58], 2021	Chebyshev Chaotic-Map	In this framework, an efficient chaotic-map based authentication is designed to ensure anonymous communication with telemedicine services. In contrast, this authentication scheme cannot fulfill the design goals of healthcare systems such as user tracking and perfect secrecy.	Yes	No	No	No

Table 1. *Cont.*

Existing Schemes	Systematic Approach	Pros and Cons	Vulnerable To			
			Forgery	Password Guessing	User Tracking	Perfect Secrecy
Proposed L2FAK and FLLA	Elliptic-curve and learning framework of neural networks	This model applies a secure averaging function and Boolean and Numerical (BN) responses according to source attributes of the data to update secret keys locally. Moreover, the model can proactively manage the shared data in any social network to protect their system parameters	Yes	Yes	Yes	Yes

3. System Model

This section provides a real-time scenario for an eHealth monitoring system offering a better quality of service and context awareness. It has a core deployment of fog and cloud network paradigms to address the challenging features of a large-scale system, such as security, scalability, heterogeneity, and programmability. The network paradigms use a distributed cloud computing model to handle data processing and to offload computing tasks to the cloud. The computing model builds an intelligent platform between the end devices and cloud data centers via authentic gateway access to examine quality metrics such as transmission efficiency and overhead ratio. The key components are as follows.

Sensing Units (IoT Devices)—Wearable sensing units collect the source medical data, such as blood pressure, heart rate, and glucose monitoring, to infer the conditional status of the patient. The application allows a medical expert to process the healthcare information of a patient via a dedicated gateway to offer better decision making.

Sink Node (Mobile Device)—A sink node can be any one of various computing nodes, such as a smart device, a microcontroller, and a sensing component to acquire and collect medical data. Most of the on-demand requests issued by end users share the healthcare information of the patient to improve the lifetime of the sensing units.

Authentic Gateway Access—The gateway acts as a reversible proxy to restrict unauthorized access and prevent suspicious activities. Moreover, it can handle authentication requests to protect the critical and sensitive information of the patient.

Cloud Server—In this framework, the cloud server acts as a semi-trusted entity to characterize the malicious behavior of the mobile device and exhibit curiosity-but-honest to deliver sufficient computing resources and data sharing between M_E/P_A and M_S. In other words, M_S cannot delete or modify the transferred data of M_E/P_A; however, M_S makes an effort to correlate the relationship between the gathered data and M_E/P_A to infer the actual data content.

Smart medical sensors are commonly implanted in or around the patient's body to read physiological data that support healthcare monitoring in real time [44]. They are more portable and smaller to provide device intercommunication. They are designed to be implanted in, or worn on, a patient's body to record vital signs such as breathing rate, heart rate, blood pressure, etc. Data communication is essential to elderly people or in an emergency situation, processing sensitive data wirelessly. It may be necessary to monitor or assess the medical situation or take immediate action to obtain proper treatment from doctors or medical experts. Figure 2 shows a model smart healthcare system with authentic gateway access. It has three real-time entities (M_E, M_D, and AG_{Access}) to handle sensitive information of patients via dedicated fog computing. Owing to limited computation resources to gather medical data, it is preferable to use lightweight cryptographic operations, including the bitwise exclusive operator and collision-resistant functions [45].

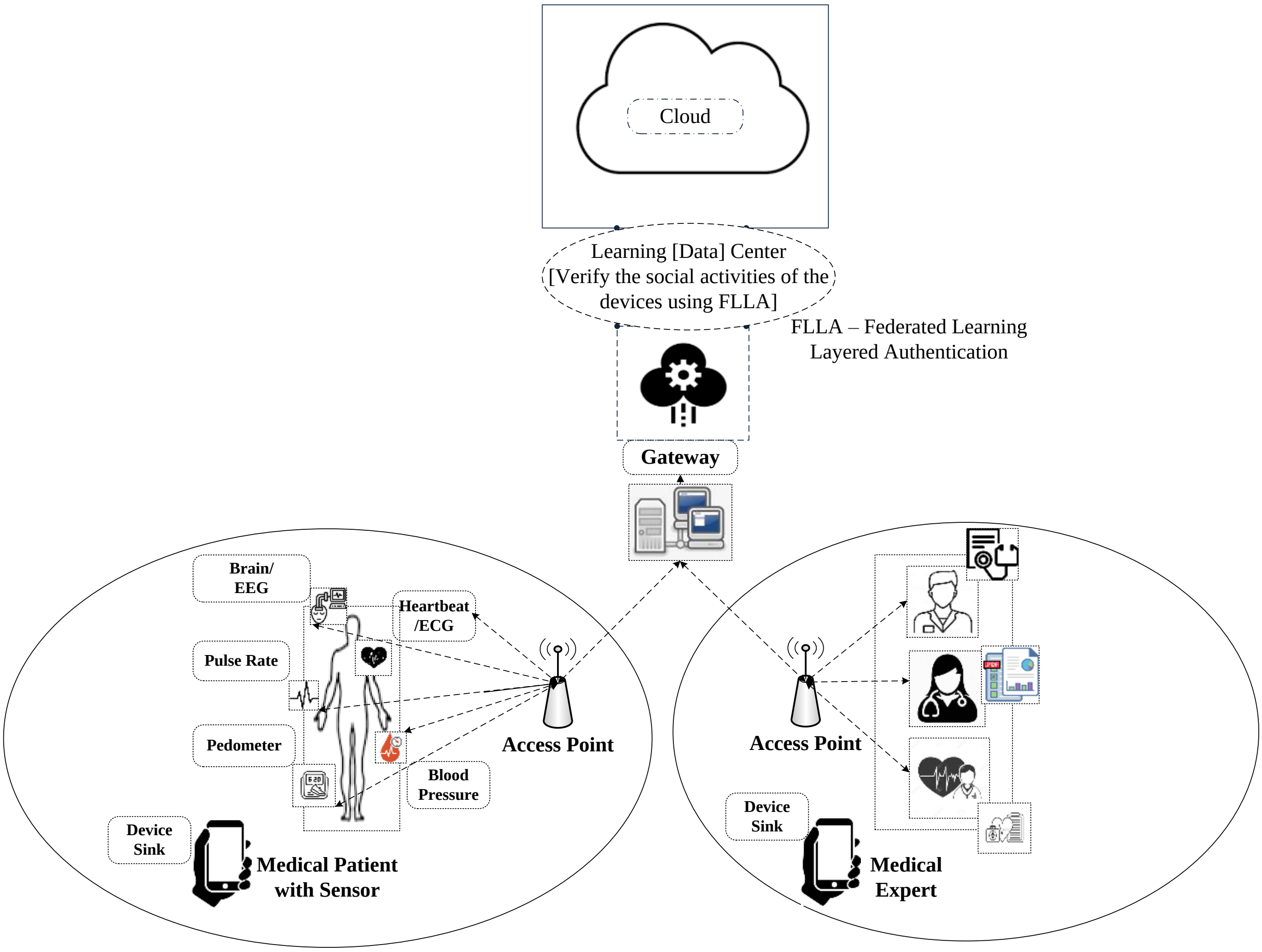

Cloud
Learning [Data] Center [Verify the social activities of the devices using FLLA]
FLLA – Federated Learning Layered Authentication
Gateway
Brain/ EEG
Heartbeat /ECG
Pulse Rate
Pedometer
Blood Pressure
Access Point
Device Sink
Medical Patient with Sensor
Access Point
Device Sink
Medical Expert

Figure 2. A Smart eHealth System Model with Authentic Gateway and Layered Authentication.

On the other hand, AG_{Access} has sufficient resources to provide a secure interface between M_D and M_E. These entities demand protected transmissions to achieve mutual authentication, data privacy, and anonymity. In addition, AG_{Access} must provide session unlinkability and nontraceability to strengthen security efficiency. Because of public network access, data transmissions are easily susceptible to severe security risks, such as replay attacks, eavesdropping, data modification, data interception, etc. Moreover, intruders or adversaries may try to launch malicious techniques such as forgery, a session key disclosure, key impersonation, privileged-insider attacks, etc. It is worth noting that the overhead constraints on medical sensors can substantially weaken system efficiency.

In the system model, the patient's condition is monitored periodically using smart sensors to assess status, including blood pressure, pulse rate, pedometer readings, etc. Smart sensors infer the medical condition of the patient through an access point. Subsequently, the inferred information is sent to the cloud via a system gateway to verify the system attributes using federated learning. The system acts as a smart entity to register the legal M_E that collects sensitive patient data to observe their physical condition. As referred to in [23], overall system costs may vary depending upon the usage of transmission bits, b_l. Moreover, communication costs may directly influence the transmission distance between sensors and the target entity. Table 2 shows the notations used under the L2FAK protocol.

Table 2. Notations Used for the L2FAK.

Parameter	Description
M_E/P_A	Medical Expert/Patient
M_D	Medical/Mobile Device
M_S	Cloud Server
D_{ID}	Identity of Medical Device
M_{id}	Identity of Medical Expert
TID_i	Temporary Pseudo-identity
AG_{Access}	Authentic Gateway Access
ID_{gw}	Gateway Identity
M_{Key}	Single Sign-on Authentication Key
S_{Key}	Secret Key
ID_{gw}	Identity of Gateway
CH	Challenge
PID_i	Pseudo-identity of M_E/P_A
SK	Session Key
$E_K(.)/D_K(.)$	Symmetric Encryption/Decryption
$H(\ .)$	One-Way Cryptographic Function
D_B	Database
A_{dv}	Adversary
F_{ID}	Fake Identities
K_P	Fake Identities of Key Pairs
S_L	Softmax Loss Function
K	Legitimate Computing Devices
Y_k	Class Label
a_k	Predicted Values of kth Computing Device
$bi_{d''}$	Model Bias
(S_V, S_W)	Sampling Vectors of the Matrix
q_l	Level of Quantization
$\hat{W}_{ij}$	Quantized Matrix
D_P	Device Prediction

Threat Model

In accordance with the system model, a formal adversarial attack is considered to assess four different types of threats which may intimidate the security efficiency of the proposed L2FAK.

Formal Security Definition: A formal security assumption is introduced with probabilistic polynomial time (PPT) to represent the behavior of malicious or revoked users. This malignant act may forge or deceive the cloud server to generate a privacy leakage [82]. Moreover, the assumption defines the security against the malicious user where an adversary with PPT AD_{PPT} is supposed to play the successive game with a competitor C.

Setup: C initiates non-identities of M_E/P_A using the proposed L2FAK. It is assumed that AD_{PPT} represents β as a non-identity of L2FAK to assess its behavior over C. As a result, C instructs β to attack the non-identity of L2FAK and utilizes the subprogram of AD_{PPT} to work over L2FAK. In addition, β as the competitor of L2FAK trains AD_{PPT} and make an effort to obtain the results of AD_{PPT} to drive an attack against the non-identity of L2FAK. Obtaining the inputs of non-identity L2FAK, C generates the parameters $SK = \left\{M_{S_i}, ps_2, ps_3, ps_4, S_{key}, H(\ .)\right\}$ and β produces the parameters $SK' = \left\{M_{S_i}, ps_2, ps_3, ps_4, S_{key}, x_1, pk_{gw}, H(\ .)\right\}$ to obtain the data content. In addition, the system parameters are processed to the adversaries β and AD_{PPT}.

Queries: The adversaries can strategically issue the data queries to C, which maintains the query lists to explore the relationship between the data or address sequences, which is initially recorded as empty, however.

(1) Hash Function $H(\ .)$: The adversary uses hash value to obtain any identity $\Im_i$. C finds w_i and returns the value to the adversary. Using this query, the adversary can obtain the parameter of any secret key S_{key}.

(2) Key: In query execution, the adversary processes the function lists $H(\ .\ )^{List}$ to the adversary. It is worth noting that $H(\ .\ )^{List}$ utilizes the hash value of $H(\ .)$ to obtain the user identities M_{id_j}. If S_{key} has not been suspected before, then C will generate a legal message request M_i. Using this query, the adversary can obtain the parameter of any S_{key} to acquire the encrypted messages.

End-Game: Lastly, the entities including adversary and competitor obtain the encrypted messages C_η^* and $C_\eta^{*'}$ respectively. If $C_\eta^* = C_\eta^{*'}$ holds, then the adversary succeeds in its computation process to derive the encrypted messages.

Definition 1. *The L2FAK protocol can be secure over forging the encrypted messages to ensure privacy preservation, even if any adversaryAD_{PPT}plays the game with the competitor to obtain a negligible probability:* $|2P_r|C_\eta^* + \left|C_\eta^{*'} - 1\right| \leq \varepsilon(\mathcal{K})$.

Four Types of Adversary Acts: To analyze the security efficiencies of the proposed L2FAK, the capabilities of an adversary AD_{PPT} are as follows.

1. AD_{PPT} may collude with multiple user entities to infer the secret key of M_E/P_A without any proper permission of M_S to gain server access.
2. M_S may be a semi-trusted cloud server to collude with revoked user entities to maintain the encrypted data without the consent of AG_{Access}. Even if the outsourced data is known to the revoked users, the semi-trusted cloud still holds the key derivatives of M_E/P_A to secure the data transmission.
3. When any user of a group tries to access the shared data, it may operate its access types in a different form to protect the content of data. Moreover, the revoked user cannot collude with the semi-trusted cloud to guess the interested information.
4. The cloud server cannot determine the significance of encrypted data content to explore its relationship with data and address sequences. In addition, the curious server can attempt to track the content of data based on the access time to determine its priority.

4. The Proposed L2FAK

This section systematically constructs the architectural processes of eHealth applications to fulfill design criteria such as confidentiality and integrity. To structure the protocol, the design is composed of four basic entities, namely, sensors, medical experts, a mobile sink, and an authentic gateway. The execution phases of the L2FAK protocol consider the following assumptions for significant roles of the real-time entities:

1. AG_{Access} assumes the role of a trusted node to establish and manage the point of service via proper authorization requests.
2. M_{key} utilizes a hardware device to generate unique passcodes among real-time entities for single sign-on authentication.
3. S_{key} uses secret key distributions to verify device identities and ensure mutual authenticity via $S_{key} = H\left(M_{key} \oplus ID_{gw}\right)$.

The L2FAK scheme is composed of four execution phases (pre-deployment, initialization, and registration, plus login and authentication) for medical-expert registration, login, authentication, and session key updates.

Phase 1—Pre-deployment: In this phase, M_E/P_A negotiates with AG_{Access} to obtain S_{key}. To be associated with a legal system, each M_D utilizes S_{key} along with information about M_E/P_A. Furthermore, it is assumed that S_{key} cannot be accessed or obtained by A_{dv}.

Phase 2—Initialization: This phase carries out systematic operations over a secure channel, sending the registration request for medical device M_D (along with its identity, D_{ID}) to server S. After receiving the request, S generates a challenge, CH, to verify the next interaction with D_{ID}. As a result, S has a series of new challenges, $CH_{SYN} = \{ch_1, ch_2, \ldots\ldots, ch_n\}$, which requires proper re-synchronization with D_{ID} to send a functional argument $\{CH, CH_{SYN}\}$ to M_D. Accordingly, M_D extracts functional outputs $R_{CH} = PUF_{ID}(CH)$ and $R_{CH-SYN} = PUF_{ID}(CH_{SYN})$ using $\{CH, CH_{SYN}\}$ to process functional parameters $\{R_{CH},\ R_{CH-SYN}\}$ with S.

To prove the legitimacy of computing device M_D, S generates first-factor authentication, including short-term identity $ST_{ID} = H\left(R_{CH} \parallel M_{key}\right)$ and a secret key, S_{key}. In addition, S finds a set of fake identities along with key pairs, $(F_{ID}, K_P) = \{(F_{ID1}, K_{P1}), (F_{ID2}, K_{P2}), \ldots\ldots, (F_{IDn}, K_{Pn})\}$, to prepare a valid argument, $\left\{\left(ST_{ID}, S_{key}\right), (F_{ID}, K_P)\right\}$, which sets up secure channel access with D_{ID}. Lastly, S stores the essential parameters, $\{(ST_{ID}, S_{key}), (CH, R_{CH}), (CH_{SYN}, R_{CH-SYN}), (F_{ID}, K_P)\}$, in its database, D_B, to verify the parameters of M_D, i.e., $\{(ST_{ID}, S_{key}), (F_{ID}, K_P)\}$.

Phase 3—Registration ($\mathrm{M_E/P_A}$): M_E/P_A deal with AG_{Access} to register credentials safely before message requests are transmitted via secure channels. The execution steps are as follows.

Step 1: M_E/P_A select their own identities, M_{id}/PA_{id}, generate a pseudo-random number, ps_1, to compute a pseudo-identity, $PID_i = H(M_{id}/PA_{id} \parallel H(ps_1))$, and then transmit PID_i to AG_{Access}.

Step 2: After receiving the parameter PID_i, AG_{Access} determines whether PID_i is already registered in D_B. AG_{Access} generates a temporary pseudo-identity, TID_i, to compute $TP_1 = H\left(TID_i \parallel x_1 \parallel ID_{gw} \parallel S_{key}\right)$ and assigns TP_1 to M_E/P_A. Subsequently, AG_{Access} stores values $\{TID_i, TP_1\}$ for M_D and allows M_E/P_A to access PID_i via D_B. Finally, AG_{Access} transmits data from medical device M_D to M_E/P_A.

Step 3: M_E/P_A set a strong password, p_{wd}, in order to compute $TP_2 = H(PID_i \parallel TID_i \parallel p_{wd})$ to protect the device credentials of M_E/P_A from A_{dv}. Later, M_E/P_A compute $TP_3 = H\left(H\left(p_{wd_i}\right) \parallel M_{id}/PA_{id}\right) \oplus H(ps_1), TP_4 = H\left(p_{wd_i} \parallel ps_1\right)$, and $TP_5 = H\left(TP_1 \parallel S_{key} \parallel PID_i\right)$ to store system parameters $\left\{TP_2, TP_3, TP_4, TID_i, S_{key}\right\}$ in M_D.

Phase 3—Registration (Sensor): Assume that a medical sensor, M_S, wishes to register with AG_{Access} via dedicated device M_D to transmit messages via secure channels.

Step 1: AG_{Access} chooses an identity, M_{S_i}, for medical sensor M_S and applies private key pk_{gw} of AG_{Access} to protect the M_S identity.

Step 2: Additionally, AG_{Access} utilizes the values of M_{S_i} and pk_{gw} to compute a pseudo-identity for M_S, i.e., $P_{M_{S_i}} = H\left(M_{S_i} \parallel pk_{gw}\right)$.

Step 3: After obtaining $P_{M_{S_i}}$, AG_{Access} sends parameters $\left\{P_{M_{S_i}}, M_{S_i}, PID_i\right\}$ to M_S and subsequently stores them in M_D via M_S to limit data access based on the characteristics and to establish secure communications with uncompromised M_S.

Phase 4—Login and Authentication: In this phase, the system can legally process message requests when M_E/P_A reviews and verifies the credibility of patient information. To gain system access, M_E/P_A enter a legible S_{key} into M_D, which authenticates the communication with M_S via AG_{Access}, as shown in Figure 3. This phase shall operate the execution steps of different communication entities M_E/P_A and M_S via AG_{Access} to exhibit the significance of secure registration and validation among the legitimate mobile/medical device M_D. Initially, S handles the registration process with M_E/P_A to verify the message requests and manage the medical devices M_D with AG_{Access} to control the system parameters. To begin with the registration process, M_D safely registers the secret key S_{key} with its trusted AG_{Access} to validate the legitimacy of the patient AG_{Access} and also generates a pseudo-random number, ps_3 to compute a legal message request M. Following this process, AG_{Access} supplies the computation parameters $\{E_1, E_2\}$ not only to enroll the medical device M_D but also to compute their signatures to advertise a secure session key SK within the medical center. The center considers a learning network to generate a local chain whereby the entities such as M_S and AG_{Access} can handle a local batch signature to create private and public slabs in order to validate the service management controlled by the inter-hospital networks. The learning network forms predictive information to validate legitimate device M_D via AG_{Access} to determine the appropriate security features including the decryption key which manages the network verification with M_S to extract the important parameter of M_D and to establish secure communication between M_E/P_A and M_S.

Step 1: M_{Ei}/P_{Ai} enter login credentials M_{idi}/PA_{idi} along with p_{wdi} via the preferred M_D to compute $H(ps_1) = H(H(p_{wdi}) \parallel M_{idi}/PA_{idi}) \oplus TP_3$. Subsequently, M_{Ei}/P_{Ai} find $PID_i = H(M_{idi}/PA_{idi} \parallel H(ps_1))$ from $H(ps_1)$ to verify whether $(H(p_{wdi}) \parallel M_{idi}/PA_{idi}) \overset{?}{\Leftrightarrow} TP_4$ is stored in M_D. After successful verification, M_E/P_A is determined to be legitimate and can successfully log in.

Then, M_{Ei}/P_{Ai} generate another pseudo-random number, ps_2, to compute $E_1 = EC_{TP_5}\left(ps_2 \parallel M_{S_i} \parallel PID_i \parallel S_{key}\right)$ and $E_2 = H\big(ps_2 \parallel M_{S_i} \parallel PID_i \parallel TP_1\big)$. Lastly, computation parameters, such as $\{E_1, E_2, TID_i\}$, are transmitted via M_D to AG_{Access}.

Step 2: AG_{Access} initially uses $TP_1 = H\big(TID_i \parallel x_1 \parallel pk_{gw}\big)$ to obtain $(ps_2 \parallel M_{S_i} \parallel PID_i \parallel S_{key}) = D_{TP_5}(E_1)$ via functional decryption. Additionally, AG_{Access} utilizes D_B to obtain the pseudo-random identities M_{idi}/PA_{idi} using $\left(ps_2 \parallel M_{S_i} \parallel PID_i \parallel S_{key}\right)$ to verify source values with E_2.

Additionally, AG_{Access} generates another pseudo-random number, ps_3, to compute $M = H\big(ps_2 \parallel M_{S_i}\big), E_3 = H\big(M \parallel M_{S_i}\big) \oplus \left(ps_2 \parallel ps_3 \parallel PID_i \parallel S_{key}\right)$, and $E_4 = H\big(M \parallel M_{S_i} \parallel ps_2 \parallel ps_3 \parallel PID_i\big)$. Finally, AG_{Access} transmits parameters $\{E_3, E_4\}$ to M_S.

Step 3: To check the legitimacy of AG_{Access} and to obtain the ps_2, ps_3, and PID_i values, M_S computes $(ps_2 \parallel ps_3 \parallel PID_i) = H\big(M \parallel M_{S_i}\big) \oplus E_3$. Furthermore, M_S determines $\big(M \parallel M_{S_i} \parallel ps_2 \parallel ps_3 \parallel PID_i\big)$ to verify values with E_4.

After successful verification, M_S generates pseudo-random number ps_4 to find $SK = H\left(M_{S_i} \parallel ps_2 \parallel ps_3 \parallel ps_4 \parallel S_{key}\right)$, which creates a random number r_l to compute $WL = EC_{GW}(r_l)$, $E_5 = H\big(M \parallel ps_3 \parallel M_{S_i} \parallel r_l\big) \oplus ps_4$, and $E_6 = H(M \parallel ps_3 \parallel ps_4 \parallel SK)$. In the end, M_S sends system parameters $\{E_5, E_6, WL\}$ to AG_{Access}.

Step 4: AG_{Access} finds $r_l = DC_{AG}(WL)$ to compute a pseudo-random number, $ps_4 = E_5 \oplus H\big(M \parallel ps_3 \| M_{S_i} \parallel r_l\big)$. Accordingly, AG_{Access} evaluates $SK = H(M_{S_i} \parallel ps_2 \parallel ps_3 \parallel ps_4 \parallel S_{key})$ to verify values with E_6.

Successful verification prompts AG_{Access} to generate a temporary identity, T_{ID}^{New}, and to compute $TP_1^{New} = H\big(T_{ID}^{New} \parallel x_1 \parallel pk_{gw}\big)$, $E_7 = EC_{TP_5}\left(ps_4 \parallel ps_3 \parallel TP_1^{New} \parallel T_{ID}^{New} \parallel S_{key}\right)$, and $E_8 = H\big(TP_1^{New} \parallel T_{ID}^{New} \parallel SK \parallel ps_3 \parallel ps_4 \parallel TP_1\big)$. Finally, AG_{Access} transmits source parameters $\{E_7, E_8\}$ to M_{Ei}/P_{Ai} via M_D.

Step 5: M_{Ei}/P_{Ai} initially decrypts E_7 using TP_5 to find the target value $(ps_4 \parallel ps_3 \parallel TP_1^{New} \parallel T_{ID}^{New} \parallel S_{key})$. By then, M_{Ei}/P_{Ai} find $SK = H\left(M_{S_i} \parallel ps_2 \parallel ps_3 \parallel ps_4 \parallel S_{key}\right)$ to verify whether the source value is similar to $H\big(TP_1^{New} \parallel T_{ID}^{New} \parallel SK \parallel ps_3 \parallel ps_4 \parallel TP_1\big)$. Eventually, M_{Ei}/P_{Ai} change TP_2 to find a new source, $TP_2^{New} = H(p_{wdi} \parallel PID_i) \oplus TP_1^{New}$, and accordingly, update source parameters $\{TP_2, TID_i\}$ with $\{TP_2^{New}, TID_i^{New}\}$.

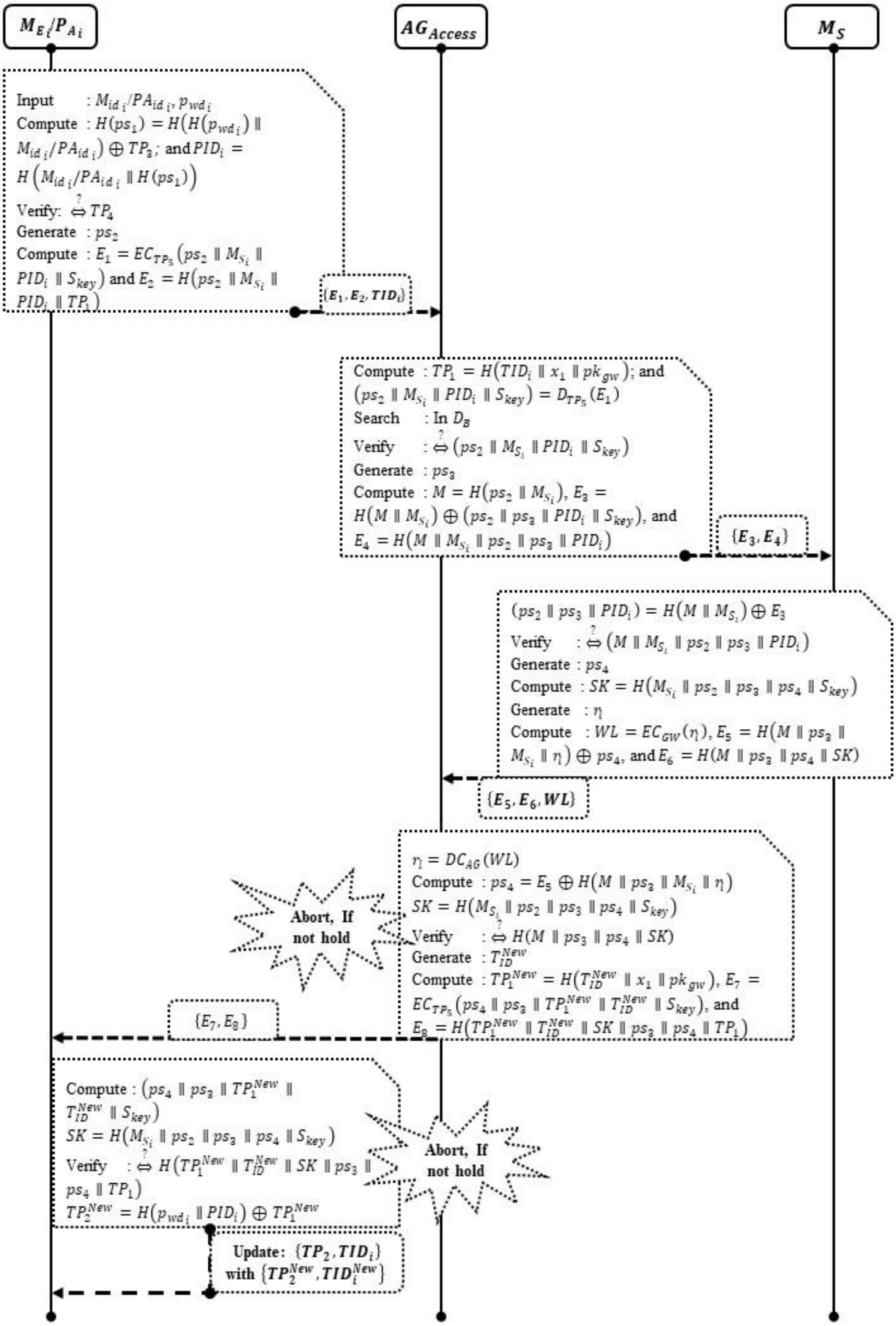

M_{E_i}/P_{A_i}
AG_{Access}
M_S
Input : $M_{id\,i}/PA_{id\,i}, p_{wd\,i}$
Compute : $H(ps_1) = H(H(p_{wd\,i}) \| M_{id\,i}/PA_{id\,i}) \oplus TP_3$; and $PID_i = H(M_{id\,i}/PA_{id\,i} \| H(ps_1))$
Verify: $\overset{?}{\Leftrightarrow} TP_4$
Generate : ps_2
Compute : $E_1 = EC_{TP_5}(ps_2 \| M_{S_i} \| PID_i \| S_{key})$ and $E_2 = H(ps_2 \| M_{S_i} \| PID_i \| TP_1)$
$\{E_1, E_2, TID_i\}$
Compute : $TP_1 = H(TID_i \| x_1 \| pk_{gw})$; and $(ps_2 \| M_{S_i} \| PID_i \| S_{key}) = D_{TP_5}(E_1)$
Search : In D_B
Verify : $\overset{?}{\Leftrightarrow} (ps_2 \| M_{S_i} \| PID_i \| S_{key})$
Generate : ps_3
Compute : $M = H(ps_2 \| M_{S_i})$, $E_3 = H(M \| M_{S_i}) \oplus (ps_2 \| ps_3 \| PID_i \| S_{key})$, and $E_4 = H(M \| M_{S_i} \| ps_2 \| ps_3 \| PID_i)$
$\{E_3, E_4\}$
$(ps_2 \| ps_3 \| PID_i) = H(M \| M_{S_i}) \oplus E_3$
Verify : $\overset{?}{\Leftrightarrow} (M \| M_{S_i} \| ps_2 \| ps_3 \| PID_i)$
Generate : ps_4
Compute : $SK = H(M_{S_i} \| ps_2 \| ps_3 \| ps_4 \| S_{key})$
Generate : η
Compute : $WL = EC_{GW}(\eta)$, $E_5 = H(M \| ps_3 \| M_{S_i} \| \eta) \oplus ps_4$, and $E_6 = H(M \| ps_3 \| ps_4 \| SK)$
$\{E_5, E_6, WL\}$
$\eta = DC_{AG}(WL)$
Compute : $ps_4 = E_5 \oplus H(M \| ps_3 \| M_{S_i} \| \eta)$
$SK = H(M_{S_i} \| ps_2 \| ps_3 \| ps_4 \| S_{key})$
Verify : $\overset{?}{\Leftrightarrow} H(M \| ps_3 \| ps_4 \| SK)$
Generate : T_{ID}^{New}
Compute : $TP_1^{New} = H(T_{ID}^{New} \| x_1 \| pk_{gw})$, $E_7 = EC_{TP_5}(ps_4 \| ps_3 \| TP_1^{New} \| T_{ID}^{New} \| S_{key})$, and $E_8 = H(TP_1^{New} \| T_{ID}^{New} \| SK \| ps_3 \| ps_4 \| TP_1)$
Abort, If not hold
$\{E_7, E_8\}$
Compute : $(ps_4 \| ps_3 \| TP_1^{New} \| T_{ID}^{New} \| S_{key})$
$SK = H(M_{S_i} \| ps_2 \| ps_3 \| ps_4 \| S_{key})$
Verify : $\overset{?}{\Leftrightarrow} H(TP_1^{New} \| T_{ID}^{New} \| SK \| ps_3 \| ps_4 \| TP_1)$
$TP_2^{New} = H(p_{wd\,i} \| PID_i) \oplus TP_1^{New}$
Abort, If not hold
Update: $\{TP_2, TID_i\}$ with $\{TP_2^{New}, TID_i^{New}\}$

Figure 3. Phase 4—Login and Authentication.

Phase 5—Learning Framework: In this phase, the application service uses the statistical features of the patients to discover a user behavior model. The designed model uses a connection module to extract the statistical vectors including a timestamp that computes the authentication levels of the interactive devices in real time. To meet the desired goals, the proposed framework uses four basic components:

Device Communication monitors the computing data via a dedicated application to manage complex issues in heterogeneous environments. Moreover, dynamic systems learn machine intelligence to discover a data-driven decision to optimize the network functionalities.

Data Preparation transforms the storage data to make an accurate prediction model which can explore a few essential tasks to uncover the relevant attributes of the application services, i.e., $\left\{\left(\mathrm{ST_{ID}}, \mathrm{S_{key}}\right), (\mathrm{F_{ID}}, \mathrm{K_P})\right\}$. Data Storage creates and maintains the application database $\mathrm{D_B}$ to verify the parameters $\left\{\left(\mathrm{ST_{ID}}, \mathrm{S_{key}}\right), (\mathrm{F_{ID}}, \mathrm{K_P})\right\}$ to leverage system performance and manage the file systems in parallel with low delivery latency.

Seamless Authentication simplifies the signing process to explore the trials of the password authentication scheme in order to examine the identities, social relationships, and access privileges.

In the lightweight device, the modeling parameters are preserved to compute the gradients effectively. In addition the parameters of the healthcare systems compare learning algorithms with various layer attributes to characterize the significance of computing devices. The layer attributes explore adaptive re-training to enhance the features of the detection model and to automate the utilization of neural networks using deep learning-based blind feature extraction. It is also worth noting that the proposed model operates the channel estimation matrix $\mathcal{H}(N \times 256)$ using a convolution network to capture the essential properties of the computing layers. Specifically, the modeling system has no consistent values between the predicted values of the authentication models, and thus, the true predicted values are computed using the softmax loss function, i.e., $S_L = -\sum_{k=1}^{N} Y_k.\log S_k$, where K defines the legitimate computing devices, Y_k represents the class label initially set to 1, and S_k denotes the kth value of the desired vector S. Hence, the softmax function can be rewritten as:

$$\mathrm{S_k} = \frac{\mathrm{e^{a_k}}}{\sum_{\mathrm{j}}^{\mathrm{K}} \mathrm{e^{aj}}} \tag{1}$$

where a_k shows the predicted values of kth computing device which is the fully connected layer of the application system. The purpose of a knowledge-based system is to acquire the blind features which functionalize the neuron to learn the complex features iteratively. Each feature tries to operate the mapping function of two adjacent layers which is as follows:

$$\begin{aligned}
&\text{Input Matrix} \ : \ IM^{Conv-Layer} \in \ R^{V \times W \times D} \\
&\text{Convolution Filter} \ : \ CF^{Conv-Layer} \in \ R^{V' \times W' \times D \times D''} \\
&\text{Output Matrix} \ : \ OM^{Conv-Layer} \in \ R^{V'' \times W'' \times D''}
\end{aligned}$$

where $V\ [V'\ or\ V'']$, $W[W'\ or\ W'']$, and $D[D'\ or\ D'']$ define the height, width, and depth of the convolution matrix. As a result, the output matrix can be expressed as:

$$OM^{Conv-Layer}_{i''.j''.d''} = bi_{d''} + \sum_{i'=1}^{V'} \sum_{j'=1}^{W'} \sum_{d=1}^{D} F^{Conv-Layer}_{i'.j'.d.\ d''} \times H_{S_v(i''-1)+i'-P_{\overline{v}},\ S_{w(j''-1)+j'-P_{\overline{w},d}}} \tag{2}$$

where $bi_{d''}$ is the model bias, (S_V, S_W) denotes the sampling vectors of the matrix, namely, vertical (V) and horizontal (W), and $(P_v^-, P_v^+, P_w^-, P_w^+)$ represents the output padding values in the directions of V and W. The mapping functions are expressed as follows:

$$V'' = \langle \frac{V - V' + P_v^- + P_v^+}{S_V} \rangle + 1 \tag{3}$$

$$W'' = \langle \frac{W - W' + P_w^- + P_w^+}{S_W} \rangle + 1 \tag{4}$$

In order to quantize the mapping function, the proposed neural network utilizes a $1 - bit$ random quantization scheme. This scheme utilizes the probabilistic quantizer to guarantee better quantization which exploits a mapping function to identify the level of quantization, i.e., $q_l = [\log_2 S_V S_W]$. Let $\omega_{i'j'} = S_V S_W \frac{w_{i'j'}}{\|W\|_F}$, where $\| \ . \ \|_F$ is the Frobenius norm of two independent solutions simplified by the Euclidean norm of the matrix. Hence, the quantized matrix $\hat{W_{ij}}$ is defined as:

$$\hat{W_{ij}} = sgn\left(w_{i'j'}\right) \langle \left(\left\lfloor \omega_{i'j'} \right\rfloor \right) + \partial_{i'j'} \rangle \| \ W \ \|_F \tag{5}$$

where $\partial_{i'j'}$ defines a random function to express the distribution as follows:

$$\partial_{i'j'} = \begin{matrix} 1 \ with \ probability \ \omega_{i'j'} - \left\lfloor \omega_{i'j'} \right\rfloor \\ 0 \ otherwise \end{matrix} \tag{6}$$

$sgn(x)$ is the function suited to quantizing the positive and negative values of the sampling vectors, i.e., $1 -$ bit level. The convolution layer directly feeds the output data of the pooling layer to minimize the computing attributes which considers $2 \times 2 \times 128$ to operate two convolutions and two pooling functions. This functional operation uses a fully connected layer as a target one which designs its own softmax loss to optimize the computation operation used in the proposed L2FAK while training the sensitive data, i.e., $S_L = -\sum_{k=1}^{N} Y_k . \log S_k$.

The proposed federated scheme uses three computing phases such as training, authentication, and re-training to learn the significance of blind features based on a convolution neural network. The classified attributes perform both forward and backward propagation to converge the computed value close to 0 which determines the legitimacy of any computing device. Each device shares its relevant parameters to train the physical characteristics of a well-trained neural network and to determine the data values of the computing device as shown in Algorithm 1. The device prediction is defined as follows:

$$D_P = \frac{\mathrm{e}^{\mathrm{a_k}}}{\sum_{\mathrm{j}}^{\mathrm{K}} \mathrm{e}^{\mathrm{aj}}} \tag{7}$$

It is worth noting that the fully connected layer determines whether the incoming messages of the computing devices are legitimate or not to verify the performance of the proposed FL with other learning mechanisms.

Algorithm 1 Federated Learning Layered Authentication (FLLA) Classifier.

```
Input: Collecting System Attributes $\{\mathrm{SA}_1, \mathrm{SA}_2, \ldots\}$ of $\mathrm{i}^{\mathrm{th}}$ Computing
Devices
Executing the number of rounds and Epoch $\mathcal{T}$ & $\tau$
Output: Authenticating the results of the Computing Devices, i.e., OM of
the neurons weights $\omega_{\mathrm{i'j'}}$
                    $\Delta_{\mathrm{FL-Q}}(\mathrm{SA}_1, \mathrm{SA}_2, \ldots, \mathrm{SA}_\mathrm{N}, \mathcal{T}, \tau)$
Step 1 : Initialize random computed values W with their corresponding
weights
Step 2 : Obtain the classifiers models including proposed and others
using storage database D_B to verify the parameters $\left\{\left(\mathrm{ST}_{\mathrm{ID}}, \mathrm{S}_{\mathrm{key}}\right), (\mathrm{F}_{\mathrm{ID}}, \mathrm{K}_\mathrm{P})\right\}$
Step 3 : For any new physical attributes Do
Step 3.1 : Send a quantized global model to train the own local model on its relevant computa-tion
data
Step 3.2 : Obtain a quantized local trained model which applies weighted averaging to receive the
quantized local model and to perform parameter quantization on $\mathrm{S}_\mathrm{V}\mathrm{S}_\mathrm{W}$
Step 3.3 : Compute a probability level of better optimization $\mathrm{q}_\mathrm{l}$ trained by the proposed FL via
$\sim 10$
Step 4 : If the computing device is classified as a legal or legitimate device
then
Step 4.1 : Allow device access via an appropriate data center
Step 4.2 : Modify the bit level of the training database D_B to find its corresponding
prediction values of $\left\{\left(\mathrm{ST}_{\mathrm{ID}}, \mathrm{S}_{\mathrm{key}}\right), (\mathrm{F}_{\mathrm{ID}}, \mathrm{K}_\mathrm{P})\right\}$
Step 5 : Else
Step 5.1 : Terminate the device connection
Step 6 : End If
Step 7 : End For
```

5. System Evaluation

This section discusses the security properties of the proposed L2FAK with the support of informal, formal, computation, and learning analysis.

5.1. Informal Analysis

The analysis of security properties is as follows.

Mutual Authentication: To analyze mutual authenticity between M_{Ei}/P_{Ai}, the communicating parties share a common session key to authenticate each other. In the L2FAK scheme, M_S authenticates M_{Ei}/P_{Ai} using $SK = H\left(M_{S_i} \parallel ps_2 \parallel ps_3 \parallel ps_4 \parallel S_{key}\right)$ via M_D. In the system login and authentication phase, AG_{Access} authenticates M_{Ei}/P_{Ai} using the calculations $TP_1 = H(TID_i \parallel x_1 \parallel pk_{gw})$ and $\left(ps_2 \parallel M_{S_i} \parallel PID_i \parallel S_{key}\right) = D_{TP_5}(E_1)$ to check whether M_{Ei}/P_{Ai} meets the conditional expression $\left(ps_2 \parallel M_{S_i} \parallel PID_i \parallel S_{key}\right)$ to initiate data transmission. Though A_{dv} tries to intercept the login requests of M_{Ei}/P_{Ai}, and attempts to falsify the activities of AG_{Access}, the attacker cannot find source parameters $\{ps_2, ps_3, PID_i\}$ to calculate derivative factors such as $\{E_3, E_4\}$. Therefore, A_{dv} cannot transmit a legitimate message to AG_{Access}. Hence, the proposed L2FAK adheres to mutual authentication of M_{Ei}/P_{Ai}.

Session-Key Agreement: In L2FAK, M_{Ei}/P_{Ai} share a common secure session key via AG_{Access}. Upon launch of the login and authentication phase, M_{Ei}/P_{Ai} can confidently exchange sensitive data by knowing the common session key. P_{Ai} data gathered by M_D are encrypted from the computation of $SK = H\left(M_{S_i} \parallel ps_2 \parallel ps_3 \parallel ps_4 \parallel S_{key}\right)$. Then, a secure session key is determined in order to validate $WL = EC_{GW}(r_l)$ using $E_5 = H(M \parallel ps_3 \parallel M_{S_i} \parallel r_l) \oplus ps_4$, and $E_6 = H(M \parallel ps_3 \parallel ps_4 \parallel SK)$. Because parameters ps_2, ps_3, ps_4, and S_{key} change periodically during execution, different sets of secure SK can be generated to provide more communication services. Hence, the proposed L2FAK provides session-key agreement between patient and medical expert.

Resilience against Privileged-Insider Attacks: The L2FAK scheme infrequently transmits communication parameters $\left\{H(.), p_{wdi}, M_{idi}, M_{S_i}, ps_2, PA_{idi}, S_{key}\right\}$ to authenticate server access as plaintext. In order to examine them further, M_{Ei}/P_{Ai} use $H(H(p_{wdi}) \parallel M_{idi} /PA_{idi}) \oplus TP_3$. Thus, the authentic server cannot obtain users' secret keys without knowing $TP_3 = H(H(p_{wd_i}) \parallel M_{id}/PA_{id}) \oplus H(ps_1)$, $TP_4 = H(p_{wd_i} \parallel ps_1)$, and $TP_5 = H(TP_1 \parallel S_{key} \parallel PID_i)$. Moreover, the hashing function, $H(S_N \oplus ID_{gw})$, is eventually verified using $\left(ps_2 \parallel M_{S_i} \parallel PID_i \parallel S_{key}\right)$ to control session access by M_{Ei}/P_{Ai}. So, an attacker cannot infer the valid session key of M_{Ei}/P_{Ai} without the presumption of $\{E_5, E_6, WL\}$. Hence, the proposed L2FAK is resilient to privileged-insider attacks.

Resilience against Replay Attacks: Suppose A_{dv} exploits old captured messages to authenticate servers, $\{E_1, E_2, TID_i\}$, medical sensors, $\left\{P_{M_{S_i}}, M_{S_i}, PID_i\right\}$, and users, $\left\{TP_2, TP_3, TP_4, TID_i, S_{key}\right\}$. However, A_{dv} cannot generate any authorized message transmission to validate pseudo-identity PID_i using $(H(p_{wdi}) \parallel M_{idi}/PA_{idi})$. Hence, the proposed L2FAK can resist the replay attack.

Resilience against User Masquerade Attacks: To forge login message $\left\{P_{M_{S_i}}, M_{S_i}, PID_i\right\}$, suppose A_{dv} tries an IoT-ECF system login with message modification $\left\{P_{M_{S_i}}{}^*, M_{S_i}{}^*, PID_i{}^{New}\right\}$. The parameters $\left\{P_{M_{S_i}}{}^*, M_{S_i}{}^*, PID_i{}^{New}\right\}$ cannot be tampered with or verified by AG_{Access}, and thus, the original data message $PID_i = H(M_{idi}/PA_{idi} \parallel H(ps_1))$ cannot be deduced via fake decryption parameter $\{M_{S_i}{}^*\}$. Hence, the proposed L2FAK can be irrepressible when facing a user masquerade attack.

Resilience against Gateway Masquerade Attacks: Since A_{dv} is unaware of some parameters, such as $\{E_5, E_6, WL\}$ from the data exchange protocol, A_{dv} cannot exploit a gateway masquerade attack against the proposed scheme. Hence, the proposed L2FAK can be irrepressible when facing gateway masquerade attacks.

Resilience against Offline Password Guessing: In most cases, the adversary tries to acquire system parameters over a public network. Assume he/she obtains the values of system parameters $\left\{TP_2, TP_3, TP_4, TID_i, S_{key}\right\}$ from S_D. In addition, M_{Ei}/P_{Ai} make an effort to find a new secret key, SK^{New}, to compute $E_8 = H(TP_1^{New} \parallel T_{ID}^{New} \parallel SK \parallel ps_3 \parallel ps_4 \parallel TP_1)$. However, valid key SK^{New} cannot be computed because it is irretrievable from the M_D of M_{Ei}/P_{Ai}. Thus, the proposed L2FAK can be resilient to offline password-guessing attacks.

Resilience against User Forgery: To forge communications of any legal entities, A_{dv} requires parameters such as $\left\{TP_2, TP_3, TP_4, TID_i, S_{key}\right\}$. To obtain them with little effort, A_{dv} tries to compute TP_3, TP_4, and TP_5 consisting of PID_i, TID_i, and p_{wd}. Since S_{key} is irretrievable, A_{dv} cannot infer or obtain a legal identity for AG_{Access} in order to derive a valid message request to authorize the session. Thus, the proposed L2FAK is resilient against the user forgery attack.

Resilience against Gateway Forgery: Assume A_{dv} generates PID_i using $H(M_{idi}/PA_{idi} \parallel H(ps_1))$. As a result, A_{dv} claims that a legal request may be successfully generated. However, the proposed L2FAK cannot permit anyone to generate a valid request without proper associations for ps_2, M_{S_i}, and S_{key}. Importantly, S_{key} and M_{Key} are very hard to derive because they are associated with high-level security features. Thus, the proposed L2FAK can be resilient against gateway forgery.

Resilience against Gateway User Tracking: As AG_{Access} randomly generates private key pk_{gw} to establish secure sessions, M_{Ei}/P_{Ai} cannot be tracked by adversaries. In addition, S_{key} is irretrievable; thus, a legal request cannot be generated to track user sessions.

Perfect Forward Secrecy: In most cases, A_{dv} tries to obtain system parameters such as $P_{M_{S_i}}$ and M_{S_i}. Moreover, A_{dv} may examine legal message requests such as $\left\{P_{M_{S_i}}, M_{S_i}, PID_i\right\}$

and $\left\{TP_2, TP_3, TP_4, TID_i, S_{key}\right\}$ to generate valid session key SK using $H(M_{S_i} \parallel ps_2 \parallel ps_3 \parallel ps_4 \parallel S_{key})$. As a rule, M_D generates a firm and secure SK that assigns a random number, ps. As a result, it is certain that A_{dv} cannot obtain legal values such as $MP_{M_{S_i}}$, M_{S_i}, and PID_i to discover a secure session. Hence, the proposed L2FAK ensures perfect forward secrecy.

Under the procedures of the L2FAK scheme, M_{Ei}/P_{Ai} can mutually endorse one another to access sensitive IoT-ECF data. Eventually, M_{Ei} can access patients' private information via AG_{Access}. As a session key is securely shared among the communication entities, the L2FAK can achieve security, namely, the properties of mutual authenticity and session-key agreement, and be irrepressible in the face of user and gateway masquerades, and privileged-insider and replay attacks, improving security efficiency.

5.2. Formal Analysis Using Random Oracle Model

This section performs formal analysis during the login and authentication phase to show the security efficiency of the proposed L2FAK [83].

Theorem 1. *The revoked user cannot learn the stored files of M_E/P_A even if they are in collision with the cloud server. Moreover, the user is not capable to learn the content of data stored as the blocks after the successful revocation.*

Proof. When any user quits communication with M_S based on the proposed L2FAK, the parameters such as ps_2, ps_3, and ps_4 are utilized to decrypt the data files. Moreover, it uses $r.ps_2 + r.ps_3 + r.ps_4 = r.SK$ to perform the computation again. Observing the following instance, the revoked user can use the secret key S_{key} to participate and learn the data contents c Subsequently, the revoked user colludes with M_S to decrypt the data file using an authentic key. The key verification is as follows:

$$\begin{aligned} e(\tau ps, \nu ps)^{H(\mathcal{K}_i).(P_{pa}, M_{pa}, PID_{pa})} &= e(\tau ps, \nu H(\mathcal{K}_i)\ (P_{pa} + M_{pa} + PID_{pa})\ ps) \\ = e(\nu ps, H(\mathcal{K}_i)\ P_{pa}\ ps)^{\tau}.e(\nu ps, H(\mathcal{K}_i)\ M_{pa}\ ps)^{\tau}&.e(\nu ps, H(\mathcal{K}_i)\ PID_{pa}\ ps)^{\tau} \\ &= ps_2{}^{\tau}.ps_3{}^{\tau}.ps_4{}^{\tau} \end{aligned} \tag{8}$$

However, the system parameters of the encrypted key imply $ps_2{}^{\tau}.ps_3{}^{\tau}.ps_4{}^{\tau} \neq rps_2{}^{\tau} .rps_3{}^{\tau}.rps_4{}^{\tau}$ to ensure that the revoked user cannot perform any decryption process to update the source file. As a consequence, the proxy M_S has the ability to control the access rights of the revoked users, whereby they cannot collude with M_S to learn the actual data content. □

Theorem 2. *The semi-trusted cloud server cannot differentiate its access operation to learn the interested data contents.*

Proof. When any content of data has gained its access several times, the curious cloud server determines such data as more significant to monitor or likely to tamper with a forged secret key. Meantime, the curious cloud collaborates with the revoked users to learn the data contents and its accessing capabilities. Thus, the probability of accessing data should be identical to the data that appeared in the cloud server. The access operation includes real and 2^N pseudo-random requests to process the application services to the cloud server while the user applies an access control algorithm. In practice, real-time data is only known to the authentic user to gain system access. It is worth noting that the accessed data is uniformly distributed to the cloud server to maintain better data consistency. Though the algorithm known as lazy obfuscation is applied to access the data content, the relationship of the data including address sequences cannot be applied by the cloud server to discover its actual form. The user performs a specific access operation on the data content to view it as a new one of the cloud servers. Hence, it is claimed that the semi-trusted cloud server cannot differentiate its access operation to learn the interested data contents. □

Theorem 3. *The accessed data pattern can be secure under the adversary act of AD_{PPT}. Assume the proposed L2FAK can support a feature of data untraceability to enhance the privacy of data content. The adversary tries to access the proposed L2FAK over a wireless channel to initiate the session between M_E/P_A and M_S to arbitrate the user U activities. Moreover, the adversary is known to determine a few computation parameters $M = H(ps_2 \parallel M_{S_i})$ and $P_{M_{S_i}} = H(M_{S_i} \parallel pk_{gw})$ which executes two queries $\{M^s, N^s\}$ and $\{N^s, M^s\}$ to breach the secure communication of the proposed L2FAK.*

$$AD_{PPT}(U) = |2P_r|C^*_\eta + \left|C^{*'}_\eta - 1\right| \tag{9}$$

where C^*_η is a coin flicked by the adversary, and $C^{*'}_\eta$ is the outcome of the flicked coin. For the execution of hash queries, the advantage with adversary act U is as follows:

$$AD_{PPT}(U) = |P_r(S_2) - P_r(S_1)| + q^{(H^2/2^{th})(S+1)} + q^{((H+1)2/2^{th})(S+1)} + q^{(H^2/2^{th})(S)} \tag{10}$$

where $q^{(H^2/2^{th})(S+1)} + q^{((H+1)2/2^{th})(S+1)} + q^{(H^2/2^{th})(S)}$ defines the collision of the hash code function with each user in the oracle model. Using Equation (8), we obtain:

$$|P_r(S_3) - P_r(S_2)| \leq \left[2q_U + \frac{2q_{M_E/P_A}}{2q_{M_S}}\right] \tag{11}$$

The advantage with adversary act U tries to obtain the shared session key SK:

$$|P_r(S_1) - P_r(S_2)| \leq q_{M_E/P_A}.\, AD_{PPT}(U) \tag{12}$$

In case of accessing the storage space M_D, the probability with adversary U is as follows:

$$|P_r(S_3)| = \frac{1}{2} max\left(\frac{q_U}{2}, \frac{q_{M_E/P_A}}{D}\right) \tag{13}$$

Using Equations (9)–(11), we obtain:

$$\begin{aligned} AD_{PPT}(U) \quad &= P_r(S_1) - 1 \\ &= 2|P_r(S_0) - P_r(S_4)| + max\left(\tfrac{q_U}{2}, \tfrac{q_{M_E/P_A}}{D}\right) \\ &\leq 2|P_r(S_0) - P_r(S_4)| + max\left(\tfrac{q_U}{2}, \tfrac{q_{M_E/P_A}}{D}\right) \\ &= 2|P_r(S_1) - P_r(S_2) + P_r(S_3) - P_r(S_4)| + max\left(\tfrac{q_U}{2}, \tfrac{q_{M_E/P_A}}{D}\right) \\ &\leq \left(\frac{{q_U}^2 + {q_{M_E/P_A}}^2 + {q_{M_S}}^2}{2^q} + \frac{\left(q_U + q_{M_E/P_A}\right)^2}{2(q-1)} + 2q_{M_E/P_A}.AD_{PPT}\left(U_{M_E/P_A}\right) + 2.\left[\tfrac{q_U}{2^q}, \tfrac{q_{M_E/P_A}}{|D|}\right]\right) \end{aligned} \tag{14}$$

5.3. Computation Analysis

In this subsection, the performance of the proposed L2FAK is evaluated along with other existing schemes [42,44,49–51,53]. In computation analysis, the system login and authentication phases were considered to examine the security features of the proposed L2FAK and the other schemes [42,44,49–51,53]. The authentication schemes employ the OpenSSL library between two computer terminals for analysis of computation costs. The user-side terminal had a Core i3-1035G1 CPU with 8GB RAM and a clock speed of 3.6 GHz, whereas the server-side terminal had a Core i5-1035G1 CPU with 16GB RAM and a 2.3 GHz clock speed to construct the simulation environment. The user and server were connected over H3C S1024R to ensure that the connected device had a 100 Mbps bandwidth to perform the simulation more than 100 times. From the NIST [Anon] recommendation [26], $P - 192$ is preferred as the standard elliptic curve.

To regulate the message digest, $SHA - 256$ cryptographic hashing was utilized. Table 3 shows the execution times of the cryptographic operations. Since L2FAK has a low computation overhead of 15.343 ms, the phase execution time of the proposed L2FAK can be further reduced to achieve better computation efficiency compared to the other authentication schemes [42,44,49–51,53], as shown in Table 4.

Table 3. Execution Times of Cryptographic Operations.

Operator	Execution Times ⟨ms⟩	
	User	Server
T_{HD}	0.16073	0.208057
T_{SY}	0.013125	0.004343
T_{EED}	0.095417	0.011054
T_{MU}	79.256041	6.132746
T_{EOR}	27.987396	2.493921
T_{AD}	0.011667	0.004737

Table 4. Assessment of Computational Efficiency.

Scheme	Registration		Login and Authentication			Execution Time ⟨ms⟩
	$\mathbf{M_E}$	$\mathbf{AG_{Access}}$	$\mathbf{M_E}$	$\mathbf{AG_{Access}}$	$\mathbf{M_S}$	
Proposed L2FAK	$7T_{HA}+1T_{EED}$	$1T_{HA}$	$7T_{HA}+1T_{EED}$	$8T_{HA}+2T_{EOR}+1T_{EED}$	$4T_{HA}+2T_{EOR}+1T_{EED}$	15.343
Yang et al. [44]	$4T_{HA}+3T_{EOR}$		$8T_{HA}+6T_{MU}+3T_{AD}$			123.080
Deebak et al. [49]	$2T_{MU}+4T_{XOR}+2T_{AD}$		$5T_{HA}+4T_{EOR}+4T_{SY}$			281.518
Abdussami et al. [50]	$5T_{HA}+2T_{EOR}$		$15T_{HA}+5T_{EOR}+1T_{EED}$			72.380
Kim et al. [51]	$6T_{HA}+4T_{EOR}$		$13T_{HA}+18T_{EOR}$			160.509
Chen et al. [53]	$5T_{HA}+1T_{EOR}+1T_{EED}$		$27T_{HA}+14T_{EOR}+2T_{EED}$			69.441
Li et al. [42]	$19T_{HA}+11T_{EOR}$		$19T_{HA}+11T_{EOR}$			342.302

T_{HA} represents the one-way hashing function; T_{SY} represents the symmetric cryptosystem function; T_{EED} represents the elliptic-curve encryption/decryption operation; T_{MU} represents one-point multiplication over ECC; T_{EOR} represents the Exclusive-OR operation; and T_{AD} represents one-point addition over ECC.

5.4. Learning Analysis

In learning analysis, datasets such as MNITS and FashionMNIST [84] are adopted to evaluate the proposed FLLA and other relevant layered mechanisms [17,18]. The evaluation mechanisms utilize a dedicated message-passing interface (MPI) to maintain optimal load factors in a distributed environment [85]. The environment uses Python to implement the source codes and prefers a high-performance computing package, i.e., mpi4py to access the computing platform. This platform is compatible with 12th Gen Intel Core i7, 16GB RAM, 14 cores, and a clock rate of 4.7 GHz. The compatible system uses MPI specification to build the source codes of the proposed FLLA and other relevant layered mechanisms [17,18], in order to provide a separate object interface. The object interfaces exploit a few significant key features of the configured prototype to facilitate the computation process. This prototype has one central server C_S, four computing service cp_s, and one coded data service D_s to test the behavior of targeted and untargeted attacks. Table 5 shows the detailed descriptions of the datasets. In MNIST, the data are relevant to handwritten numbers of 250 different people, where 50% are high-school students, and another 50% are Census Bureau.

Table 5. Detailed Description of Datasets.

Parameters	**MNIST**	**FashionMNIST**
Domain Name	Handwritten Numbers	Clothing
Training Data	60,000	60,000
Testing data	10,000	10,000
Classes	10	10
Clients	3	3
Data Type	Images	Images

Moreover, this dataset has a similar portion of digital data to test its relevance and is composed of $60,000$ training and $10,000$ testing images to verify the performance of the proposed FLLA along with other mechanisms [17,18] in terms of accuracy and testing rate. In case of no special instructions, this analysis chooses 200 as primary data to meet the constraint of data distribution represented as PD_0. The FashionMNIST uses a similar size as MNIST to categorize its selective images of clothing. To realize the scenario of the proposed FLLA along with other mechanisms [17,18] in practice, this experiment uses poisoning attacks. This attack considers the activities of a malicious client to define the roles of targeted and untargeted attacks. The former attack arbitrarily performs its changes to operate the global model, whereas the latter exploits label-flipping to control the behavior of the malicious client, i.e., from l to $(N - l - 1)$, where $l \in \{0, 1, \ldots, N - 1\}$ and N represents the total number of labeling data.

Evaluation Metrics: The metrics such as test accuracy and error rate are used as an indicator of the evaluation model to train the datasets. The object of the proposed FLLA is to enhance the inference rate or detection accuracy of the global model. In data analysis, federated learning chooses a prominent model, the so-called FEDSGD, as a baseline which has the existence of different malicious clients to examine the results of the proposed FLLA along with other mechanisms [17,18].

Learning Settings: The evaluation considers cross-silo settings and defines the number of computing cores $n_c = 10$ to exercise the clients during the training process. The selected model uses a three-layered neural network to load two different datasets on the interface of Keras with a backend platform of TensorFlow. Table 6 enlists the modeling parameters of two different datasets including MNIST and FashionMNIST to allocate the data inputs to the object interface. Each interface handles 6000 data sources which have a distribution of malicious clients ranging from 20% to 40% to perform a few critical scenarios [86]. The batch size b_s and loss function l_f are set to 128 and 50 rounds, respectively, to observe the results of the proposed FLLA along with other mechanisms [17,18]. Note. The epoch e is set to 50 to train the learning models in order to obtain the optimal solution for every iteration.

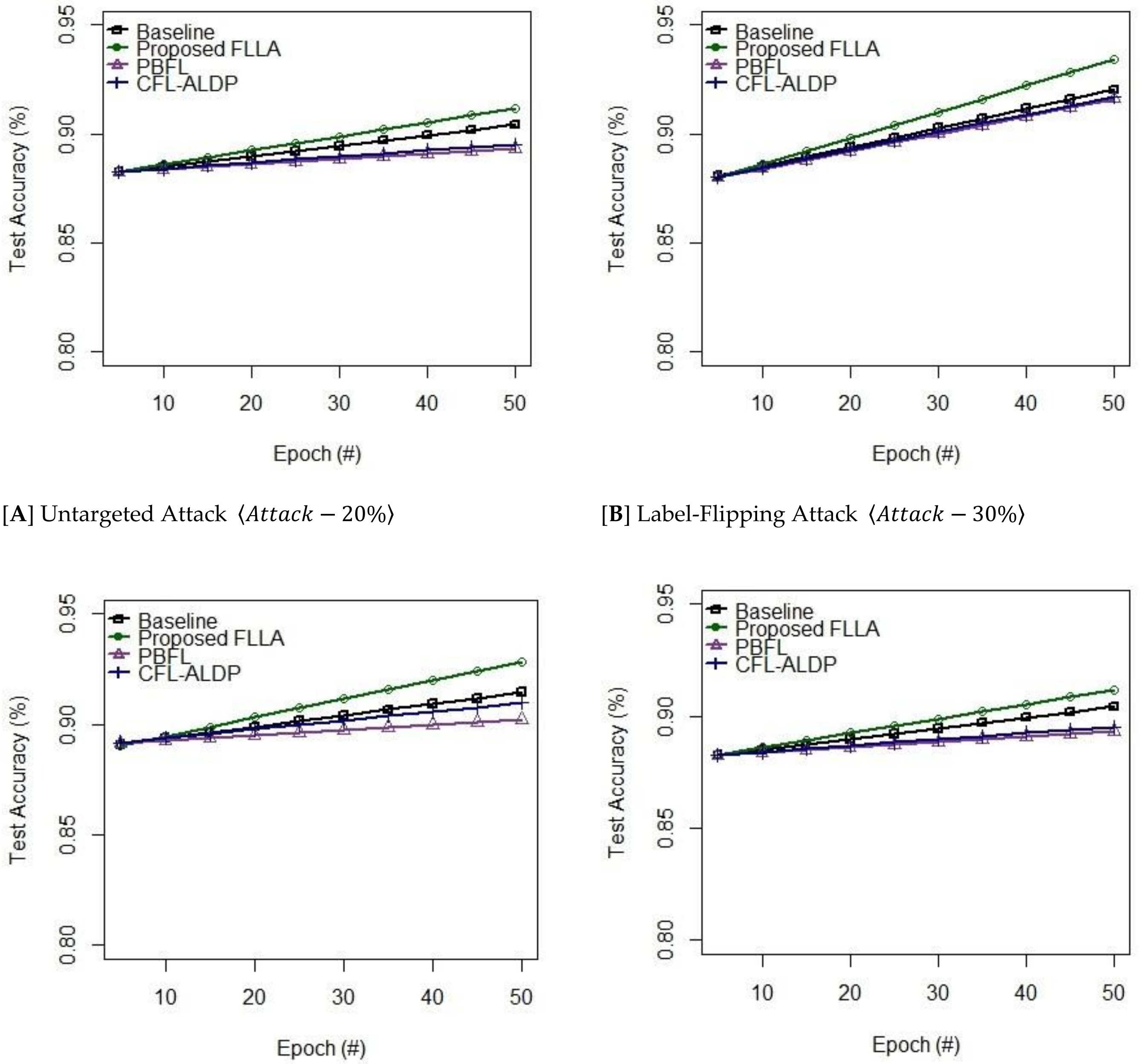
Table 6. Detailed Description of Datasets.

Layered Type	**Output Shape**	**Set Values**
Flatten [flatten]	786	0
Dense [dense]	128	100,780
Dense [dense_1]	10	1310

Experimental Results: The results show the effectiveness of the proposed FLLA along with other mechanisms [17,18] in contact with poisoning attacks. The classified outputs prove that the proposed FLLA achieves better robustness, accuracy, reliability, and privacy than other mechanisms [17,18]. Table 7 shows the test error rate of the proposed and other existing mechanisms versus the distribution of malicious clients in the global model [targeted and untargeted attack] on MNIST and FashionMNIST. The training process involves 50 iterations on the given dataset MNST and Fashion MNIST to signify the importance of the security features. Precisely, in the existence of malicious clients, the proposed FLLA retains the constant accuracy rate as its own baseline to resist various types of targeted and untargeted attacks. Figures 4 and 5 show test accuracy versus Epoch (#) on MNIST and FashionMNIST. The proposed FLLA and other existing mechanisms [17,18] acquire the layered features to observe the transition states of the distribution matrix and to identify any abnormal condition determining any anomaly degree of the data points. The system cores executed via a message-passing interface rely on layered features to analyze the abnormal behavior of any computing device as shown in Table 7.

Table 7. Test Error Rate of the Proposed and other Existing Mechanisms versus Distribution of Malicious Clients in the Global Model [Targeted and Untargeted Attack] on MNIST and FashionMNIST.

Dataset	**Learning Mechanisms**	**Distribution of Malicious Clients in the Global Model**		
		20%	**30**%	**40**%
MNIST	Proposed FLLA (Untargeted)	0.04	0.05	0.05
	PBFL (Untargeted)	0.05	0.06	0.06
	CFL-ALDP (Untargeted)	0.06	0.06	0.21
	Proposed FLLA (Targeted)	0.05	0.05	0.05
	PBFL (Targeted)	0.06	0.08	0.18
	CFL-ALDP (Targeted)	0.07	0.09	0.13
FashionMNIST	Proposed FLLA (Untargeted)	0.15	0.18	0.19
	PBFL (Untargeted)	0.17	0.19	0.21
	CFL-ALDP (Untargeted)	0.21	0.23	0.27
	Proposed FLLA (Targeted)	0.14	0.15	0.15
	PBFL (Targeted)	0.15	0.15	0.19
	CFL-ALDP (Targeted)	0.19	0.19	0.23



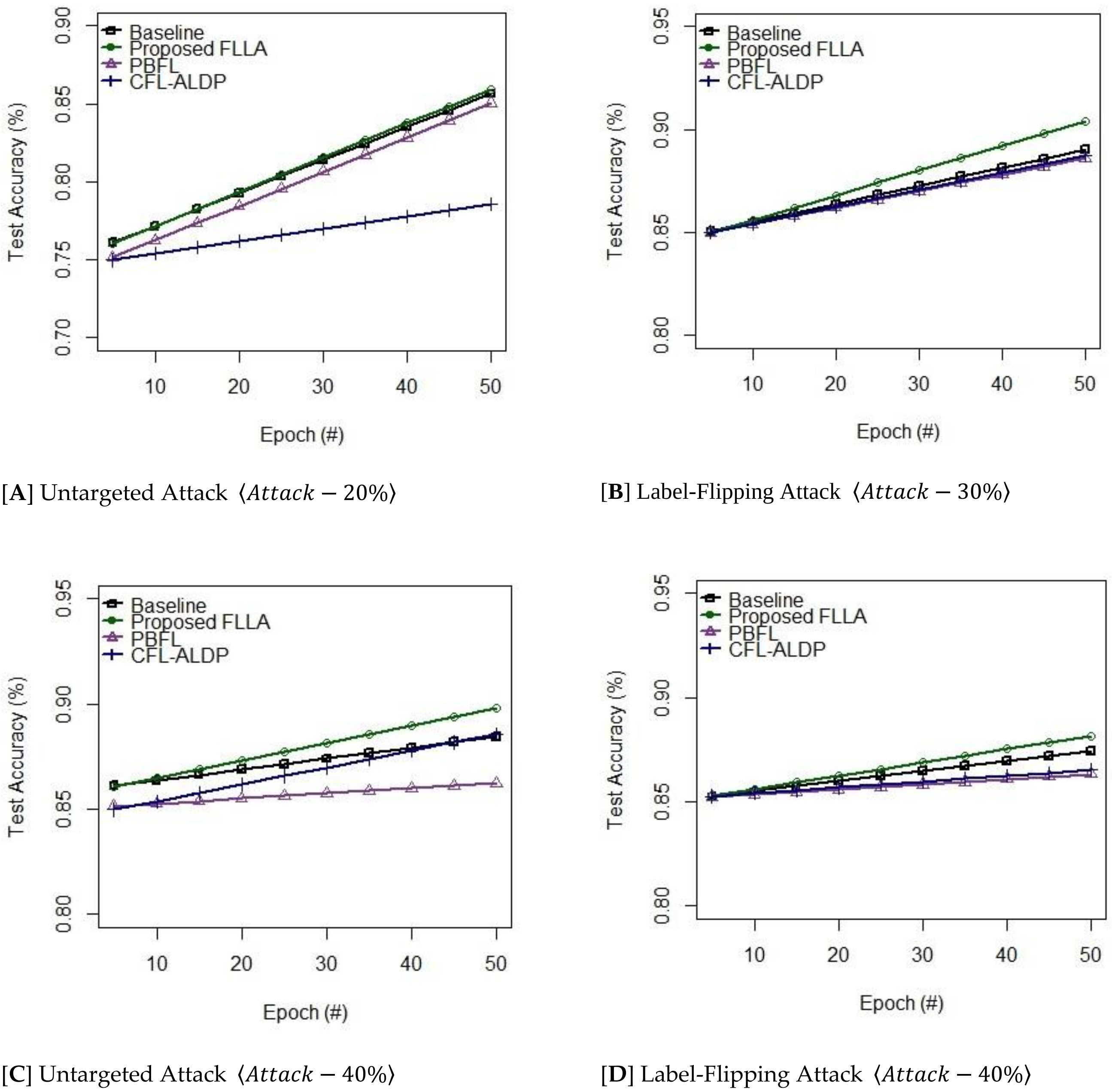
[**A**] Untargeted Attack $\langle Attack - 20\%\rangle$

[**B**] Label-Flipping Attack $\langle Attack - 30\%\rangle$

[**C**] Untargeted Attack $\langle Attack - 40\%\rangle$

[**D**] Label-Flipping Attack $\langle Attack - 40\%\rangle$

Figure 4. Test Accuracy Rate (%) on MNIST.



[**A**] Untargeted Attack $\langle Attack - 20\% \rangle$

[**B**] Label-Flipping Attack $\langle Attack - 30\% \rangle$

[**C**] Untargeted Attack $\langle Attack - 40\% \rangle$

[**D**] Label-Flipping Attack $\langle Attack - 40\% \rangle$

Figure 5. Test Accuracy Rate (%) on FashionMNIST.

While the features such as the proposed FLLA and other existing mechanisms [17,18] were applied to the behavior of the computing devices, we observed that the proposed FLLA maintain a better consistent rate of accuracy than the other mechanisms [17,18]. A few hyperparameters such as learning rate $\alpha = 0.001$ and influence factor $\gamma = 0.1$ were applied to change the computing models which choose its probabilistic quantizer to guarantee better quantization. Moreover, adaptive learning may momentarily accelerate the training process to Investigate the modeling performance of the layered features. In order to examine in real time, the training process was repeatedly iterated ≈50 times. From Figures 4 and 5, it is more evident that the proposed FLLA obtains a more reliable authentication procedure in extracting the system attributes of the physical layer than other learning mechanisms [17,18], whereby the behavior of the FLLA system can fully be characterized to secure the authentication process. Importantly, key-based cryptosystems demand more computation time to establish a secure connection, whereas the physical layer security depends on the quantification of the system attributes to enable device authentication and adaptive training to fulfill the objectives of model-based authentication.

6. Performance Analysis

This section describes a real-time testbed that verifies the transmission efficiency of the proposed L2FAK compared with other schemes [42,44,49–51,53]. To realize the efficiency factor, the testbed chosen used resource-constrained devices with a low code overhead, as shown in Table 8. Components such as the Raspberry Pi-3 Model B and Arduino Mega 2560 were deployed for authentic gateway access and edge computing devices, respectively [87]. Note that the Arduino was equipped with ATmega2560 with 8 KB of SRAM and 256 KB of flash memory to process data transmissions from about 700 identities. Importantly, the uninitialized power-up state, i.e., on-chip SRAM, was utilized to generate a unique device key, and the user registration phase was executed to gain system access. The registration and authentication phases of the proposed L2FAK and other existing schemes [42,44,49–51,53] were implemented on Python 3.5, which generated the user identities to process the data flow on the Ubuntu platform.

Table 8. Hardware Configuration Details.

Host Terminal [Raspberry Pi 3 Model B]	Wireless LAN–802.11 b/g/n
	Processor–1.2 GHz Quad-Core ARM
	Memory–1 GB LP-DDR2
Arduino Mega 2560	ATmega2560; SRAM–8 KB; Flash Memory–256 KB
Operating System	Ubuntu MATE 18.04.2
Number of user identities	≈700

In addition, dedicated firmware was written in C to read uninitialized memory between the heap and the stack when extracting SRAM data to establish communication with the host terminal. To measure the transmission ratio, real-time analysis was conducted that varied packet sizes of about 256 *bits*. The execution of firmware steps is as follows.

Step 1: Load the firmware to read the available memory space that contains only the subroutine for SRAM data.

Step 2: Combine authentication and application subroutines to shift and store the generated ID in the microcontroller.

Step 3: Load the function $D[ID_{start}]$ to $D[ID_{start} + \langle e - 1 \rangle]$ that returns the locations of the stable bits. However, the location of the stable bits may vary due to availability in the hardware.

Step 4: Match the data pointers (stack and heap) to return the retrieval rate of data transmission (DT).

Step 5: Extract the user identities to compute the session key, storing the value in the microcontroller to authenticate device access.

6.1. Data Transmission Ratio

To test the data flow process, the DT ratio considers the number of user identities. It is randomly generated upon successful execution of power-up states that analyze the retrieval rate of data transmission. In Figure 6, we observe that the proposed L2FAK has a better power-up state to achieve maximum authentication access (i.e., 0.8545) than the other schemes [42,44,49–51,53]. Due to the increasing number of users, the collision probability may appear high. From the analysis, the transmission delay soars when the number of packet transmissions increases in proportion to the number of user identities. However, the proposed L2FAK keeps the delay within the restriction limit to improve transmission efficiency between the authentic gateway and the edge devices compared to the other schemes [42,44,49–51,53].

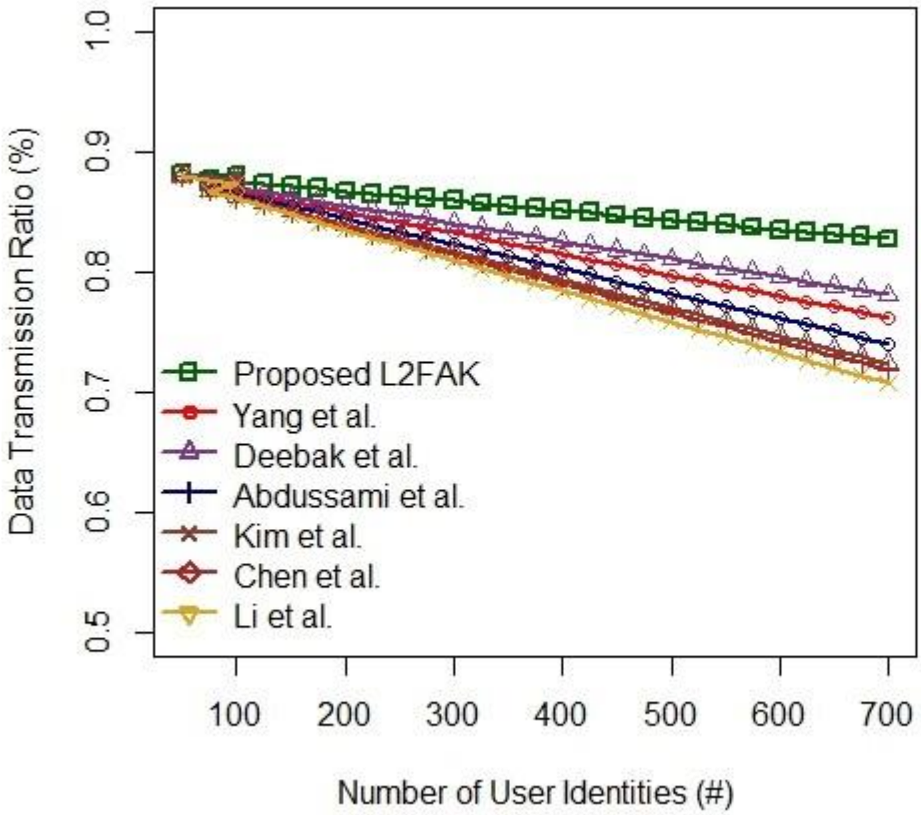


Figure 6. Data Transmission Ratio (%) vs. the Number of User Identities (#).

6.2. Overhead Analysis Ratio

Overhead analysis (OA) included the system authentication phase of the proposed L2FAK and the other schemes [42,44,49–51,53] to examine the core features of AG_{Access} and edge computing device M_E. Flow connectivity is as follows:

Step 1: The authentication phase prefers a dedicated AG_{Access} to generate valid tokens, e.g., for M_E. The real-time entities, including AG_{Access} and M_E, use a reliable authentic token to process authentication requests that integrate a legal message request, $\left\{H(.), C, N_i, S_{key}\right\}$, to generate valid session key SK.

Step 2: M_E applies $\left\{N_i, S_{key}\right\}$ to retrieve and convert the computational parameters using the $SHA-2$ algorithm. It can execute the extraction subroutines of user identities to construct a $256-bit$ stable identity using the addressed slots from SRAM. Computation parameters such as M_{id} and $SHA-2\langle N_i\rangle$ are processed to generate a valid $\langle X-OR\rangle$ value for S_{key}.

Step 3: AG_{Access} processes the generated M_{id} retrieved from $M_E\langle N_i\rangle$ to decrypt the authentication request, i.e., $M'_{id} = SHA-2\langle N_i\rangle \oplus S_{key}$. The generated identity then compares the values with a stored identity to process the authentication request.

As to analyzing overhead costs, key parameters such as key size and timing frame are preferred. The overall function has an overhead ratio of 3.65% in processing the system authentication phase. The overhead cost includes the hash algorithm and string processing to compute the memory requirements that use the symmetric key to store $256-bit$ values. Device security plays a crucial role in achieving the security level of the IoT architecture; thus, a proper configuration setup is made to examine the core features of low-cost application systems.

Figure 7 shows the overhead ratio versus the number of user identities. It is worth noting that the performance of IoT devices considers the generated identities to authorize the legal authentication requests of M_E at regular intervals. The system analysis included the generation of about 700 IoT devices in order to analyze the RAM power-up states among different computing devices. The examination reveals that the proposed L2FAK incurs lower overhead costs, ≈89.45% , to determine genuine legal authentication requests, i.e., the identities of IoT devices, than the other schemes [42,44,49–51,53].

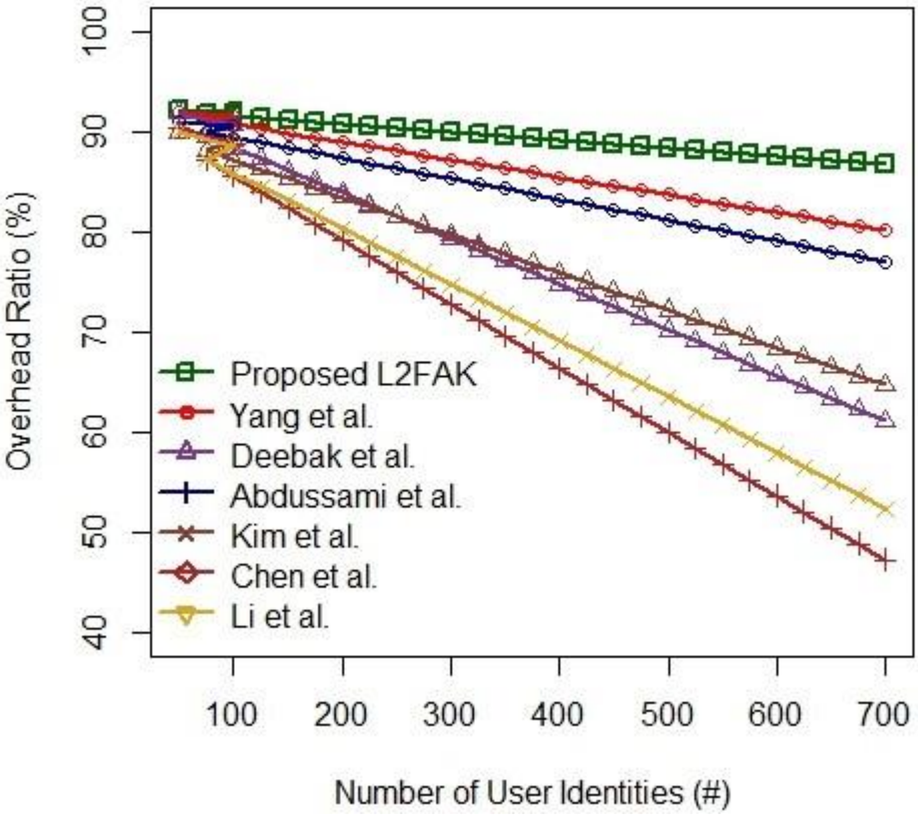


Figure 7. Overhead Ratio (%) vs. the Number of User Identities (#).

7. Conclusions

In this paper, the L2FAK protocol has been presented using a mobile sink in the IoT-ECF paradigm for smart eHealth systems. Two factors are strategically exploited through an authentic-ware system to mitigate computation costs. Computation analysis proves that the proposed L2FAK incurs lower operational costs to enhance the performance of a real-time system. The proposed L2FAK includes a lightweight operation to improve the computational efficiencies from system authentication and key agreement phases. Using informal and formal analysis, the security efficiency of the proposed L2FAK proved it strengthens the security level of the authentication phase. Moreover, the performance analysis shows that the L2FAK achieves better transmission efficiency and a better overhead ratio than other schemes [23,24,44,47,48]. In addition, applied layered authentication using federated learning, i.e., FLLA, utilizes the most appropriate system attributes of the proposed L2FAK to ensure device privacy and improve authentication accuracy in healthcare applications. The experiments are established using TensorFlow Federated to examine the proposed FLLA and other relevant mechanisms on two different datasets including MNIST and FashionMNIST. The analytical results show that the proposed FLLA preserves the privacy features of authentication schemes exceedingly better than other mechanisms used to promise accuracy on standard datasets.

In the future, we will use reliable resource-constrained IoT devices, such as gateway devices and an advanced Raspberry Pi, to implement and evaluate several instances of a cloud server. In addition, we prefer to incorporate lightweight operators to analyze different traffic patterns, which may evolve into several test cases to examine the core features of fog instances and cloud servers to enhance system efficiencies, including computation, communication, and storage.

Author Contributions: Conceptualization, B.D.D. and S.O.H.; methodology, B.D.D.; validation, B.D.D.; formal analysis, B.D.D.; investigation, B.D.D.; writing—original draft preparation, B.D.D.; writing—review and editing, B.D.D. and S.O.H.; supervision, S.O.H.; project administration, S.O.H.; funding acquisition, S.O.H. and B.D.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Brain Pool Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and Information Communication Technology (ICT) under Grant No. 2022H1D3A2A02081848 and by the Gachon University research fund under Grant GCU-202206210001.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare they have no conflicts of interest regarding the publishing of this paper.

References

1. Jangirala, S.; Das, A.K.; Vasilakos, A.V. Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. *IEEE Trans. Ind. Inform.* **2019**, *16*, 7081–7093. [CrossRef]
2. Ahmed, J.; Nguyen, T.N.; Ali, B.; Javed, M.A.; Mirza, J. On the physical layer security of federated learning based IoMT networks. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 691–697. [CrossRef]
3. Luo, S.; Zhu, D.; Li, Z.; Wu, C. Ensemble federated adversarial training with non-iid data. *arXiv* **2021**, arXiv:2110.14814.
4. Edemekong, P.F.; Annamaraju, P.; Haydel, M.J. *Health Insurance Portability and Accountability Act*; StatPearls Publishing LLC.: Tampa, FL, USA, 2018.
5. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A review of internet of things (IoT) security issues, challenges and techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6.
6. Maurya, S.; Joseph, S.; Asokan, A.; Algethami, A.A.; Hamdi, M.; Rauf, H.T. Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT. *Sensors* **2021**, *21*, 7793.
7. Wang, W.; Chen, Y.; Zhang, Q. Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures. *IEEE Trans. Wirel. Commun.* **2015**, *15*, 1218–1225. [CrossRef]
8. Ma, X.; Liu, J.; Jiang, H. Resource allocation for heterogeneous applications with device-to-device communication underlaying cellular networks. *IEEE J. Sel. Areas Commun.* **2015**, *34*, 15–26. [CrossRef]
9. Al-Sarawi, S.; Anbar, M.; Abdullah, R.; Al Hawari, A.B. Internet of Things market analysis forecasts, 2020–2030. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 449–453.
10. Sinha, P.; Jha, V.K.; Rai, A.K.; Bhushan, B. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In Proceedings of the 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 28–29 July 2017; pp. 288–293.
11. Moon, A.H.; Iqbal, U.; Bhat, G.M. Mutual entity authentication protocol based on ECDSA for WSN. *Procedia Comput. Sci.* **2016**, *89*, 187–192. [CrossRef]
12. Saqib, M.; Jasra, B.; Moon, A.H. Mutual Authentication Protocol for Green Internet of Things in Content Centric Network. *J. Green Eng.* **2020**, *10*, 4896–4909.
13. Saqib, M.; Jasra, B.; Moon, A.H. A Systematized Security and Communication Protocols Stack Review for Internet of Things. In Proceedings of the 2020 IEEE International Conference for Innovation in Technology (INOCON), Bangluru, India, 6–8 November 2020; pp. 1–9.
14. Ullah, F.; Habib, M.A.; Farhan, M.; Khalid, S.; Durrani, M.Y.; Jabbar, S. Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. *Sustain. Cities Soc.* **2017**, *34*, 90–96. [CrossRef]
15. Jabla, R.; Khemaja, M.; Buendia, F.; Faiz, S. Automatic Rule Generation for Decision-Making in Context-Aware Systems Using Machine Learning. *Comput. Intell. Neurosci.* **2022**, *2022*, 5202537. [CrossRef]
16. Morshed, A.; Jayaraman, P.P.; Sellis, T.; Georgakopoulos, D.; Villari, M.; Ranjan, R. Deep osmosis: Holistic distributed deep learning in osmotic computing. *IEEE Cloud Comput.* **2017**, *4*, 22–32. [CrossRef]
17. Miao, Y.; Liu, Z.; Li, H.; Choo, K.-K.R.; Deng, R.H. Privacy-preserving Byzantine-robust federated learning via blockchain systems. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2848–2861. [CrossRef]
18. Miao, Y.; Xie, R.; Li, X.; Liu, X.; Ma, Z.; Deng, R.H. Compressed Federated Learning Based on Adaptive Local Differential Privacy. In Proceedings of the 38th Annual Computer Security Applications Conference, Austin, TX, USA, 5–9 December 2022; pp. 159–170.
19. Alhothaily, A.; Hu, C.; Alrawais, A.; Song, T.; Cheng, X.; Chen, D. A secure and practical authentication scheme using personal devices. *IEEE Access* **2017**, *5*, 11677–11687. [CrossRef]

20. Castiglioni, I.; Rundo, L.; Codari, M.; Di Leo, G.; Salvatore, C.; Interlenghi, M.; Gallivanone, F.; Cozzi, A.; D'Amico, N.C.; Sardanelli, F. AI applications to medical images: From machine learning to deep learning. *Phys. Med.* **2021**, *83*, 9–24. [CrossRef]
21. Alkatheiri, M.S.; Saleem, S.; Alqarni, M.A.; Aseeri, A.O.; Chauhdary, S.H.; Zhuang, Y. A lightweight authentication scheme for a network of unmanned aerial vehicles (UAVs) by using physical unclonable functions. *Electronics* **2022**, *11*, 2921. [CrossRef]
22. Wang, C.-X.; Huang, J.; Wang, H.; Gao, X.; You, X.; Hao, Y. 6G wireless channel measurements and models: Trends and challenges. *IEEE Veh. Technol. Mag.* **2020**, *15*, 22–32. [CrossRef]
23. Phuong, T.T. Privacy-preserving deep learning via weight transmission. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3003–3015. [CrossRef]
24. Rafique, W.; Qi, L.; Yaqoob, I.; Imran, M.; Rasool, R.U.; Dou, W. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1761–1804. [CrossRef]
25. Gupta, M.; Benson, J.; Patwa, F.; Sandhu, R. Dynamic groups and attribute-based access control for next-generation smart cars. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, Dallas, TX, USA, 25–27 March 2019; pp. 61–72.
26. Yiu, N.C. Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology. *Future Internet* **2021**, *13*, 84. [CrossRef]
27. Atitallah, S.B.; Driss, M.; Boulila, W.; Ghézala, H.B. Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. *Comput. Sci. Rev.* **2020**, *38*, 100303. [CrossRef]
28. Park, J.; Samarakoon, S.; Bennis, M.; Debbah, M. Wireless network intelligence at the edge. *Proc. IEEE* **2019**, *107*, 2204–2239. [CrossRef]
29. Souza, V.; Masip-Bruin, X.; Marín-Tordera, E.; Sànchez-López, S.; Garcia, J.; Ren, G.; Jukan, A.; Ferrer, A.J. Towards a proper service placement in combined Fog-to-Cloud (F2C) architectures. *Future Gener. Comput. Syst.* **2018**, *87*, 1–15. [CrossRef]
30. Zhang, P.; Zhou, M.; Fortino, G. Security and trust issues in fog computing: A survey. *Future Gener. Comput. Syst.* **2018**, *88*, 16–27. [CrossRef]
31. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
32. Laroui, M.; Nour, B.; Moungla, H.; Cherif, M.A.; Afifi, H.; Guizani, M. Edge and fog computing for IoT: A survey on current research activities & future directions. *Comput. Commun.* **2021**, *180*, 210–231.
33. Talal, M.; Zaidan, A.A.; Zaidan, B.B.; Albahri, A.S.; Alamoodi, A.H.; Albahri, O.S.; Alsalem, M.A.; Lim, C.K.; Tan, K.L.; Shir, W.L.; et al. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *J. Med. Syst.* **2019**, *43*, 1–34. [CrossRef]
34. Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wirel. Commun.* **2020**, *27*, 126–132. [CrossRef]
35. Zhang, C.; Liu, X.; Xu, J.; Chen, T.; Li, G.; Jiang, F.; Li, X. An Edge based Federated Learning Framework for Person Re-identification in UAV Delivery Service. In Proceedings of the 2021 IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 5–10 September 2021; pp. 500–505.
36. Taleb, T.; Afolabi, I.; Bagaa, M. Orchestrating 5G network slices to support industrial internet and to shape next-generation smart factories. *IEEE Netw.* **2019**, *33*, 146–154. [CrossRef]
37. Singh, S.K.; Rathore, S.; Park, J.H. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
38. Shen, S.; Zhu, T.; Wu, D.; Wang, W.; Zhou, W. From distributed machine learning to federated learning: In the view of data privacy and security. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6002. [CrossRef]
39. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A survey on security threats and countermeasures in internet of medical things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
40. Khan, S.R.; Sikandar, M.; Almogren, A.; Din, I.U.; Guerrieri, A.; Fortino, G. IoMT-based computational approach for detecting brain tumor. *Future Gener. Comput. Syst.* **2020**, *109*, 360–367. [CrossRef]
41. Amjad, S.; Abbas, S.; Abubaker, Z.; Alsharif, M.H.; Jahid, A.; Javaid, N. Blockchain based authentication and cluster head selection using DDR-LEACH in internet of sensor things. *Sensors* **2022**, *22*, 1972. [CrossRef] [PubMed]
42. Li, J.; Su, Z.; Guo, D.; Choo, K.-K.R.; Ji, Y. PSL-MAAKA: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things. *IEEE Internet Things J.* **2021**, *8*, 13183–13195. [CrossRef]
43. Jiang, Q.; Qian, Y.; Ma, J.; Ma, X.; Cheng, Q.; Wei, F. User centric three-factor authentication protocol for cloud-assisted wearable devices. *Int. J. Commun. Syst.* **2019**, *32*, e3900. [CrossRef]
44. Yang, X.; Yi, X.; Nepal, S.; Khalil, I.; Huang, X.; Shen, J. Efficient and anonymous authentication for healthcare service with cloud based WBANs. *IEEE Trans. Serv. Comput.* **2021**, *15*, 2728–2741. [CrossRef]
45. Izza, S.; Benssalah, M.; Drouiche, K. An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *J. Inf. Secur. Appl.* **2021**, *58*, 102705. [CrossRef]
46. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wireless Personal Commun.* **2021**, *117*, 47–69. [CrossRef]
47. Chunka, C.; Banerjee, S. An efficient mutual authentication and symmetric key agreement scheme for wireless body area network. *Arab. J. Sci. Eng.* **2021**, *46*, 8457–8473. [CrossRef]

48. Wei, F.; Zhang, R.; Ma, C. A provably secure anonymous two-factor authenticated key exchange protocol for cloud computing. *Fundam. Inform.* **2018**, *157*, 201–220. [CrossRef]
49. Deebak, B.D.; Memon, F.H.; Khowaja, S.A.; Dev, K.; Wang, W.; Qureshi, N.M.F. In the digital age of 5G networks: Seamless privacy-preserving authentication for cognitive-inspired internet of medical things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8916–8923. [CrossRef]
50. Abdussami, M.; Amin, R.; Vollala, S. Provably secured lightweight authenticated key agreement protocol for modern health industry. *Ad Hoc Netw.* **2023**, *141*, 103094. [CrossRef]
51. Kim, K.; Ryu, J.; Lee, Y.; Won, D. An Improved Lightweight User Authentication Scheme for the Internet of Medical Things. *Sensors* **2023**, *23*, 1122. [CrossRef]
52. Praveen, R.; Pabitha, P. A secure lightweight fuzzy embedder based user authentication scheme for internet of medical things applications. *J. Intell. Fuzzy Syst.* **2023**, 1–20. [CrossRef]
53. Chen, C.-M.; Liu, S.; Li, X.; Islam, S.H.; Das, A.K. A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. *J. Syst. Archit.* **2023**, *136*, 102831. [CrossRef]
54. Nair, A.K.; Sahoo, J.; Raj, E.D. Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Comput. Stand. Interfaces* **2023**, *86*, 103720. [CrossRef]
55. Gupta, D.S.; Mazumdar, N.; Nag, A.; Singh, J.P. Secure data authentication and access control protocol for industrial healthcare system. *J. Ambient. Intell. Humaniz. Comput.* **2023**, 1–12. [CrossRef]
56. Chatterjee, K.; Singh, A.; Neha; Yu, K. A Multifactor Ring Signature based Authentication Scheme for Quality Assessment of IoMT Environment in COVID-19 Scenario. *ACM J. Data Inf. Qual.* **2023**. [CrossRef]
57. Deebak, B.D.; Al-Turjman, F. Secure-user sign-in authentication for IoT-based eHealth systems. *Complex Intell. Syst.* **2021**, 1–21. [CrossRef]
58. Dharminder, D.; Kumar, U.; Gupta, P. A construction of a conformal Chebyshev chaotic map-based authentication protocol for healthcare telemedicine services. *Complex Intell. Syst.* **2021**, *7*, 1–12. [CrossRef]
59. Dsouza, C.; Ahn, G.J.; Taguinod, M. Policy-driven security management for fog computing: Preliminary framework and a case study. In Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), Redwood City, CA, USA, 13–15 August 2014; pp. 16–23.
60. Sarker, I.H.; Kayes, A.S.M. ABC-RuleMiner: User behavioral rule-based machine learning method for context-aware intelligent services. *J. Netw. Comput. Appl.* **2020**, *168*, 102762. [CrossRef]
61. Shivraj, V.L.; Rajan, M.A.; Singh, M.; Balamuralidhar, P. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In Proceedings of the 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 17–19 February 2015; pp. 1–6.
62. Lu, R.; Heung, K.; Lashkari, A.H.; Ghorbani, A.A. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **2017**, *5*, 3302–3312. [CrossRef]
63. Kumar, P.M.; Gandhi, U.D. Enhanced DTLS with CoAP-based authentication scheme for the Internet of things in healthcare application. *J. Supercomput.* **2020**, *76*, 3963–3983. [CrossRef]
64. Ibrahim, M.H. Octopus: An edge-fog mutual authentication scheme. *Int. J. Netw. Secur.* **2016**, *18*, 1089–1101.
65. Amor, A.B.; Abid, M.; Meddeb, A. A privacy-preserving authentication scheme in an edge-fog environment. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 1225–1231.
66. Xu, G.; Qiu, S.; Ahmad, H.; Xu, G.; Guo, Y.; Zhang, M.; Xu, H. A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography. *Sensors* **2018**, *18*, 2394. [CrossRef] [PubMed]
67. Lee, J.; Yu, S.; Park, K.; Park, Y.; Park, Y. Secure three-factor authentication protocol for multi-gateway IoT environments. *Sensors* **2019**, *19*, 2358. [CrossRef] [PubMed]
68. Yu, S.; Park, K.; Park, Y. A secure lightweight three-factor authentication scheme for IoT in cloud computing environment. *Sensors* **2019**, *19*, 3598. [CrossRef] [PubMed]
69. Watters, P.; Scolyer-Gray, P.; Kayes, A.; Chowdhury, M.J.M. This would work perfectly if it weren't for all the humans: Two factor authentication in late modern societies. *First Monday* **2019**, *24*. [CrossRef]
70. Kalaria, R.; Kayes, A.; Rahayu, W.; Pardede, E. A Secure Mutual Authentication Approach to Fog Computing Environment. *Comput. Secur.* **2021**, *111*, 102483. [CrossRef]
71. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Kumar, N. A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Gener. Comput. Syst.* **2018**, *80*, 483–495. [CrossRef]
72. He, D.; Kumar, N.; Chen, J.; Lee, C.-C.; Chilamkurti, N.; Yeo, S.-S. Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks. *Multimed. Syst.* **2015**, *21*, 49–60. [CrossRef]
73. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and anonymous two-factor authentication protocol for healthcare applications with wireless medical sensor networks. *Multimed. Syst.* **2017**, *23*, 195–205. [CrossRef]
74. Kumari, S.; Om, H. Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. *Comput. Netw.* **2016**, *104*, 137–154. [CrossRef]
75. Farash, M.S.; Chaudhry, S.A.; Heydari, M.; Sadough, S.M.S.; Kumari, S.; Khan, M.K. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *Int. J. Commun. Syst.* **2017**, *30*, e3019. [CrossRef]

76. 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. *Future Gener. Comput. Syst.* **2018**, *82*, 727–737. [CrossRef]
77. Wazid, M.; Das, A.K.; Shetty, S.; JPC Rodrigues, J.; Park, Y. LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment. *Sensors* **2019**, *19*, 5539. [CrossRef]
78. Deebak, B.D. Lightweight authentication and key management in mobile-sink for smart IoT-assisted systems. *Sustain. Cities Soc.* **2020**, *63*, 102416. [CrossRef]
79. Gope, P.; Millwood, O.; Sikdar, B. A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1971–1980. [CrossRef]
80. Subramani, J.; Maria, A.; Rajasekaran, A.S.; Al-Turjman, F. Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3484–3491. [CrossRef]
81. Jiang, Z.; Liu, W.; Ma, R.; Shirazi, S.H.; Xie, Y. Lightweight healthcare wireless body area network scheme with amplified security. *IEEE Access* **2021**, *9*, 125739–125752. [CrossRef]
82. Fadi, A.T.; Deebak, B.D. Seamless authentication: For IoT-big data technologies in smart industrial application systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2919–2927.
83. Kumar, N.; Aujla, G.S.; Das, A.K.; Conti, M. ECCAuth: A secure authentication protocol for demand response management in a smart grid system. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6572–6582. [CrossRef]
84. Kadam, S.S.; Adamuthe, A.C.; Patil, A.B. CNN model for image classification on MNIST and fashion-MNIST dataset. *J. Sci. Res.* **2020**, *64*, 374–384. [CrossRef]
85. Barker, B. Message passing interface (mpi). In *Workshop: High Performance Computing on Stampede*; Cornell University Publisher: Houston, TX, USA, 2015; Volume 262.
86. Zhang, Z.; Cao, X.; Jia, J.; Gong, N.Z. FLDetector: Defending federated learning against model poisoning attacks via detecting malicious clients. In Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Washington, DC, USA, 14–18 August 2022; pp. 2545–2555.
87. Ray, P.P.; Dash, D.; De, D. Internet of things-based real-time model study on e-healthcare: Device, message service and dew computing. *Comput. Netw.* **2019**, *149*, 226–239. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.