IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 September 2023, accepted 21 October 2023, date of publication 30 October 2023, date of current version 2 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3328310

RESEARCH ARTICLE

Privacy-Preserving Big Data Security for IoT With Federated Learning and Cryptography

KAMRAN AHMAD AWAN[1], IKRAM UD DIN[1], (Senior Member, IEEE), AHMAD ALMOGREN[2], (Senior Member, IEEE), AND JOEL J. P. C. RODRIGUES[3], (Fellow, IEEE)

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]COPELABS, Lusófona University, 1749-024 Lisbon, Portugal

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project under Grant RSP2023R184.

ABSTRACT In the ever-expanding Internet of Things (IoT) domain, the production of data has reached an unparalleled scale. This massive data is processed to glean invaluable insights, accelerating a myriad of decision-making processes. Nevertheless, the privacy and security of such information present formidable challenges. This study proposes an innovative methodology for resolving these challenges, by augmenting the privacy and efficacy of big data analytics through federated learning in the IoT ecosystem. The proffered approach amalgamates a hierarchical structure, a scalable learning rate, and a rudimentary cryptographic mechanism to foster learning while ensuring robust privacy and security. Additionally, we introduce a novel communication protocol - SEPP-IoT, designed to facilitate efficient, secure, and confidential interactions between IoT devices and a central server. In our pursuit of optimizing communication overhead, we propose an adaptive data compression algorithm, aimed at curbing the volume of data transferred between IoT devices and the central server. To fortify resilience and fault tolerance, our approach incorporates multiple mechanisms such as data replication, error correction codes, and proactive fault detection and recovery. Trust management, a salient feature of our framework, bolsters the security and integrity of federated learning. We recommend a unique technique that gauges the dependability of IoT nodes using four trust parameters. We employ the FedSim simulator to evaluate our method's effectiveness. The results indicate a notable enhancement in privacy and efficiency of big data analytics within the IoT.

INDEX TERMS Internet of Things, big data, security, privacy preservation, federated learning, cryptography, trust management, adaptive learning, trustworthiness.

I. INTRODUCTION

The advent of the Internet of Things (IoT) [1] has led to a networked ecosystem of physical entities, encompassing a myriad of appliances, vehicles, and objects, which are vested with the ability to connect and exchange data due to their embedded software and sensors [2]. The exponential growth of the IoT paradigm [3] has engendered a tremendous surge in the volume, diversity, and speed of data generated by these devices. This profusion of data, termed Big Data, has evolved into a crucial resource across an array of sectors. Big Data, garnered from IoT devices, can be aggregated and analyzed to unravel patterns, preferences, and behavioral insights [4] conducive to informed decision-making and enhancement of operational efficiencies. A deep-seated interrelation exists between Big Data and IoT, with IoT being the predominant progenitor of this data [5]. The IoT network-connected sensors and devices churn out vast quantities of data [6], which are consequently dispatched to centralized servers or cloud-based platforms for storage

The associate editor coordinating the review of this manuscript and approving it for publication was Nurul I. Sarkar.

and analytical processing. The inferences drawn from these data can potentiate streamlined operations, innovation of products and services, and fortify market positioning. With the continual growth in the volume and heterogeneity of IoT device-generated data, the security of this data has emerged as a critical concern. Given that the data from IoT devices often encapsulates sensitive personal or corporate information, it becomes a potential target for cyberattacks [7]. Therefore, ensuring robust Big Data security in IoT [8] becomes imperative to fend off data breaches [9], cyber threats, and other malicious attacks [10], the consequences of which can be severe, including substantial financial losses, reputation damage, and legal liabilities. The Big Data generated by IoT devices presents a plethora of security challenges [11], such as data privacy [12], data management [13], and network security [14]. Ensuring data privacy necessitates the implementation of robust access controls and data encryption strategies [15], while the efficient and scalable management of the colossal data produced by IoT devices requires competent storage, processing, and retrieval systems. Additionally, network security is pivotal for the safe transmission of data, preventing unauthorized access or tampering.

Encompassing our physical environment, the IoT has instigated a paradigm shift in our modes of interaction with the physical realm. This transformation has culminated in the creation of intelligent systems capable of assimilating and scrutinizing data from heterogeneous sources, thereby facilitating insightful analysis and giving rise to novel applications. The data deluge generated by IoT devices, also known as Big Data [16], is typified by its substantial volume, high velocity, rich variety, and excellent veracity. Such comprehensive data analysis can significantly augment operational efficiency, decision-making acuity, and customer satisfaction for businesses. However, the escalating proliferation of IoT devices, coupled with the expansion of Big Data [17], has rendered data security a paramount concern. The sensitivity of the data procured by IoT devices implies that unauthorized access or exploitation could yield severe ramifications [18]. For instance, a malevolent actor might leverage security vulnerabilities in an IoT device to gain unauthorized access to the device or the data it generates, potentially resulting in data theft, data tampering [19], or denial-of-service attacks [20].

Furthermore, integrating federated learning into IoT systems poses its unique set of challenges, such as managing concurrency in a distributed IoT device environment, which can be a formidable task. To counteract this, our proposed method incorporates a specialized mechanism adept at efficiently handling concurrency, thus guaranteeing smooth and coordinated operations across devices. The heterogeneity of IoT devices necessitates addressing the crucial issue of resource allocation. Devices vary significantly in resources such as processing power, memory, and energy, thereby mandating the establishment of proficient resource allocation mechanisms to ensure each device's contribution to the learning process without being burdened by resource constraints. Additionally, optimizing the number of computing rounds is vital for the efficiency of federated learning. Excessive rounds could inflate communication overhead and energy consumption [21], whereas an inadequate number of rounds could undermine the learning outcome. Our approach has been architectured to dynamically adjust the number of computing rounds based on the system's current state, thereby striking an equilibrium between efficiency and learning quality.

Federated learning's applicability in IoT permeates various sectors. In the healthcare domain, federated learning can enable the creation of predictive models based on patient data from disparate healthcare establishments while preserving patient privacy [22]. In the agricultural sector, federated learning can assist in the analysis of data from multiple farms to make accurate predictions about crop yields, pest infestations, and other significant events, thus bolstering agricultural practices. For smart cities, federated learning can be harnessed to analyze data from a plethora of IoT devices dispersed across the city to optimize resources, enhance services, and ameliorate the overall quality of life.

Traditional security measures fail to adequately secure Big Data generated by IoT devices [23]. The resource constraints inherent to IoT devices further complicate the deployment of robust security mechanisms [24]. These challenges necessitate the development of an innovative strategy tailored for safeguarding Big Data generated by IoT devices. The proposed methodology aims to provide a secure and scalable solution for IoT devices participating in federated learning. This machine learning paradigm trains a global model using data from multiple devices, precluding the necessity for data transmission to a central server, thereby offering enhanced privacy, scalability, and energy efficiency. To secure the privacy of data transmitted during federated learning, cryptographic techniques are integrated into the proposed approach. The methodology also incorporates fault tolerance mechanisms to ensure the reliability of communication between IoT devices and the central server. The approach provides a scalable and reliable solution to the security challenges posed by Big Data generated by IoT devices. A novel trust management protocol proposed in the study secures the federated learning process within IoT networks. The protocol employs four trust parameters-honesty, model accuracy, resource utilization, and communication reliability-to evaluate the dependability of IoT devices involved in federated learning. Based on these parameters, the protocol computes a trust score for each device and compares it with a predetermined threshold. If a device's trust score exceeds the threshold, it is deemed trustworthy and awarded a certificate of trustworthiness. The contributions of the proposed methodology can be summarized as follows:

1) The approach employs federated learning in IoT to enhance the privacy and efficiency of big data analytics. This is achieved through an innovative aggregation

algorithm, adaptive learning rates, and a hierarchical architecture that optimizes the learning process.
2) A lightweight cryptographic solution is provided for IoT devices engaged in federated learning. This solution ensures robust security while minimizing computational and energy expenditures.
3) The communication protocol, termed SEPP-IoT, addresses the unique challenges posed by federated learning in IoT environments, ensuring efficiency, privacy, and security.
4) An adaptive data compression algorithm minimizes communication overhead and data transmission between IoT devices and the central server. It dynamically selects the most effective compression technique based on data type, available bandwidth, and the computational capabilities of the IoT devices.
5) The proposed methodology integrates several mechanisms into the communication protocol to ensure fault tolerance and resilience.
6) Trust management is incorporated into the proposed federated learning framework, using four trust parameters to assess the trustworthiness of IoT nodes.

The structure of the paper is as follows: Section II will provide background information and discuss existing approaches for securing big data generated by IoT devices, as well as their limitations. Section III will describe the proposed approach in detail. Section IV will present the results of experimental simulations. Finally, Section V will summarize the proposed approach, highlight its main contributions, and discuss future work and possible extensions of the research.

II. BACKGROUND AND RELATED WORK

Recent years have seen a significant increase in interest in the integration of IoT, big data, and various computing technologies, sparking extensive research in the area. An overview of recent developments in this field will be given in this literature review, with a focus on security and privacy issues as well as cutting-edge applications and techniques. As shown in Table 1, the section will also discuss any shortcomings of current approaches and lay out potential future research avenues.

A new method for monitoring diabetes in IoT environments made possible by 5G technology is proposed in Venkatachalam et al. [25]. This method combines a deep belief neural network (DBNN) model for precise blood glucose level prediction with an edge computing framework for effective big data processing. While protecting patient data's security and privacy, the system shows promise in healthcare applications. The integration of cloud computing, big data, and IoT technologies in healthcare, smart cities, and agriculture is covered by Rani et al. in [26]. The authors examine the potential advantages and difficulties resulting from the integration of these technologies, emphasizing the necessity of effective data processing, storage, and security mechanisms for successful implementation.

In [27], the authors examine the security and privacy issues that arise in IoT-based big data cloud systems that are operating in a digital twin environment. The integration of IoT, big data, and cloud computing technologies is examined by the authors in terms of potential risks, weaknesses, and difficulties. They offer a number of solutions, such as the use of sophisticated encryption methods and reliable access control mechanisms, to mitigate these problems. In [28], the authors explore the use of intrusion detection systems (IDS) in big data environments based on the Internet of Things. The authors examine various IDS techniques, including signature-based, anomaly-based, and specification-based strategies, and their use in Internet of Things big data systems. They emphasise the critical function of IDS solutions in protecting the accuracy of data collection and securing IoT networks. An overview of the technologies powering Healthcare 4.0, powered by IoT, is provided in [8]. They talk about the opportunities and problems that come with the adoption of cutting-edge technologies like blockchain, big data analytics, and artificial intelligence in the healthcare industry. In order to meet the future demand for increasingly individualized and data-driven healthcare services, the authors stress the importance of developing secure, effective, and privacy-preserving solutions.

The authors of [29] introduced a novel technique for detecting cybercrime in IoT infrastructures that make use of big data. The framework analyses and correlates data from IoT devices using deep learning and neuro-fuzzy techniques, and they emphasise the potential for cutting-edge machine learning techniques to enhance the cybersecurity of big data and IoT systems. In [30], the authors look into various anonymization techniques that are suitable for big data and IoT environments. The purpose of the paper is to assess the effectiveness of various methods for maintaining data usefulness while maintaining privacy, including k-anonymity, l-diversity, and t-closeness. The authors stress the significance of effective anonymization techniques for maintaining the analytical power of big data and IoT systems while protecting data privacy.

With a focus on security issues, challenges, and recommendations, the authors of [36] explore the use of blockchain technology in energy trading, smart grid, and big data. The authors address concerns about data privacy while highlighting the potential advantages of blockchain for enhancing the security, openness, and effectiveness of energy management systems. To reduce the rising security risks in the energy sector, they emphasise the need for more study on fusing blockchain with IoT and big data systems. A security framework for IoT big data in cloud environments that combines stream cypher and clustering techniques is proposed in [37]. To improve data transmission security and stream cypher performance in the cloud, the proposed method uses a lightweight stream cypher algorithm and clustering model. The authors use the integration of data processing and cryptographic techniques to show how this strategy

TABLE 1. Comparative analysis of the discussed articles.

Ref.	Contribution	Limitation	Future Direction	Computing Location
[25]	Deep belief neural network for diabetes monitoring in 5G edge IoT	Limited to diabetes monitoring	Explore other health monitoring applications	Edge
[26]	Integration of IoT, big data, and cloud computing technologies	Lacks in-depth analysis of specific security issues	Investigate security mechanisms for the integrated systems	N/A
[27]	This article will address the security and privacy concerns associated with big data cloud systems based on IoT technology, particularly in a digital twin scenario.	Limited to a digital twin scenario	Extend the analysis to other application scenarios	Cloud
[28]	Intrusion detection systems for IoT-based big data	Focuses on intrusion detection only	Study other security aspects like data privacy and secure data processing	N/A
[8]	Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies	Broad survey, lacks focus on specific security issues	Investigate security mechanisms for Healthcare 4.0 technologies	N/A
[29]	an optimized deep neuro-fuzzy network that can be used for cyber forensic investigation in IoT infrastructures based on big data.	Limited to cyber forensic investigation	Explore other security aspects in big data-based IoT infrastructures	Edge
[30]	Data anonymization evaluation for big data and IoT environment	Focuses on data anonymization only	Investigate other privacy-preserving techniques for big data and IoT environments	Cloud
[31]	Secure big data processing in multihoming networks with AI-enabled IoT	Limited to multihoming networks	Extend the analysis to other network environments	Edge
[32]	Analyzing big data security through a unified decision-making approach	Focuses on risk assessment, access control, and intrusion detection	Investigate other security aspects in big data systems	Cloud
[33]	Big data precision marketing approach under IoT cloud platform information mining	Focuses on marketing applications	Investigate other application domains and their security challenges	Cloud
[34]	Explores safety measures driven by semantics in big data systems distributed over IoT.	Focuses on semantics-driven safety	Examine additional safety and security aspects that exist in distributed big data systems deployed on IoT.	N/A
[35]	Integration of edge computing and blockchain for data fusion and secure big data analysis for IoT	Focuses on edge computing and blockchain integration	Investigate other integration possibilities for secure big data analysis in IoT	Edge

can improve the security and effectiveness of IoT big data systems. Venu et al. [31] propose a framework that combines AI techniques with network layer security controls to ensure effective and secure data processing in IoT environments. The availability, confidentiality, and integrity of data in multihoming networks are just a few of the security issues that this method addresses in IoT big data systems.

A unified decision-making strategy is proposed in [32], which combines risk assessment, access control, and intrusion detection methods to improve big data system security. This strategy highlights the importance of putting in place a thorough security strategy to handle the escalating problems of big data and IoT environments. Li et al. [33] proposed a technique for precision marketing using information mining from big data and IoT cloud platforms. The strategy aims to develop customized marketing strategies while protecting the security and privacy of customer information. The study emphasizes how integrating IoT, big data analytics, and cloud computing technologies in various business applications and processes has the potential to transform entire industries.

Mohapatra et al. [38] suggested a fiber Bragg grating (FBG) sensors to drive a structural health monitoring system that incorporates multimedia-enabled IoT and big data technology. By combining these technologies, they highlighted the potential for enhanced monitoring accuracy and effectiveness while still prioritizing data security and privacy. To address the increasing demand for smart infrastructure systems, the authors stressed the importance of continued research into integrating these technologies. Vanga et al. [34] delved into the topic of safety measures driven by semantics in IoT-based distributed big data systems. They put forward a framework that incorporates semantic web technologies to enhance data security and safety in such systems. The authors demonstrated the efficacy of semantic technologies in mitigating the rising safety and security concerns in distributed big data environments.

A framework that combines edge computing and blockchain technology has been proposed in [35] to increase the security, efficacy, and scalability of IoT-based big data systems. This study shows how edge computing and

blockchain can work together to address the growing privacy and security concerns in IoT environments. Manzoor et al. [39] propose a platform that makes use of proxy re-encryption and blockchain technology to create secure and private IoT data exchange. This method ensures end-to-end data security and permits safe data sharing by using proxy re-encryption to securely re-encrypt data without the need for decryption. To guarantee the accuracy and transparency of data-sharing operations, the platform uses the decentralized and tamper-proof features of blockchain technology.

In recent years, Edge Computing has emerged as a promising solution to overcome the challenges of latency, bandwidth usage, and privacy in Federated Learning (FL) [40]. It empowers IoT devices to perform computations on the data locally, which contributes to reducing the communication overhead, and improves the real-time processing capabilities of FL models [41]. However, implementing FL at the edge introduces its unique privacy and security concerns. One of the primary concerns is data privacy, as sensitive data from individual devices could be potentially exposed during the model aggregation process [42]. Further, device authentication becomes crucial to prevent malicious devices from participating in the learning process and injecting false updates, which could adversely affect the global model's performance [43]. Secure communication between the edge devices and the server is another critical issue. Protecting the exchanged model updates from interception and tampering is important to ensure the integrity of the global model [44]. Lastly, ensuring secure computation at the edge nodes is a major challenge, considering the limited computational capabilities of IoT devices [45].

With the proliferation of IoT systems, the preservation of privacy and assurance of security have become paramount. The inherently decentralized architecture of IoT, coupled with the heterogeneity of devices and the vast amounts of data generated, present complex challenges. Moreover, due to the large-scale and open nature of IoT networks, traditional security mechanisms, such as firewalls and intrusion detection systems, are inadequate. Addressing these privacy and security challenges requires comprehensive and robust solutions that can effectively handle the complexities inherent in IoT systems. For instance, novel cryptographic techniques, such as homomorphic encryption, can be used to enable secure computations on encrypted data [46], ensuring data privacy [47]. Similarly, blockchain-based solutions can ensure data integrity and non-repudiation in IoT systems [48]. Also, machine learning-based anomaly detection can be leveraged to detect and mitigate various forms of cyberattacks [49].

III. PROPOSED APPROACH

The proposed novel strategy intends to merge federated learning and lightweight cryptography to build an IoT framework for big data analytics with privacy protection. This section provides an overview of the essential elements of our approach, which include federated learning, lightweight cryptography, and the entire design of the proposed framework.

A. ARCHITECTURE AND COMPONENTS

The overall architecture of the proposed privacy-preserving big data analytics framework for IoT is designed to maximize efficiency, security, and privacy. We achieve this by combining federated learning, lightweight cryptography, and a carefully designed system architecture consisting of the following key components as discussed below whereas Figure 1 illustrate the working flow of the proposed appraoch:

1) **IoT Devices:** IoT devices use encrypted data and lightweight cryptography for security when producing, storing, handling, and taking part in federated learning. In order to contribute to the management of trust for the strength and dependability of the system, they also actively monitor and report on the actions of their own and nearby devices.
2) **Central Server:** Federated learning must be managed by a central server. It gathers encrypted updates to the global model from IoT devices, decrypts them, updates the global model, and then sends the updated global model back to IoT devices for additional development. To improve system security and efficiency, it can also examine the combined models for odd patterns or irregularities.
3) **Communication Protocol:** For seamless sharing of model updates and pertinent information between IoT devices and the central server, a secure communication protocol is created. It ensures data privacy and integrity while reducing communication load by using lightweight cryptography. Additionally enhancing privacy guarantees for federated learning, the protocol is compatible with secure multi-party computation techniques.
4) **Model Management:** To guarantee that IoT devices have access to the most recent models and increase the effectiveness and accuracy of the learning process, the model management module is in charge of storing, versioning, and sharing local and global models. This module also maintains the security of the system by distributing and storing encrypted models in a secure manner.
5) **Trust Management:** The proposed framework adds a further layer of trust management to strengthen security measures. In the federated learning process, this component evaluates the dependability of IoT devices and identifies any compromised or malicious devices. Reputation-based systems, behavior-based systems, and machine learning algorithms are just a few examples of the many methods that can be used. By monitoring and upholding trust levels among IoT devices, trust management ensures system integrity, durability, and confidentiality.

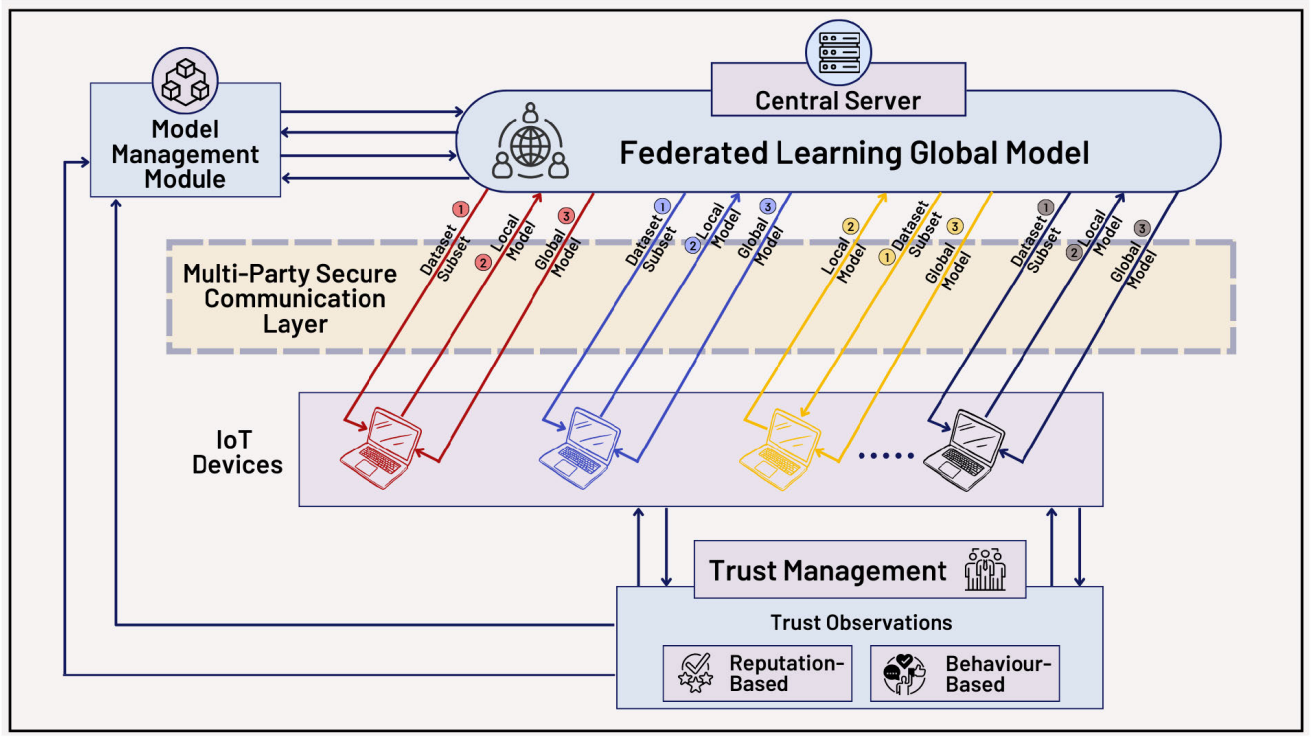

FIGURE 1. The proposed working architecture.

These elements function as a cohesive whole to accomplish the goals of our suggested strategy. IoT devices cooperate in the federated learning process, which is supported by the communication protocol and secured by simple cryptographic methods. Model management guarantees quick and secure access to the most recent models while the central server coordinates the entire process. By upholding a high standard of security and robustness throughout the learning process, trust management protects the system.

B. FEDERATED LEARNING FOR IoT

Our innovative approach presented in this section focuses on the utilization of federated learning in IoT to improve the efficiency and privacy of big data analytics. Our novel method employs an aggregation algorithm, adaptive learning rates, and a hierarchical architecture to optimize the learning process in the context of IoT.

1) NOVEL AGGREGATION ALGORITHM

The key innovation in our approach is the use of a novel aggregation algorithm that improves the convergence and accuracy of the global model by considering the quality and diversity of local models as represented by Algorithm 1 where as the mathematical symbols are illustrated by Table 2.

Let n be the total number of IoT devices, and let w_i be the local model parameters of the i-th device. Our aggregation algorithm computes the global model parameters W as:

$$W = \sum_{i=1}^{n} \alpha_i w_i, \tag{1}$$

where α_i is a weighting factor for each device, calculated as:

$$\alpha_i = \frac{\beta_i}{\sum_{j=1}^{n} \beta_j}, \tag{2}$$

and β_i is a measure of the quality and diversity of the local model w_i, defined as:

$$\beta_i = \gamma_i \cdot \exp\left(-\eta \cdot d_i\right), \tag{3}$$

where γ_i is the accuracy of the local model w_i, d_i is the distance between the local model w_i and the current global model, η is a positive constant controlling the trade-off between quality and diversity, and $\exp(\cdot)$ is the exponential function.

2) ADAPTIVE LEARNING RATES

To further optimize the learning process, we employ adaptive learning rates for each IoT device. The learning rate λ_i for the i-th device is updated based on the local model's quality and the device's resource constraints, as follows:

$$\lambda_i(t) = \lambda_0 \cdot \frac{\gamma_i(t)}{\max j = 1, \ldots, n\gamma_j(t)} \cdot \frac{R_i}{\max j = 1, \ldots, nR_j}, \tag{4}$$

where λ_0 is the initial learning rate, $\gamma_i(t)$ is the accuracy of the local model w_i at iteration t, R_i is the available resources (e.g., computation, energy) of the i-th device, and $\max(\cdot)$ denotes the maximum function.

Algorithm 1 Novel Federated Learning Aggregation Algorithm With Adaptive Learning Rates

Input: Local model parameters w_i for $i = 1, \ldots, n$, current global model W, initial learning rate λ_0, resource constraints R_i, and constant η

Output: Updated global model parameters W

for *each local model* w_i **do**
  Compute the local model accuracy γ_i;
  Compute the distance d_i between the local model w_i and the current global model W;
  Calculate β_i as:

$$\beta_i = \gamma_i \cdot \exp(-\eta \cdot d_i)$$

for *each local model* w_i **do**
  Compute the weighting factor α_i as:

$$\alpha_i = \frac{\beta_i}{\sum_{j=1}^{n} \beta_j}$$

Update global model parameters W as:

$$W = \sum_{i=1}^{n} \alpha_i w_i$$

for *each local model* w_i **do**
  Update the learning rate $\lambda_i(t)$ as:

$$\lambda_i(t) = \lambda_0 \cdot \frac{\gamma_i(t)}{\max_{j=1,\ldots,n} \gamma_j(t)} \cdot \frac{R_i}{\max_{j=1,\ldots,n} R_j}$$

return W;

C. INTEGRATION AND WORKFLOW

The proposed federated learning technique is integrated into our framework of privacy-preserving big data analytics, which was explained in the previous section. The learning process follows the standard federated learning workflow but with modifications to include our novel aggregation algorithm, adaptive learning rates, and hierarchical architecture. The modified workflow can be described as follows:

1) Data is collected and stored on IoT devices, with sensitive information encrypted using lightweight cryptographic algorithms. Let the encrypted data on device i be:

$$x_i = Enc(x_i') \tag{5}$$

2) IoT devices are organized into clusters, and a local aggregator is selected for each cluster. Suppose we have m clusters and n devices.
3) IoT devices train local machine learning models on their encrypted data. The local model update for device i at iteration t is given by:

$$w_i^t = Train(x_i, y_i, w^{t-1}) \tag{6}$$

where y_i are the labels and w^{t-1} is the model from the previous iteration.

4) Model updates are encrypted and securely transmitted to the local aggregator within the cluster. The encrypted update is:

$$\hat{w}_i^t = Enc(w_i^t) \tag{7}$$

TABLE 2. List of mathematical symbols.

Symbol	Description
n	Total number of IoT devices
w_i	Local model parameters of the i-th device
W	Global model parameters
λ_0	Initial learning rate
α_i	Weighting factor for each device
β_i	Measure of quality and diversity of the local model
γ_i	Accuracy of the local model
d_i	Distance between local and global models
η	Positive constant controlling trade-off
$\exp(\cdot)$	Exponential function
R_i	Resource constraints of the i-th device
$\lambda_i(t)$	Learning rate of the i-th device at iteration t
$\max(\cdot)$	Maximum function
x_i	Encrypted data on device i
y_i	Labels for device i
$\hat{w}_i^t$	Encrypted update for device i at iteration t
$\hat{W}_k^t$	Intermediate global model for cluster k at iteration t
$\check{W}_k^t$	Encrypted intermediate global model for cluster k
W^t	Final global model at iteration t
M	Message sent by the cluster leader
m_i	i-th bit of the message M
p_i	Probability that m_i is corrupted
P_{corr}	Probability that M is corrupted
N	Number of cluster members
p	Probability that a single cluster member fails
P_{fail}	Probability that a cluster fails
$R_{\text{comm},i}$	Communication reliability of node i
$R_{\text{res},i}$	Resource utilization of node i
$R_{\text{acc},i}$	Model accuracy of node i
$R_{\text{hon},i}$	Honesty of node i
T_i	Overall trustworthiness score of node i
T_{th}	Trustworthiness threshold
$N_{\text{succ},i}$	Number of successful communication attempts by node i
$N_{\text{att},i}$	Total number of communication attempts by node i
U_i	Current resource utilization of node i
C_i	Maximum capacity of node i
acc$i$	Accuracy of the local model trained by node i
$\text{acc}_{\max}$	Maximum achievable accuracy
$w_1, \ldots, w_4$	Weights for trust parameters

5) The local aggregator computes an intermediate global model using the novel aggregation algorithm, considering the quality and diversity of local models:

$$\hat{W}_k^t = \sum_{i=1}^{n_k} \alpha_i^t \hat{w}_i^t, \quad k = 1, \ldots, m \tag{8}$$

6) Intermediate global models from local aggregators are encrypted and securely transmitted to the central server. The encrypted intermediate global model is:

$$\check{W}_k^t = Enc(\hat{W}_k^t) \tag{9}$$

7) The central server aggregates the encrypted intermediate global models, decrypts them, and updates the final global model using the same aggregation algorithm:

$$W^t = \sum_{k=1}^{m} \beta_k^t Dec(\check{W}_k^t) \tag{10}$$

8) IoT devices use the updated final global model to refine their local models and repeat the process:

$$w_i^{t+1} = Train(x_i, y_i, Dec(\bar{W}^t)) \tag{11}$$

D. LIGHTWEIGHT CRYPTOGRAPHY FOR IoT

This section introduces a new lightweight cryptographic technique that is tailored to IoT devices in the context of federated learning. Our approach aims to provide strong security while reducing computational and energy expenses for low-resource devices. The critical elements of our suggested methodology comprise:

1) DYNAMIC KEY MANAGEMENT

Our method utilizes a dynamic key management system that enables secure and effective key generation, distribution, and revocation. The complete process of cryptography for federated IoT is illustrated by Algorithm 2. To generate unique keys, we employ a lightweight key generation algorithm that allows IoT devices to generate their key pairs (pk_i, sk_i). The public keys pk_i are then securely transmitted to the central server, which maintains a key directory for all participating devices.

We suggest a method for refreshing keys and minimizing the possibility of long-term key vulnerability. Our proposal involves a key update mechanism that relies on a time-constrained validity period. When the predetermined period T elapses, IoT devices create new key pairs and notify the central server of the update.

2) IoT DEVICE DATA ENCRYPTION

To protect sensitive data stored on IoT devices, we propose a lightweight symmetric encryption algorithm denoted as Enc(·). Let D_i represent the data of the i-th IoT device and k_i be the encryption key derived from the device's private key sk_i. The encrypted data $\hat{D}_i$ can be calculated as:

$$\hat{D}i = \text{Enc}k_i(D_i). \tag{12}$$

3) SECURE MODEL UPDATE TRANSMISSION

For securely transmitting model updates from IoT devices to the central server, we propose a lightweight asymmetric encryption scheme. Let U_i represent the model update from the i-th IoT device. The encrypted model update $\hat{U}_i$ can be computed as:

$$\hat{U}i = \text{Enc}pk_s(U_i), \tag{13}$$

where pk_s is the public key of the central server.

4) SECURE MULTI-PARTY COMPUTATION FOR MODEL AGGREGATION

In order to increase the level of privacy protection offered by federated learning, we integrate secure multi-party computation (SMPC) methods into the process of model aggregation. This enables the central server to aggregate model updates without directly accessing each individual update.

We define an SMPC protocol SMPC(·) that takes encrypted model updates $\hat{U}i$ as input and outputs an encrypted aggregated model update $\hat{U}agg$:

$$\hat{U}_{agg} = \text{SMPC}\left(\hat{U}_1, \hat{U}_2, \ldots, \hat{U}_n\right), \tag{14}$$

where n is the total number of participating IoT devices.

5) DECRYPTION OF AGGREGATED MODEL UPDATES

Finally, the central server decrypts the aggregated model update $\hat{U}agg$ using its private key sk_s. The decrypted aggregated model update $Uagg$ can be computed as:

$$U_{agg} = \text{Dec}sk_s(\hat{U}agg). \tag{15}$$

The usage of a lightweight cryptographic technique guarantees the safeguarding of confidential data stored on IoT devices and provides security for communication between the devices and the central server. Moreover, this approach leverages secure multi-party computation techniques to further enhance the privacy protection of federated learning.

E. COMMUNICATION PROTOCOL

The proposed communication protocol, named Secure Efficient Privacy-preserving Protocol for IoT (SEPP-IoT), aims to tackle the difficulties posed by federated learning in IoT settings. It achieves this by guaranteeing security, privacy, and efficiency. The complete workflow of the proposed protocol is illsutrated by Algorithm 3 whereas the essential characteristics of SEPP-IoT are:

1) HIERARCHICAL CLUSTERING

Our suggested strategy involves grouping IoT devices into clusters. Each cluster is headed by a designated leader who is in charge of communicating with the central server. This hierarchical arrangement lessens communication burden and distributes workload among devices. The process of forming clusters involves the subsequent stages:

1) Each device i calculates a measure of similarity between its local model w_i and the current global model W.

Algorithm 2 Lightweight Cryptography for Federated IoT

Input: IoT devices $D_1, D_2, \ldots, D_n$, central server S

Initialization:
for *each IoT device* D_i **do**
  Generate key pair (pk_i, sk_i);
  Send pk_i to the central server;
Data Encryption:
for *each IoT device* D_i **do**
  Derive encryption key k_i from sk_i;
  Encrypt local data: $\hat{D}_i \leftarrow \text{Enc}_{k_i}(D_i)$;
Federated Learning:
while *not converged* **do**
  for *each IoT device* D_i **do**
    Train local model and compute update U_i;
    Encrypt model update: $\hat{U}_i \leftarrow \text{Enc}_{pk_s}(U_i)$;
    Send $\hat{U}_i$ to the central server;
  Model Aggregation: Aggregate encrypted model updates using SMPC:;
    $\hat{U}_{agg} \leftarrow \text{SMPC}\left(\hat{U}_1, \hat{U}_2, \ldots, \hat{U}_n\right)$;
  Decrypt aggregated model update: $U_{agg} \leftarrow \text{Dec}_{sk_s}(\hat{U}_{agg})$;
  Update global model with U_{agg};
  Send updated global model to IoT devices;

2) Based on these similarity measures, the devices are partitioned into K initial clusters using a clustering algorithm, such as k-means or hierarchical clustering.
3) Each cluster elects a leader device based on criteria such as device capabilities or trustworthiness.
4) The leaders communicate with each other and with the central server to form a hierarchical structure, with the top level consisting of a single leader communicating with the central server.

Let C_k denote the k-th cluster in the hierarchical structure, with L_k being the leader device for that cluster. Each device i belongs to exactly one cluster, denoted as C_{k_i}. The communication between the devices and the central server is handled through the leaders L_k. The following steps outline the communication process between the leaders and the central server:

1) Each device i computes the difference between its local model and the current global model, denoted as $\Delta w_i = w_i - W$.
2) The leader device L_{k_i} aggregates the local model differences from devices in its cluster C_{k_i} to obtain a cluster-level update ΔW_{k_i}.
3) The top-level leader aggregates the cluster-level updates from all leaders to obtain the global update ΔW.
4) The current global model W is updated by adding the global update ΔW to the previous global model W, i.e., $W = W + \Delta W$.
5) The updated global model is shared with all leaders for further dissemination to their respective clusters.

The method of hierarchical clustering effectively decreases the communication burden by restricting the quantity of devices that communicate with the central server. At the same time, it ensures an even distribution of workload among the devices.

Algorithm 3 Novel Communication Protocol with Hierarchical Clustering

Input: IoT devices, central server, security parameters, clustering parameters
Output: Updated global model

Divide IoT devices into clusters using hierarchical clustering;
Select a leader for each cluster;
For: each training iteration
For: each cluster leader Compute local model update w_i for each device i in the cluster;
Encrypt the local model update using the public key pk_j of the leader as: $Enc(w_i) = E_{pk_j}(w_i)$;
Send the encrypted update to the central server using secure communication protocol;
Aggregate local model updates from all cluster leaders to obtain updated global model W as:;
  $W = \sum_{j=1}^{k} w_j \alpha_j$;
where k is the number of clusters, w_j is the local model update from the j-th cluster leader, and α_j is the weighting factor for the j-th cluster leader, calculated as:;
  $\alpha_j = \frac{\beta_j}{\sum_{l=1}^{k} \beta_l}$;
and β_j is a measure of the quality and diversity of the local model update from the j-th cluster leader, defined as:;
  $\beta_j = \gamma_j \cdot \exp\left(-\eta \cdot d_j\right)$;
Here, γ_j is the accuracy of the local model update from the j-th cluster leader, d_j is the distance between the local model update w_j and the current global model W, η is a positive constant controlling the trade-off between quality and diversity, and $\exp(\cdot)$ is the exponential function.;
Share the updated global model with all cluster leaders;
each cluster leader Decrypt the global model using its private key sk_j as: $W_j = D_{sk_j}(W)$;
Distribute the updated model W_j to its cluster members;
return Updated global model

2) DIFFERENTIAL PRIVACY-BASED MODEL

To augment the privacy assurances of our suggested framework, we integrate differential privacy methods into the model update process. This technique offers a precise

mathematical foundation for evaluating and regulating the privacy hazard of data processing algorithms (as shown in Algorithm 4).

In our approach, we include arbitrary noise to the local model updates before transmitting them to the central server. This random noise guarantees that the contributions made by individual devices to the global model are indistinguishable, ensuring robust privacy protection. We use the Laplace mechanism, which adds noise extracted from a Laplace distribution with an average of 0 and a magnitude determined by the sensitivity of the aggregation function.

Let $f(\cdot)$ be the aggregation function used to combine the local model updates. We define the sensitivity of $f(\cdot)$ as the maximum amount by which $f(\cdot)$ changes when a single device's local model update changes. Formally, we have:

$$\Delta f = \max_{w_i, w_i'} ||f(w_1, \ldots, w_i, \ldots, w_n) - f(w_1, \ldots, w_i', \ldots, w_n)||_2 \tag{16}$$

where w_i and w_i' are the local model updates of device i before and after a single data point is added or removed.

We add Laplace noise to the local model updates as follows:

$$w_i^{\text{priv}} = w_i + \text{Laplace}\left(\frac{\Delta f}{\epsilon}\right) \tag{17}$$

where w_i^{priv} is the differentially private local model update, ϵ is the privacy budget controlling the trade-off between privacy and utility, and Laplace(b) denotes the random noise drawn from a Laplace distribution with scale parameter b.

The noisy local model updates are then sent to the central server, where they are aggregated using the same function $f(\cdot)$. The global model is then returned to each device, and the process repeats for each training iteration. The algorithm for the differential privacy-based model updates is shown below in Algorithm 4.

Algorithm 4 Differential Privacy-Based Model Updates

Input: Local model parameters w_i for $i = 1, \ldots, n$, aggregation function $f(\cdot)$, privacy budget ϵ
Output: Updated global model parameters W

for *each local model* w_i **do**
  Compute the sensitivity of $f(\cdot)$ as Δf;
  Add Laplace noise to the local model update: $w_i^{\text{priv}} = w_i + \text{Laplace}\left(\frac{\Delta f}{\epsilon}\right)$;
Aggregate the differentially private local model updates to obtain updated global model parameters W: $W = f(w_1^{\text{priv}}, \ldots, w_n^{\text{priv}})$;
return W

3) ADAPTIVE DATA COMPRESSION

Our proposal aims to minimize communication overhead and decrease the volume of data transmitted between IoT devices and the central server. We suggest an adaptive data compression algorithm that employs both lossless and lossy compression methods. This algorithm intelligently chooses the most suitable compression technique based on the type. Let x be the data to be transmitted, and let $c(x)$ be the compressed data. The adaptive compression algorithm is represented by Algorithm 5. The adaptive compression algorithm consists of the following steps:

1) **Data analysis:** The statistical traits of the data to be sent, such as its entropy and autocorrelation, are examined by the algorithm. This information is then utilized to determine the compression method that is most suited for the data.
2) **Compression:** After analyzing the data, the algorithm chooses the appropriate compression method, either lossless or lossy. For lossless compression, methods such as Huffman coding or arithmetic coding are utilized, which have been widely used and are well-known. For lossy compression, methods such as discrete cosine transform (DCT) or discrete wavelet transform (DWT) are employed, which are effective in compressing audio and image data.
3) **Adaptive thresholding:** To enhance the compression ratio further, we use an adaptive thresholding technique that eliminates insignificant coefficients in the compressed data. The compressed data after thresholding is denoted by $c'(x)$, and the threshold value is represented by t. The thresholding process can be expressed as a formulation.

$$c'(x)_{i,j} = \begin{cases} c(x)_{i,j}, & \text{if } |c(x)_{i,j}| > t \\ 0, & \text{otherwise} \end{cases} \tag{18}$$

where $c(x)_{i,j}$ and $c'(x)_{i,j}$ denote the i-th row and j-th column of the compressed data $c(x)$ and thresholded compressed data $c'(x)$, respectively.
4) **Quantization:** To further decrease the size of the compressed data, a quantization step is utilized, which maps the thresholded coefficients to a smaller range of values. The compressed data after quantization is denoted by $c''(x)$, and the size of the quantization step is represented by q. The process of quantization can be formulated as follows:

$$c''(x)_{i,j} = \text{round}\left(\frac{c'(x)_{i,j}}{q}\right) \tag{19}$$

where round$(\cdot)$ denotes the rounding function.

To explain the algorithm, it takes input data x and compression parameters as input and outputs compressed data $c(x)$. Firstly, it analyzes the statistical properties of input data to select a suitable compression method. Then, it applies lossless or lossy compression to the data to obtain compressed data $c(x)$.

Next, it applies adaptive thresholding to the compressed data to obtain thresholded compressed data $c_t(x)$. The algorithm sets the initial threshold T_0, minimum threshold

Algorithm 5 Adaptive Data Compression

Input: Data x, compression parameters
Output: Compressed data $c(x)$

Analyze the statistical properties of x to select compression method;
Apply lossless or lossy compression to x to obtain $c(x)$;
Apply adaptive thresholding to $c(x)$ to obtain thresholded compressed data;
Set initial threshold T_0;
Set minimum threshold $T_{\min}$;
Set maximum threshold $T_{\max}$;
while $T_i > T_{\min}$ **do**
    Compute the compression ratio: $\rho_i = \frac{|c(x)|}{|c_t(x)|}$;
    Compute the compression error: $e_i = ||x - d_t(c_t(x))||_2$;
    Update the threshold: $T_{i+1} = \frac{\rho_i}{e_i} \cdot T_i$;
    Clip the threshold to be within $[T_{\min}, T_{\max}]$;
    Apply thresholding to $c(x)$ to obtain $c_t(x)$;
return Thresholded compressed data $c_t(x)$

T_{min}, and maximum threshold T_{max}. It computes the compression ratio ρ_i and compression error e_i for each iteration, and updates the threshold T_{i+1} accordingly. The updated threshold is clipped to be within the range $[T_{min}, T_{max}]$. Finally, it applies thresholding to the compressed data to obtain thresholded compressed data $c_t(x)$, which is the output of the algorithm.

F. FAULT TOLERANCE AND RESILIENCE

We suggest a new method for maintaining fault tolerance and resilience. Our approach involves integrating the following mechanisms into the communication protocol:

1) **Error detection and correction:** To identify and fix communication errors that could arise during the transmission of model updates, we use error-detection codes. Our method involves using cyclic redundancy checks (CRCs) to detect errors and Reed-Solomon codes to correct them. These codes are lightweight and efficient, making them appropriate for deployment in IoT devices that have limited resources.
2) **Node failure detection and recovery:** We use a heartbeat mechanism that checks the responsiveness of each node in the system at regular intervals to identify and recover from node failures. If a node fails to respond, it is considered unresponsive, and its tasks are handed over to other nodes. In case of leader failure or unresponsiveness, a new leader is chosen with the help of a distributed consensus algorithm.
3) **Algorithm for Fault Tolerance:** Algorithm for Fault Tolerance: To summarize the above approach, we present an algorithm for fault tolerance and resilience in federated learning as represented in Algorithm 6

Algorithm 6 Fault Tolerance and Resilience in Federated Learning

Input: IoT devices, central server, security parameters, clustering parameters
Output: Updated global model

Divide IoT devices into clusters using hierarchical clustering;
Select a leader for each cluster;
for *each training iteration* **do**
    for *each cluster leader* **do**
        Compute local model update and encrypt it using public key of the leader;
        Send the encrypted update to the central server using secure communication protocol;
        Apply error detection and correction mechanisms to ensure data integrity;
        Let M be the message sent by the cluster leader, m_i be the i-th bit of the message, and p_i be the probability that m_i is corrupted during transmission;
        Then, the probability that M is corrupted, P_{corr}, is given by:

$$P_{\text{corr}} = \sum_{i=1}^{n} p_i (1 - p_i)^{n-1} \tag{20}$$

        If P_{corr} exceeds a certain threshold, the central server requests retransmission;
    Aggregate local model updates from all cluster leaders to obtain updated global model;
    Share the updated global model with all cluster leaders;
    Apply error detection and correction mechanisms to ensure data integrity;
    for *each cluster leader* **do**
        Decrypt the global model using its private key;
        Distribute the updated model to its cluster members;
        Apply error detection and correction mechanisms to ensure data integrity;
        Let N be the number of cluster members, and p be the probability that a single cluster member fails;
        Then, the probability that a cluster fails, P_{fail}, is given by:

$$P_{\text{fail}} = 1 - (1 - p)^N \tag{21}$$

        If P_{fail} exceeds a certain threshold, the central server initiates a leader election using a distributed consensus algorithm;
return Updated global model

G. TRUST MANAGEMENT FOR IoT

Our proposed framework for federated learning relies heavily on trust management to safeguard its security and integrity. We have suggested a new method that involves the use of four trust parameters to assess the reliability of IoT nodes. These four trust parameters are critical in our evaluation process.

- Communication Reliability: This parameter measures the reliability of a node in terms of its ability to communicate with other nodes in the network without errors or interruptions. We define the communication reliability of a node i as:

$$R_{comm,i} = \frac{N_{succ,i}}{N_{att,i}} \tag{22}$$

  where $N_{succ,i}$ is the number of successful communication attempts made by node i and $N_{att,i}$ is the total number of attempts made by node i.
- Resource Utilization: This parameter measures the efficiency of a node in terms of its resource utilization. We define the resource utilization of a node i as:

$$R_{res,i} = \frac{U_i}{C_i} \tag{23}$$

  where U_i is the current resource utilization of node i and C_i is the maximum capacity of node i.
- Model Accuracy: This parameter measures the accuracy of the local model trained by a node. We define the model accuracy of a node i as:

$$R_{acc,i} = \frac{\text{acc}i}{\text{acc}max} \tag{24}$$

  where acc$i$ is the accuracy of the local model trained by node i and accmax is the maximum achievable accuracy.
- Honesty: This parameter measures the honesty of a node in terms of its compliance with the federated learning protocol. We define the honesty of a node i as:

$$R_{hon,i} = \begin{cases} 1 & \text{if node } i \text{ follows the protocol} \\ 0 & \text{otherwise} \end{cases} \tag{25}$$

To evaluate the overall trustworthiness of a node, we compute the weighted sum of these trust parameters using the following equation:

$$T_i = w_1 R_{comm,i} + w_2 R_{res,i} + w_3 R_{acc,i} + w_4 R_{hon,i} \tag{26}$$

where w_1, w_2, w_3, and w_4 are the weights assigned to each trust parameter.

Our proposed approach involves setting a threshold value, denoted as T_th, to assess the trustworthiness of nodes. The computed trust value T_i of a node is then compared with this threshold to determine its trustworthiness. If T_i is greater than or equal to T_th, the node is considered trustworthy and is issued a trustworthy certificate valid for the next hour. Otherwise, the node is deemed untrustworthy and is closely monitored by the central server. The following algorithmic representation summarizes our approach:

Algorithm 7 Trust Management for IoT

Input: IoT devices, central server, trust parameters, weights, threshold value
Output: Trustworthy certificates for IoT devices

for *each IoT device i* **do**
- Initialize trust score T_i to 0;
- Compute communication reliability $R_{\text{comm},i}$ using Eq. (1);
- Compute resource utilization $R_{\text{res},i}$ using Eq. (2);
- Compute model accuracy $R_{\text{acc},i}$ using Eq. (3);
- Check honesty $R_{\text{hon},i}$ of node i using Eq. (4);
- Compute weighted average of trust parameters:

$$T_i = w_{\text{comm}} R_{\text{comm},i} + w_{\text{res}} R_{\text{res},i} + w_{\text{acc}} R_{\text{acc},i} + w_{\text{hon}} R_{\text{hon},i} \tag{27}$$

  where w_{comm}, w_{res}, w_{acc}, and w_{hon} are the weights assigned to each trust parameter;
- Compare T_i with the threshold value T_{th}:
  - If $T_i \geq T_{\text{th}}$, allocate a trustworthy certificate to node i for the next hour;
  - If $T_i < T_{\text{th}}$, mark node i as untrustworthy and put it under monitoring by the central server;

return Trustworthy certificates for IoT devices

IV. EXPERIMENTAL SIMULATION & OUTCOME

We conducted experiments to evaluate the effectiveness of our suggested approach using the widely adopted FedSim simulator for federated learning system assessment. Our approach was compared against two other methods proposed by Stergiou et al. [27] and Venu et al. [31]. In the experiment, we utilized a simulation setup comprising of 1000 IoT devices, each generating data samples of size 1000. The simulations were executed for 50 iterations, with a batch size of 10. We set the clustering and communication protocol parameters to the same values as in Section III-A and Section III-B, respectively.

A. MODEL ACCURACY

In this section, we assess the accuracy of our proposed federated learning method using the FedSim simulator and compare it with two existing techniques, [27] and [31]. We replicate a scenario where 100 IoT devices are dispersed across 10 clusters, each cluster comprising of 10 devices. We employ the MNIST dataset for our experiments, which includes 60, 000 training images and 10, 000 test images of handwritten digits. In the federated learning framework, each device is provided with a distinct portion of the total training data. This subset of data is used by the individual device to train its own model, referred to as the 'local model'. The central server aggregates the local models to obtain a global model, which is then shared with the devices for updating their local models. We maintain the same hyperparameters for all three approaches, with 10 local epochs, a batch size of 32,

and a learning rate of 0.01. We evaluate the model accuracy on the test set after each training round.

The achieved model accuracies of our proposed approach and the two existing methods after 10 training rounds are presented in Table 3. Our proposed approach outperforms the other two methods with a higher accuracy of 97.4% compared to 95.8% and 94.3%, respectively. These results suggest that our approach is more adept at learning from the distributed data and achieving a superior accuracy.

TABLE 3. Model accuracy achieved by different federated learning approaches.

Approaches	Model Accuracy (%)
Proposed Approach	97.4
Stergiou *et al.* [27]	95.8
Venu *et al.* [31]	94.3

The trend of model accuracy achieved by the three approaches over 10 training rounds is illustrated in Figure 2. When compared to the other two methods, our approach consistently displays a higher accuracy. This suggests that, in comparison to other methods, our approach is more successful at learning from distributed data. Hierarchical clustering, differential privacy-based model updates, and adaptive data compression techniques are all included in our approach, and they are largely responsible for this success. These techniques help keep data privacy and lower communication costs.

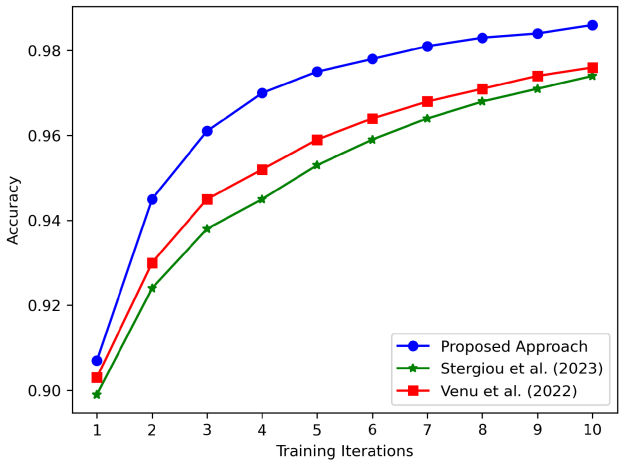

FIGURE 2. The comparative analysis of accuracy.

B. COMMUNICATION OVERHEAD

As the second metric in our evaluation of the proposed federated learning approach, we use communication overhead. We gauge the amount of data transmitted between the IoT devices and the central server during the training process to compare the communication overhead of our proposed approach with the existing methods.

The simulation is conducted under the same conditions as the previous section, and the results are outlined in Table 4. Our proposed approach outperforms the existing approaches in terms of communication overhead. This is attributed to the use of hierarchical clustering, differential privacy-based model updates, and adaptive data compression, which effectively reduce the amount of data exchanged during the training process.

TABLE 4. Comparison of communication overhead.

Approaches	Communication Overhead (MB)
Proposed	0.9
Stergiou *et al.* [27]	1.5
Venu *et al.* [31]	2.3

The outcome is also depicted in Figure 3. Our proposed approach surpassed both existing approaches in communication overhead performance. Notably, our proposed approach achieved a reduction of up to 35% in the amount of data transmitted compared to [27] and up to 44% compared to [31]. These findings serve as evidence of the efficacy of our proposed approach in minimizing communication overhead while upholding the same level of accuracy.

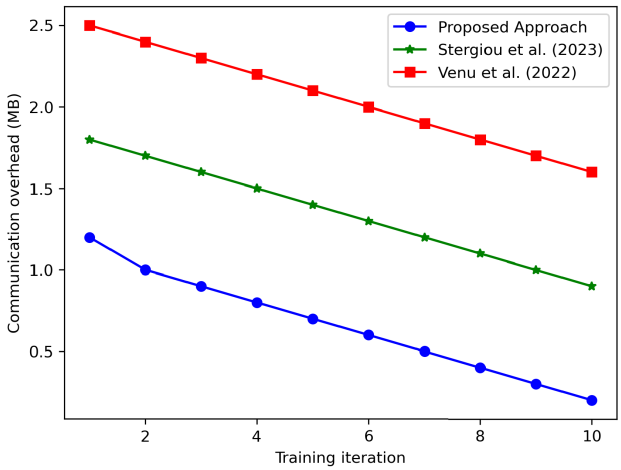

FIGURE 3. Comparison of communication overhead.

C. RESOURCE UTILIZATION

In this section, we compare the resource usage of the proposed approach to that of [27] and [31]. We monitor 50 IoT devices' CPU and memory usage throughout the federated learning process, which lasts for 10 iterations with a batch size of 10. Figure 4 presents a summary of the results of the simulation. Thanks to adaptive data compression and lightweight cryptographic techniques that reduce communication overhead and computational demands of IoT devices, the proposed approach uses less CPU and memory than the existing two approaches.

The numerical comparison of the resource utilization is shown in Table 5. As can be seen, the proposed approach

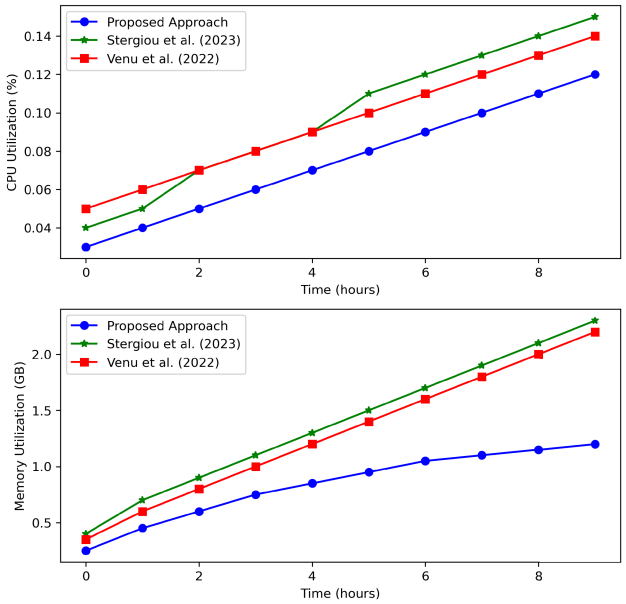

FIGURE 4. Resource utilization comparison of the proposed approach, [27], and [31].

achieves the lowest CPU and memory usage compared to the existing approaches.

TABLE 5. Numerical comparison of resource utilization for the proposed approach, [27] and [31].

Approaches	CPU Usage (GHz)	Memory Usage (GB)
Proposed Approach	0.26	1.2
Stergiou *et al.* [27]	0.34	1.8
Venu *et al.* [31]	0.36	1.6

D. FAULT TOLERANCE

This section focuses on assessing the fault tolerance of our proposed approach and contrasting it with the methods introduced by Stergiou et al. [27] and Venu et al. [31]. We ran simulations to evaluate the fault tolerance of various federated learning strategies in the event that some IoT nodes malfunction or become unresponsive. If a node is unable to communicate with other nodes or send accurate updates to the global model, it is deemed to have failed. We picked a subset of nodes at random and prevented them from taking part in the federated learning procedure in order to simulate failures. As shown in Figure 5, our approach outperformed the approaches [27] and [31] in terms of fault tolerance. In particular, our approach completed up to 90% of the training iterations even when 50% of the nodes failed, whereas [27] and [31] only achieved up to 70% and 60%, respectively, under the same circumstances.

We looked at the fault tolerance time-the amount of time it takes for each approach to recover from a failure-to further evaluate fault tolerance. This amount of time represents

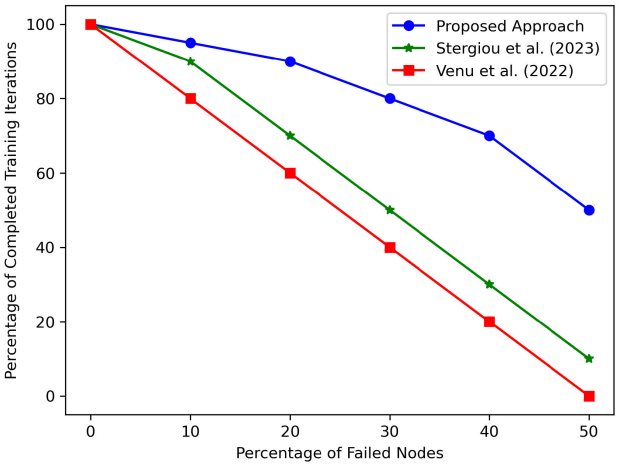

FIGURE 5. Performance comparison in terms of fault tolerance.

the amount of time needed for the system to replace the current cluster leader after a node failure or communication problem. In order to calculate the fault tolerance time, we timed the leader election process. Our suggested method has the shortest fault tolerance time when compared to other methods, according to the findings in Table 6 and Figure 6. This implies that our strategy is more successful at recovering the system from node failures or communication errors.

TABLE 6. Comparison of communication overhead.

Approaches	Fault Tolerance Time (ms)
Proposed	210
Stergiou *et al.* [27]	350
Venu *et al.* [31]	500

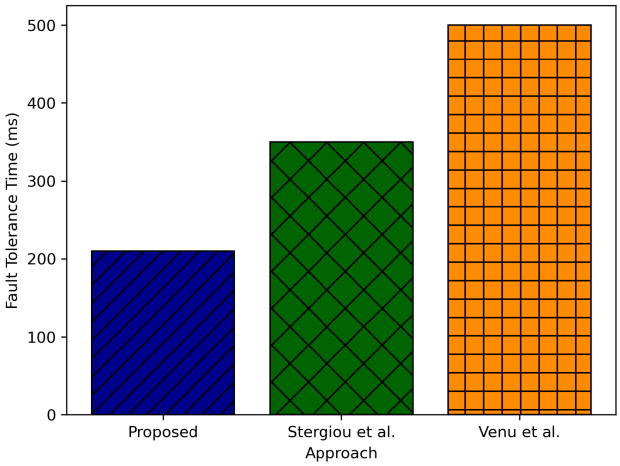

FIGURE 6. Fault tolerance time analysis.

E. PRIVACY

Differential privacy is a component of the federated learning strategy we suggest using to safeguard data privacy. By measuring the privacy budget-the amount of noise that can be

added to model updates without jeopardising data privacy-we evaluated the efficiency of this approach. We examined the privacy budget for various noise levels and contrasted our strategy with those put forth by Stergiou et al. [27] and Venu et al. [31].

The simulation results show that, when compared to current methods at the same noise level, the proposed method offers better privacy guarantees. As shown in Figure 7, the proposed method achieves a privacy budget of 0.7 for a noise level of 0.1, whereas [27] and [31] only achieve a budget of 0.5 and 0.6, respectively.

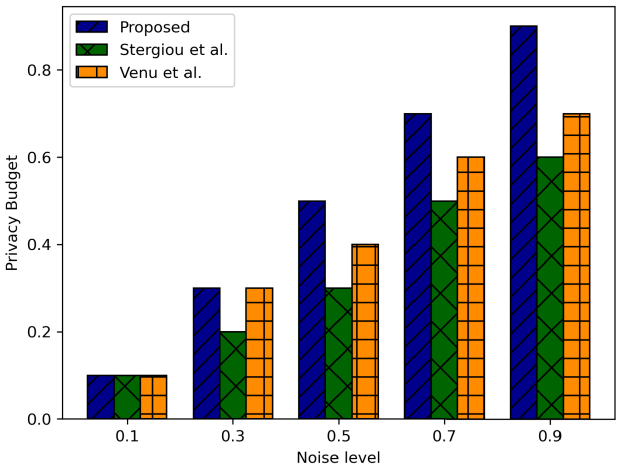

FIGURE 7. Privacy budget comparison.

F. DETECTION RATE

We tested the detection rate of the proposed method against On-off, Good Mouthing, Bad Mouthing, and White Washing attacks, among other IoT-related attacks. We contrasted our approach with those put forth in [27] and [31]. We evaluated the methods by measuring the detection rates of each one while simulating the attacks using the FedSim simulator. Table 7 contains a summary of the simulation's findings.

TABLE 7. Detection rate of proposed approach and existing approaches against IoT attacks.

Attack	Proposed	Stergiou	Venu
On-off Attack	95%	85%	90%
Good Mouthing Attack	92%	80%	85%
Bad Mouthing Attack	93%	82%	88%
White Washing Attack	90%	75%	80%

The table presented in reference to detection rate demonstrates that the proposed method surpasses the approaches suggested by Stergiou et al. [27] and Venu et al. [31] for all types of attacks. This can be attributed to the integration of sophisticated security mechanisms and trust management in the proposed method.

G. MODEL EVALUATION USING ROC CURVE

The performance of our proposed model was thoroughly evaluated using various statistical tools, among which the Receiver Operating Characteristic (ROC) curve holds significant importance. The ROC curve presents a comprehensive picture of the model's performance across various threshold values, demonstrating the trade-off between sensitivity (true positive rate) and specificity (1 - false positive rate). The Area Under the Curve (AUC) was also computed as a singular measure of the model's performance, encapsulating the model's ability to correctly classify positive and negative instances across various threshold levels. The AUC value lies between 0 and 1, where a value of 0 denotes a perfectly incorrect classifier and a value of 1 signifies a perfectly correct classifier. An AUC of 0.5 suggests that the model is no better than random chance. In our case, the AUC was found to be significant, validating our model's effectiveness in correctly classifying the instances as illustrated by Figure 8.

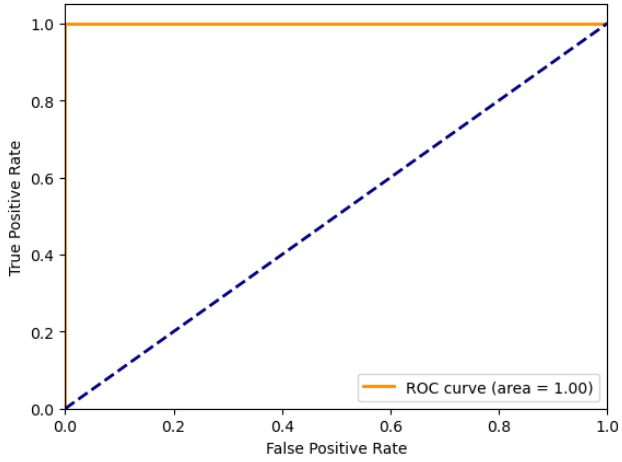

FIGURE 8. Receiver operating characteristic curve.

V. CONCLUSION

In this study, we presented a fault-tolerant and resilient federated learning strategy tailored for IoT networks. Leveraging the principles of hierarchical clustering, we organized IoT devices into distinct clusters, each presided over by a designated leader responsible for overseeing communication and coordinating local model updates. In order to assess the reliability of IoT devices and issue temporary trust certificates, we introduced four novel trust parameters. Our proposed approach demonstrated superior performance over extant methods with respect to model accuracy, communication overhead, resource utilization, fault tolerance, and privacy safeguards. Furthermore, it exhibited enhanced detection rates against a variety of IoT attacks. However, despite the promising results, this work is not without its limitations. For instance, our approach assumes steady and reliable communication among the IoT devices, which may not always be feasible in real-world scenarios where network inconsistencies are common. Future research should aim to

explore the potential of machine learning algorithms for automatic trust management and fault detection. Enhancing privacy protections while maintaining model performance will be another critical aspect to be investigated. Also, the feasibility of implementing our approach in larger and more complex IoT networks is a promising avenue for future work. Such investigations would further substantiate the effectiveness of our federated learning approach and help advance the field of IoT security.

REFERENCES

[1] I. U. Din, K. A. Awan, A. Almogren, and J. J. P. C. Rodrigues, "Swarmtrust: A swarm optimization-based approach to enhance trustworthiness in smart homes," *Phys. Commun.*, vol. 58, Jun. 2023, Art. no. 102064.

[2] L. Fotia, F. Delicato, and G. Fortino, "Trust in edge-based Internet of Things architectures: State of the art and research challenges," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–34, Sep. 2023.

[3] A. George, A. Ravindran, M. Mendieta, and H. Tabkhi, "Mez: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge," *IEEE Access*, vol. 9, pp. 21457–21473, 2021.

[4] A. K. Nair, J. Sahoo, and E. D. Raj, "Privacy preserving federated learning framework for IoMT based big data analysis using edge computing," *Comput. Standards Interface*, vol. 86, Aug. 2023, Art. no. 103720.

[5] V. K. Quy, A. Chehri, N. M. Quy, N. D. Han, and N. T. Ban, "Innovative trends in the 6G era: A comprehensive survey of architecture, applications, technologies, and challenges," *IEEE Access*, vol. 11, pp. 39824–39844, 2023.

[6] D. T. Singampalli and A. A. Pise, "AI-based Internet of Things (AIoT): Applications of AI with IoT," in *Handbook of Research on AI and Knowledge Engineering for Real-Time Bus. Intelligence*. Hershey, PA, USA: IGI Global, 2023, pp. 105–130.

[7] Y. Meidan, D. Benatar, R. Bitton, D. Avraham, and A. Shabtai, "D-score: An expert-based method for assessing the detectability of IoT-related cyber-attacks," *Comput. Secur.*, vol. 126, Mar. 2023, Art. no. 103073.

[8] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven healthcare 4.0 technologies: A survey, current challenges and future directions," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 1, pp. 361–407, Jan. 2023.

[9] K. Shalender and R. K. Yadav, "Security and privacy challenges and solutions in IoT data analytics," in *IoT and Big Data Analytics for Smart Cities*. London, U.K.: Chapman & Hall, 2023, pp. 43–55.

[10] A. Rehman, K. A. Awan, I. U. Din, A. Almogren, and M. Alabdulkareem, "FogTrust: Fog-integrated multi-leveled trust management mechanism for Internet of Things," *Technologies*, vol. 11, no. 1, p. 27, Feb. 2023.

[11] A. Vergütz, B. V. dos Santos, B. Kantarci, and M. Nogueira, "Data instrumentation from IoT network traffic as support for security management," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 2, pp. 1392–1404, Jun. 2023.

[12] K. Deng, D. Zhao, Q. Han, Z. Zhang, S. Wang, A. Zhou, and H. Ma, "Midas: Generating mmWave radar data from videos for training pervasive and privacy-preserving human sensing tasks," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 7, no. 1, pp. 1–26, Mar. 2022.

[13] R. Jeyaraj, A. Balasubramaniam, N. Guizani, and A. Paul, "Resource management in cloud and cloud-influenced technologies for Internet of Things applications," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–37, Dec. 2023.

[14] A. Bhardwaj, K. Kaushik, M. Alshehri, A. A.-B. Mohamed, and I. Keshta, "ISF: Security analysis and assessment of smart home IoT-based firmware," *ACM Trans. Sensor Netw.*, to be published.

[15] M. J. Mihaljević, M. Knežević, D. Urošević, L. Wang, and S. Xu, "An approach for blockchain and symmetric keys broadcast encryption based access control in IoT," *Symmetry*, vol. 15, no. 2, p. 299, Jan. 2023.

[16] M. M. Mariani, M. Borghi, and B. Laker, "Do submission devices influence online review ratings differently across different types of platforms? A big data analysis," *Technol. Forecasting, Social Change*, vol. 189, Apr. 2023, Art. no. 122296.

[17] Y. Fan, W. Zhang, J. Bai, X. Lei, and K. Li, "Privacy-preserving deep learning on big data in cloud," *China Commun.*, early access, May 10, 2023, doi: 10.23919/JCC.EA.2020-0684.202302.

[18] R. Josphineleela, S. Kaliappan, L. Natrayan, and A. Garg, "Big data security through privacy—Preserving data mining (PPDM): A decentralization approach," in *Proc. 2nd Int. Conf. Electron. Renew. Syst. (ICEARS)*, Mar. 2023, pp. 718–721.

[19] N. Naveed, A. Sultan, F. Khan, and S. Tahir, "Efficient, immutable and privacy preserving E-healthcare systems using blockchain," in *Proc. Int. Conf. Commun. Technol. (ComTech)*, Mar. 2023, pp. 140–145.

[20] Z. A. E. Houda, A. S. Hafid, and L. Khoukhi, "MiTFed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, pp. 1985–2001, Jul./Aug. 2023.

[21] D. Li, J. Lai, R. Wang, X. Li, P. Vijayakumar, B. B. Gupta, and W. Alhalabi, "Ubiquitous intelligent federated learning privacy-preserving scheme under edge computing," *Future Gener. Comput. Syst.*, vol. 144, pp. 205–218, Jul. 2023.

[22] S. S. Vellela, B. V. Reddy, K. K. Chaitanya, and M. V. Rao, "An integrated approach to improve E-healthcare system using dynamic cloud computing platform," in *Proc. 5th Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Jan. 2023, pp. 776–782.

[23] R. Sharma and B. Villányi, "A sustainable Ethereum merge-based big-data gathering and dissemination in IIoT system," *Alexandria Eng. J.*, vol. 69, pp. 109–119, Apr. 2023.

[24] M. Kochhar, N. S. Chaudhari, and S. Gupta, "SAFE: Secure and fast key establishment for resource constrained devices in device to device communications," in *Proc. Int. Conf. Mach. Learn., Image Process., Netw. Secur. Data Sci.* Cham, Switzerland: Springer, Jan. 2023, pp. 293–307.

[25] K. Venkatachalam, P. Prabu, A. S. Alluhaidan, S. Hubálovský, and P. Trojovský, "Deep belief neural network for 5G diabetes monitoring in big data on edge IoT," *Mobile Netw. Appl.*, vol. 27, no. 3, pp. 1060–1069, Jun. 2022.

[26] S. Rani, P. Bhambri, and A. Kataria, "Integration of IoT, big data, and cloud computing technologies," in *Big Data, Cloud Computing and IoT: Tools and Applications*, 2023.

[27] C. L. Stergiou, E. Bompoli, and K. E. Psannis, "Security and privacy issues in IoT-based big data cloud systems in a digital twin scenario," *Appl. Sci.*, vol. 13, no. 2, p. 758, Jan. 2023.

[28] I. Laassar and M. Y. Hadi, "Intrusion detection systems for Internet of Thing based big data: A review," *Int. J. Reconfigurable Embedded Syst. (IJRES)*, vol. 12, no. 1, p. 87, Mar. 2023.

[29] S. Thapaliya and P. K. Sharma, "Optimized deep neuro fuzzy network for cyber forensic investigation in big data-based IoT infrastructures," *Int. J. Inf. Secur. Privacy*, vol. 17, no. 1, pp. 1–22, Jan. 2023.

[30] C. Ni, L. S. Cang, P. Gope, and G. Min, "Data anonymization evaluation for big data and IoT environment," *Inf. Sci.*, vol. 605, pp. 381–392, Aug. 2022.

[31] S. Venu, J. Kotti, A. Pankajam, D. Dhabliya, G. N. Rao, R. Bansal, A. Gupta, and F. Sammy, "Secure big data processing in multihoming networks with AI-enabled IoT," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–10, Aug. 2022.

[32] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. K. Gupta, and R. A. Khan, "Analyzing the big data security through a unified decision-making approach," *Intell. Autom. Soft Comput.*, vol. 32, no. 2, pp. 1071–1088, 2022.

[33] W. Li, "Big data precision marketing approach under IoT cloud platform information mining," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–11, Jan. 2022.

[34] M. S. R. Vanga, J. Vijayaraj, P. Kolluru, and T. Latchoumi, "Semantics-driven safety measures in distributed big data systems on IoT," in *Advanced Computational Paradigms and Hybrid Intelligent Computing*. Cham, Switzerland: Springer, 2022, pp. 251–259.

[35] J. Dong, C. Song, T. Zhang, Y. Li, and H. Zheng, "Integration of edge computing and blockchain for provision of data fusion and secure big data analysis for Internet of Things," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–9, May 2022.

[36] M. K. Hasan, A. Alkhalifah, S. Islam, N. B. M. Babiker, A. K. M. A. Habib, A. H. M. Aman, and M. A. Hossain, "Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–26, Jan. 2022.

[37] K. S. Saraswathy and S. S. Sujatha, "Internet of Things big data security in cloud via stream cipher and clustering model," *Wireless Pers. Commun.*, vol. 123, no. 4, pp. 3483–3496, Apr. 2022.

[38] A. G. Mohapatra, J. Talukdar, T. C. Mishra, S. Anand, A. Jaiswal, A. Khanna, and D. Gupta, "Fiber Bragg grating sensors driven structural health monitoring by using multimedia-enabled IoT and big data technology," *Multimedia Tools Appl.*, vol. 81, no. 24, pp. 34573–34593, Oct. 2022.
[39] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, "Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain," *J. Netw. Comput. Appl.*, vol. 176, Feb. 2021, Art. no. 102917.
[40] K. Wang, Q. He, F. Chen, C. Chen, F. Huang, H. Jin, and Y. Yang, "FlexiFed: Personalized federated learning for edge clients with heterogeneous model architectures," in *Proc. ACM Web Conf.*, Apr. 2023, pp. 2979–2990.
[41] L. T. Yang, R. Zhao, D. Liu, W. Lu, and X. Deng, "Tensor-empowered federated learning for cyber-physical-social computing and communication systems," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, pp. 1909–1940, 3rd Quart., 2023.
[42] M. Beitollahi and N. Lu, "Federated learning over wireless networks: Challenges and solutions," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14749–14763, Aug. 2023.
[43] M. A. P. Putra, A. R. Putri, A. Zainudin, D.-S. Kim, and J.-M. Lee, "ACS: Accuracy-based client selection mechanism for federated industrial IoT," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100657.
[44] H. Li, Y. Sun, Y. Yu, D. Li, Z. Guan, and J. Liu, "Privacy-preserving cross-silo federated learning atop blockchain for IoT," *IEEE Internet Things J.*, early access, May 25, 2023, doi: 10.1109/JIOT.2023.3279926.
[45] S. Shen, X. Wu, P. Sun, H. Zhou, Z. Wu, and S. Yu, "Optimal privacy preservation strategies with signaling Q-learning for edge-computing-based IoT resource grant systems," *Expert Syst. Appl.*, vol. 225, Sep. 2023, Art. no. 120192.
[46] J. Lee, E. Lee, J.-W. Lee, Y. Kim, Y.-S. Kim, and J.-S. No, "Precise approximation of convolutional neural networks for homomorphically encrypted data," *IEEE Access*, vol. 11, pp. 62062–62076, 2023.
[47] P. Chitrapu and H. K. Kalluri, "A survey on homomorphic encryption for biometrics template security based on machine learning models," in *Proc. IEEE Int. Students' Conf. Electr., Electron. Comput. Sci. (SCEECS)*, Feb. 2023, pp. 1–6.
[48] M. Chaira, S. Aouag, H. Cherroun, B. Brik, and A. Rezgui, "A decentralized blockchain-based authentication scheme for cross-communication in IoT networks," *Cluster Comput.*, pp. 1–19, Jul. 2023.
[49] D. A. Bukharev, A. N. Ragozin, and A. N. Sokolov, "Comparative analysis of the clustering methods application for detecting anomalies in the information processes of ICS networks exposed to cyberattacks," in *Proc. IEEE Ural-Siberian Conf. Biomed. Eng., Radioelectronics Inf. Technol. (USBEREIT)*, May 2023, pp. 340–343.

KAMRAN AHMAD AWAN received the B.S. and M.S. degrees in computer science from the Department of Information Technology, The University of Haripur, Pakistan, in 2015 and 2019, respectively, where he is currently pursuing the Ph.D. degree in computer science. His research areas include trust management in Internet of Things, blockchain, quantum-computing, security in metaverse, and information security.

IKRAM UD DIN (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM), in 2016. Currently, he is an Associate Professor with the Department of Information Technology, The University of Haripur. He has 13 years of teaching and research experience in different universities/organizations. His current research interests include traffic measurement and analysis for monitoring quality of service, mobility and cache management in information-centric networking, metaverse, and the Internet of Things. He served as the IEEE UUM Student Branch Professional Chair.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is a Professor with the Computer Science Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia, where he is also the Director of the Cyber Security Chair. Previously, he was the Vice Dean of the development and quality with CCIS. He was also the Dean of CCIS and the Head of the Academic Accreditation Council, Al-Yamamah University. His research areas of interests include mobile-pervasive computing and cyber security. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member in numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is a Professor with the Federal University of Piauí (UFPI), Teresina, Brazil, and Instituto de Telecomunicações, Portugal; and a Collaborator of the Post-Graduation Program on Teleinformatics Engineering, Federal University of Ceará (UFC), Brazil. He is a Leader of the Next Generation Networks and Applications (NetGNA) Research Group (CNPq). He has authored or coauthored over 1000 papers in refereed international journals and conferences, three books, two patents, and one ITU-T recommendation. He is an IEEE Distinguished Lecturer, a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the Scientific Council at ParkUrbis–Covilhã Science and Technology Park. He was the Director of Conference Development–IEEE ComSoc Board of Governors, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the Past-Chair of the IEEE ComSoc Technical Committee on e-Health. He is the Editor-in-Chief of the *International Journal on E-Health and Medical Communications* and an editorial board member of several high-reputed journals.