FL-DABE-BC: A Privacy-Enhanced, Decentralized Authentication, and Secure Communication for Federated Learning Framework with Decentralized Attribute-Based Encryption and Blockchain for IoT Scenarios

Sathwik Narkedimilli*, Amballa Venkata Sriram*, Satvik Raghav†
*Department of Computer Science, Indian Institute of Information Technology (IIIT) Dharwad, Dharwad
Email: 21bcs103@iiitdwd.ac.in, 21bcs008@iiitdwd.ac.in
†Department of Electronics and Communication Engineering, Amrita School of Engineering, Bengaluru
Email: satvikraghav007@gmail.com

***Abstract*—In IoT scenarios, where data privacy and security are among the major concerns, FL is a decentralized training approach that can be used to train machine learning models without transferring sensitive data from IoT devices. The framework proposed in our research advances the concept of FL for IoT scenarios, adding the most advanced security schemes such as Decentralized Attribute-Based Encryption (DABE) for decentralized authentication, Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), and Blockchain technology to secure the entire process of modeling training against data privacy and security issues. In this framework, data from all IoT devices are locally encrypted using DABE for decentralized authentication and data encryption, then based on HE, data can be securely computed on encrypted data. Afterward, SMPC technology is employed to preserve privacy and collaborative computations. The output from SMPC is securely transmitted via Blockchain, which guarantees transparent communication and data integrity and securely stores all relevant transactions and model updates in a distributed ledger across the entire FL network.**

The framework begins with IoT devices collecting and preparing data for local model training, where the data is encrypted using DABE. Initial deep learning models configured in cloud servers are distributed to edge devices via a blockchain network, ensuring immutable record-keeping and secure peer authentication. After local training, the updated model weights are encrypted and securely transmitted to fog layers via the blockchain, where micro-services perform aggregation using homomorphic encryption and SMPC. The FL server aggregates these local updates with differential privacy to prevent data leakage and iteratively refines the global model. The final global model is then distributed back to the IoT devices for deployment, enabling real-time analytics in IoT market spaces. This framework effectively addresses the challenges of secure decentralized learning in IoT environments, offering a robust solution for privacy-preserving, efficient, and secure federated learning.

***Index Terms*—Federated Learning, Decentralized Attribute-Based Encryption, Blockchain**

I. Introduction

The Internet of Things (IoT) [1] is a brilliant way to connect different physical objects with digital information. Its rapid adoption is already revolutionizing many different aspects of different industries. IoT has already resulted in amazingly future-oriented applications, including consumer-grade home automation and medical science. But if we want to see further growth in these areas and move to new areas such as industrial automation, we also need to address the key challenges of addressing data privacy and security concerns. Centralized machine learning models, often involving the transfer of sensitive information from IoT devices to centralized servers, have proven to be inadequate for these purposes. They also potentially expose data to a variety of malicious attacks. This has made it an increasingly urgent priority to move to decentralized, secure learning frameworks.

FL has the potential to overcome these issues as it enables the training of machine learning models on devices without transferring the underlying data into a central server. This is facilitated by the FL approach of allowing trained models to be updated individually on IoT devices and shared with a central server as part of the iterative aggregation process. However, a lack of security in FL frameworks could still result in privacy leaks and data exposure in IoT environments, which process sensitive data. This makes it crucial to develop robust security strategies that can be seamlessly incorporated into FL frameworks to achieve a high level of data privacy and integrity, such as using distributed data.

Our proposed framework named FL-DABE-BC, which is a novel privacy-pres framework for IoT environments, combines key components of Decentralized Attribute-Based Encryption (DABE), Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), and Blockchain. FL-DABE-BC first uses DABE for decentralized authentication and fine-grained data encryption on IoT devices. The data encryption with DABE is done on the local IoT device, thus reducing the chances of a breach of sensitive information and enhancing the security of the overall federated learning process. Additionally, the integration of Microservices [2] allows for scalable and modular deployment, enabling the framework to efficiently

manage and process IoT data while maintaining high levels of security and privacy.

Enhancing data privacy and secure computation capabilities, FL-DABE-BC leverages Homomorphic Encryption and Secure Multi-Party Computation. Homomorphic Encryption enables complex computations to be performed directly on encrypted data. By leveraging this technique, data doesn't need to be exposed and available for easier processing. It assures data privacy during aggregation, processing, and model training as well. At the same time, SMPC enables the parties to cooperate to perform computations on their private inputs while keeping them confidential to other parties involved in the process. This method adds serious robustness to data privacy and security since it mitigates vulnerabilities in distributed learning.

To ensure transparency and immutability in communication between devices/servers in the FL-DABE-BC framework, blockchain technology is employed as the communication channel for the transfer of model updates and the integrity of the data. All the transaction and model update information deployed on the blockchain is stored in the distributed ledger in a secure manner, which is impossible to be modified by a single device/server. Thus, the collaboration among the participating devices/servers in federated learning can be enhanced with this transparent and secure distributed ledger system. With the integration of blockchain, the FL-DABE-BC framework proposed here can provide an end-to-end solution to IoT-based federated learning, which addresses the issues of privacy, security, integrity, and effective communication between the nodes (EDGE-FOG-CLOUD layers). The integration of peer-to-peer (P2P) networks like blockchain has proven to improve the efficiency of communication by optimizing bandwidth [3] and ensuring secure data exchange. As a result, the FL-DABE-BC framework offers an end-to-end solution for IoT-based federated learning that addresses privacy, security, integrity, and effective communication across the EDGE-FOG-CLOUD layers.

II. Preliminaries

A. Federated Learning

Federated Learning (FL) [4] is the machine-learning paradigm that provides a decentralized approach to train models on end-user devices such as smartphones or Internet-of-Things (IoT) devices without having to move the raw data to a central server. In this way, the data stays on the user devices, and only model updates like gradients or weights are shared with the central server for combining (aggregation). FL is an important step towards minimizing risks of data privacy and security concerns by removing the need for centralized data storage and processing, which is becoming commonplace as our society increasingly moves services into the cloud. It also takes full advantage of the computational power of edge devices. As such, FL is very useful for scenarios where the data is sensitive, especially when the network bandwidth is limited.

B. Decentralized Attribute-Based Encryption

DABE (Decentralized Attribute-Based Encryption) [5] is a cryptographic technique that enhances security and privacy by allowing data to be encrypted based on specific user attributes rather than a single key or identity. In a decentralized setting, such as in IoT environments, DABE enables fine-grained access control and secure data sharing among multiple users and devices. Unlike traditional encryption methods, where a central authority manages encryption keys, DABE distributes the control among multiple authorities, reducing the risk of a single point of failure. This decentralized approach aligns well with federated learning, as it allows data to be securely encrypted on each device based on user attributes, ensuring that only authorized entities can decrypt and access the data.

C. Blockchain

Blockchain [6] is a distributed, immutable ledger system able to record transactions in a secure, transparent, and tamper-proof way. In federated learning, it can be used to verify and log updates to models, with all transactions openly broadcasted, recorded according to a timestamp, and accessible to all participants. It can be used for secure peer-to-peer communication between IoT devices and fog nodes, as well as for decentralized authentication and executing privacy-preserving operations without exposing the original data or models to unauthorized entities who might try to modify the data or model transactions. In this way, it can provide a trustworthy environment to execute collaborative learning without centralized supervision and oversight.

D. Cryptographic Primitives

1) *Homomorphic Encryption (HE)*: It [7] enables computations to be carried out directly on encrypted data in such a way that the results are still encrypted; as a result, no sensitive information needs to be revealed during the processing stages.
2) *Secure Multi-Party Computation (SMPC)*: It [8] allows multiple parties to jointly compute a function on their inputs while keeping their inputs private. The second application is federated learning. In federated learning, multiple devices or users collaborate in training a model while keeping their data private.
3) *Differential Privacy (DP)*: It [9] is a technique that, by introducing controlled noise in the data or the model outputs, prevents the identification of individual data points even if the aggregate data is revealed.

These cryptographic primitives provide strong privacy and security guarantees; they are the essential building blocks for designing federated learning frameworks that work in IoT environments.

III. Literature Review

The paper 'Recent Advances on Federated Learning: A Systematic Survey' [10] reviews seminal FL frameworks. FedAvg is the initial algorithm that averages the client model updates offline and allows decentralized learning. At the same

time, FedMA aligns and averages parameters from clients with heterogeneous data to tackle heterogeneous data challenges. FedProx extends FedAvg, adding a proximal term to address the heterogeneity of client data and achieve stable model convergence. The algorithms in this paper are among the initial developments for FL, from simple aggregation to more complicated methods in dealing with client diversity. The other paper introduces FedSGD [11], which adopts synchronous updates to ensure model consistency but suffers from communication overhead and stragglers.

The application of federated learning (FL) to Intrusion Detection Systems (IDS) [12] presents a promising approach for enhancing data privacy and scalability in real-time detection scenarios. Research highlights the integration of distributed IDS to manage large-scale network data while preserving user privacy. However, challenges such as communication overhead, data source heterogeneity, and incorporating advanced threat intelligence within FL models remain significant. These issues underscore the need for optimized frameworks that balance privacy, efficiency, and effective threat detection in diverse and complex environments.

In intelligent transportation systems (ITS), federated learning frameworks have been adapted to address the dynamic nature of vehicular networks. The V2X-Boosted FL model, incorporating contextual client selection [13], prioritizes relevant and high-quality data for training, optimizing resource use and model accuracy. Similarly, the semi-asynchronous hierarchical FL framework [14] accommodates varying data processing capabilities among vehicles, reducing communication latency and enhancing real-time applicability. Both approaches highlight the ongoing challenges of data heterogeneity, dynamic client availability, and secure communication within ITS.

To enhance privacy in federated learning, combining group signatures and FL [15] offers a robust solution, as demonstrated in recent studies. This method allows for the verification of data authenticity without revealing participant identities, thus preserving privacy and trust in decentralized networks. Additionally, the integration of blockchain and smart contracts with FL [16] introduces a tamper-proof ledger for model updates, addressing security and transparency issues. Despite these advancements, challenges such as computational overhead, scalability, and smart contract deployment complexities continue to demand innovative solutions.

Incorporating local differential privacy (LDP) within federated learning framework [17] is a growing area of interest, particularly in sensitive applications such as Power IoT systems and Vehicular Ad Hoc Networks (VANETs). The IFed framework [18] and FL with LDP for VANETs both aim to maintain data privacy while allowing real-time data processing. These models effectively mitigate privacy risks and protect against inference attacks. However, they face challenges like resource constraints, data sparsity, and maintaining model accuracy without compromising privacy, highlighting areas for further research and development.

Recent advancements in federated learning (FL) and secure communication have improved IoT data analytics and community systems. FL frameworks like FedMicro-IDA [2] and V2X-boosted FL optimizes privacy, efficiency, and model accuracy, despite challenges like dynamic client availability. Blockchain and smart contracts enhance security with tamper-proof ledgers, while local differential privacy (LDP) ensures secure data sharing [19]. Scalability and resource constraints, however, remain significant challenges in these systems.

IV. Proposed Model

A. The FL-DABE-BC Workflow

The FL-DABE-BC framework uses Decentralized Attribute-Based Encryption (DABE) for secure data encryption and blockchain for immutable records in IoT environments. Data is encrypted locally, aggregated using homomorphic encryption and SMPC, and refined with differential privacy. The final global model is securely deployed for real-time analytics. Fig 1 demonstrates the workflow of the model and the steps include :

1) *Data Collection and Preparation by IoT Devices*:
The process starts with IoT devices in the market spaces such as retail stores and smart cities collecting raw data from their surroundings in the form of customer interactions, environmental conditions, and sensor-derived metrics. Then, the raw data is preprocessed at the edge of each IoT device to make it ready for model training. This is done by normalizing the data to achieve a consistent aspect and extracting features to highlight the important patterns. Further, labeling these data points is done to categorize them.
Anonymized, preprocessed data is then encrypted using a technology known as Decentralized Attribute-Based Encryption (DABE) before it can be accessed. DABE only permits the decryption of data based on defined attributes, enabling only the fog nodes or cloud servers with the correct credentials to see, use, or analyze the data. This prevents any unauthorized entities from gaining access to it, which is important for ensuring sensitive data's privacy at the edge, where IoT devices operate.

2) *Initial Model Configuration and Distribution*:
After the data has been properly prepared, the cloud servers only initiate the work of training initial DL models, which would be customized based on the nature of the available data and the corresponding machine-learning tasks. To ensure the model's integrity during transmission, homomorphic encryption would be performed on the initial models. Homomorphic encryption allows computations to be performed on the encrypted data, meaning that the models can be securely transmitted over the network.
Encrypted model copies are provided to edge clients (the IoT) via a blockchain network. A blockchain maintains unchangeable and transparent records of all model transactions. The immutability of blockchain

transactions enhances security since it makes tampering or unauthorized changes impossible. Every IoT device needs to verify the identity of their peers using DABE, before initiating the download of the model. Only authenticated peers can engage in the training process.

3) *Local Training on IoT Devices*:
Once the models are in place, local training with encrypted IoT data can begin: every device can train on its encrypted data in a distributed manner. Each device can do its part to update the model based on its data. This procedure is repeated multiple times so that the model improves and 'fine-tunes' depending on the specific characteristics of the local data.
After each iteration, the locally updated model weights are encrypted using DABE. This step ensures that the locally updated model weights cannot be compromised through eavesdropping, or be accessed by unauthorized nodes before they are stored or transmitted to other nodes. More importantly, only authorized nodes (such as fog nodes or cloud servers) can decrypt and utilize the updated weights.

4) *Communication and Secure Aggregation*:
It's the encrypted local model weights that get uploaded to the fog layer via the blockchain network. The aggregation of these weights is performed by microservices deployed within the fog layer. Since the weights need to be aggregated by the fog nodes, this needs to happen under conditions that maintain data confidentiality. Homomorphic encryption is employed to achieve this: it allows the fog nodes to combine the weight values without the need to decode the individual data elements first.
Security and privacy are further enhanced by using Sec Computation (SMPC) between the nodes in the fog layer. SMPC allows multiple parties to jointly compute aggregate weights without revealing the inputs that each party used in the computation. Each participating node contributes to the computation but its local data remains private. Blockchain is used to securely log and track the SMPC computations in a transparent and tamper-proof manner.

5) *Aggregating Local Model Weights*:
The FL server in the cloud collects the aggregated model weights from the fog layer and, using homomorphic encryption, it can then aggregate these weights without ever having to decrypt them. This way the FL server will not know what each node is contributing, and the model weights in the aggregated model will never be exposed to the cloud as they travel as encrypted data. The data stays confidential, and the integrity of the model-training process is maintained.
Once the weights are combined, the model is subjected to differential privacy techniques. Differential privacy 'whitens' the combined model, preventing leakage of individual data points, memorization of data, and protection of overall model privacy. This phenomenon is key to both protecting the privacy of users and enabling the model to learn from the diversity of available datasets.

6) *Iterative Process of Model Training*:
The federated learning process is composed of multiple iterative communication rounds. In each round, the IoT devices carry out local training, encrypt and upload their latest weights to the cloud, and take part in the federated aggregation implemented by the fog layer and the blockchain. The FL server aggregates the model weights and updates the global model. The blockchain technology guarantees that every message communication between the nodes is safe and traceable, making it impossible for any adversary to access or tamper with these channels.
At the end of every aggregation, the new world model is encrypted and sent back to the FL clients (IoT devices and fog nodes) through the blockchain network. The FL clients authorize their server via DABE and update their local models with the new world model. This process is repeated until the world model achieves certain performance metrics (eg, accuracy or loss), as determined by predefined thresholds.

7) *Final Model Deployment and Local Data Analytics*:
Once the global model achieves effective performance, it is finalized, encrypted, and authenticated through DABE. The final global model is then deployed to all IoT devices and fog nodes, allowing them to use the model for real-time data analytics. IoT devices utilize the updated global model to make informed decisions and generate insights based on new data collected from their environments, such as customer behavior analysis or inventory management.

8) *Microservices in the Fog Layer*:
Microservices are deployed on fog nodes to manage various tasks, including data aggregation, real-time analytics, and secure communication within the blockchain network. These microservices provide a modular and scalable architecture, allowing the framework to efficiently process data and perform computations at the network's edge. This design ensures efficient local processing, reducing latency and improving overall performance in large-scale IoT deployments.

B. Assumptions for FL-DABE-BC

There are several assumptions underlying the FL-DABE-BC framework. Every entity (IoT device, fog node, microservices, or cloud server) in the framework assumes that all IoT devices, fog nodes, microservices, and cloud servers have a unique cryptographic key managed by the DABE system. The DABE

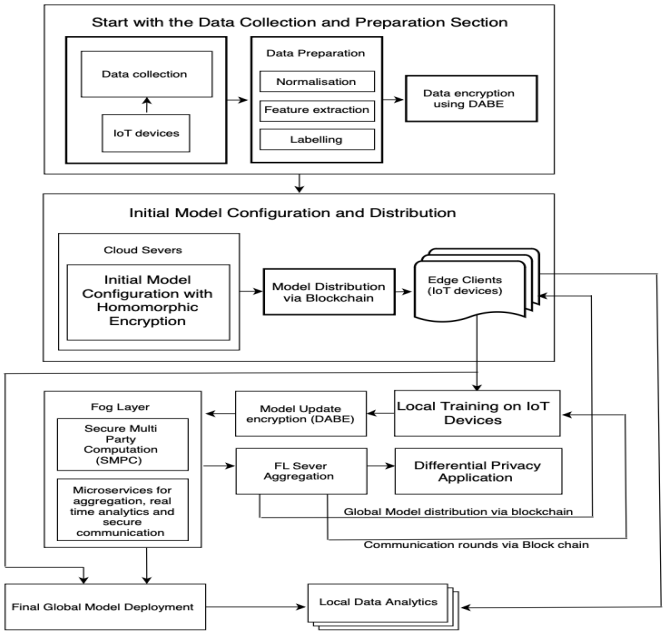

Fig. 1. Architecture of the proposed model

system will ensure that the key for each user has attributes that are granted to every entity whose attributes match. It is assumed that all entities trust the DABE system. They assume that the system is correctly implemented and secure so that nobody can tamper with it or access a key without the correct attributes. Third, the framework assumes the secure implementation of homomorphic encryption and SMPC that allows aggregating encrypted data without exposing sensitive information.

Furthermore, the underlying blockchain network is presumed to be secure and immutable, offering open and auditable logging of all transactions, data exchanges and updates of models. The blockchain is trusted to manage and record all SMPC processes, ensuring correctness and transparency for all federated learning activities. The integrity of the blockchain ensures that all IoT devices, fog nodes, microservices, and clouds in the showcase IoT market spaces can trust activities and exchanges. The differential privacy techniques are assumed to prevent data leakage, keeping the privacy of each data point in place even after aggregation. These assumptions collectively allow for the federated learning framework to securely work in IoT market spaces, maintaining data integrity and privacy.

The proposed federated learning framework is scalable, can work in dynamic environments, and can leverage the increasing number of IoT devices and fog nodes. Furthermore, DABE and blockchain transparently and securely manage data in a decentralized manner across multiple computing nodes. The microservices in the fog layer support scalable modular data processing and also allow tasks to be parallelized. Blockchain (with a layer-2 solution like offloading computation to other nodes using zkML [20]) enables seamless communication and integration, facilitating the federated learning framework to scale out over multiple nodes to meet large data storage and computational needs in large IoT deployments.

C. BAN Logic analysis for FL-DABE-BC

BAN Logic (Burrows-Abadi-Needham Logic) [21] is a formal method for reasoning about authentication protocols. It employs a set of rules and notational conventions to model the reasoning of the parties in a communication protocol. BAN logic helps to uncover flaws: weak or ambiguous beliefs can be quickly identified. Its task can be summarised as explicitly representing what each party believes about identities, message freshness, and trust in the data they're receiving. This way, protocols can be checked against the desired security properties.

The following is the BAN logic for the FL-DABE-BC framework, analyzing its authentication and security properties. By using BAN logic, the framework's assumptions and trust relationships are clearly defined, ensuring that its protocols are secure and correctly implemented.

Notations in BAN Logic:

- $P \rhd X$: **Principal** P **believes** statement X is true.
- $P \lhd X$: **Principal** P **has received** statement X.
- $P \overset{\text{says}}{} X$: **Principal** P **at some point sent** statement X.
- $P \rhd \#X$: **Principal** P **has jurisdiction over** statement X.
- $\{X\}_K$: **The message** X **is encrypted with key** K.
- $K \leftrightarrow P$: **K is a shared key between** P **and another principal, known only to them**.

Entities in the Framework:

- IoT devices (D)
- Fog nodes (F)
- Microservices in Fog Layer (M)
- Cloud servers (C)
- Blockchain network (B)

Assumptions and Initial Beliefs:

- **A1:** All entities believe in the validity of their cryptographic keys:

$$D \rhd (K_{D,F} \leftrightarrow F)$$
$$F \rhd (K_{F,M} \leftrightarrow M)$$
$$M \rhd (K_{M,C} \leftrightarrow C)$$
$$C \rhd (K_{C,B} \leftrightarrow B)$$

- **A2:** All entities believe that blockchain transactions are securely logged and can be trusted:

$$D \rhd (B \rhd \#\text{Transactions})$$
$$F \rhd (B \rhd \#\text{Transactions})$$
$$M \rhd (B \rhd \#\text{Transactions})$$
$$C \rhd (B \rhd \#\text{Transactions})$$

- **A3:** All entities believe in the correctness and security of Decentralized Attribute-Based Encryption (DABE),

Homomorphic Encryption (HE), and Secure Multi-Party Computation (SMPC):

$$D \triangleright \#\text{DABE is secure}$$
$$F \triangleright \#\text{DABE is secure}$$
$$M \triangleright \#\text{HE and SMPC are secure}$$
$$C \triangleright \#\text{HE is secure}$$
$$B \triangleright \#\text{HE and SMPC are secure}$$

- **A4:** Fog nodes (F) believe in the integrity and secure operation of microservices (M) for aggregating model updates:

$$F \triangleright M \triangleright \#\text{Aggregation and Computation}$$

Goals of Authentication and Security:

- **G1:** IoT devices (D) believe in the integrity of the model updates received from the cloud servers (C):

$$D \triangleright C \triangleright \text{Global Model}$$

- **G2:** Fog nodes (F) and microservices (M) believe in the integrity of data and model updates sent from IoT devices (D):

$$F \triangleright D \triangleright \text{Local Model Updates}$$
$$M \triangleright F \triangleright \text{Aggregated Model Updates}$$

- **G3:** Cloud servers (C) trust the secure aggregation of model updates performed using SMPC over blockchain (B):

$$C \triangleright \#(B \triangleright \text{SMPC Aggregation})$$

Protocol Messages Using BAN Logic:

- **M1:** IoT devices (D) send encrypted data to fog nodes (F) using DABE and log the transaction on blockchain (B):

$$D \rightarrow F : \{\text{Data}\}_{K_{D,F}}, \log(\text{Data Transfer})_B$$

Postulate: $F \triangleleft \{\text{Data}\}_{K_{D,F}}$

- **M2:** Fog nodes (F) forward encrypted local models to microservices (M) for aggregation, and log the process on blockchain (B):

$$F \rightarrow M : \{\text{Local Model}\}_{K_{F,M}}, \log(\text{Forwarding})_B$$

Postulate: $M \triangleleft \{\text{Local Model}\}_{K_{F,M}}$

- **M3:** Microservices (M) aggregate the local models using homomorphic encryption and SMPC, and send aggregated models to cloud servers (C), logging the operation on blockchain (B):

$$M \rightarrow C : \{\text{Aggregated Model}\}_{HE}, \log(\text{Aggregation})_B$$

Postulate: $C \triangleleft \{\text{Aggregated Model}\}_{HE}$

- **M4:** Cloud servers (C) update the global model and broadcast the encrypted global model updates back to IoT devices (D) via blockchain (B):

$$C \rightarrow D : \{\text{Global Model Update}\}_{K_{C,D}}, \log(\text{Update})_B$$

Postulate: $D \triangleleft \{\text{Global Model Update}\}_{K_{C,D}}$

Derivations and Authentication Verification:

- **D1:** From **M1**, **A1**, and **A3**:

$$F \triangleright (D \triangleright \text{Data})$$

Fog nodes believe the data sent by IoT devices is authentic and securely encrypted.

- **D2:** From **M2**, **A1**, **A2**, and **A4**:

$$M \triangleright (F \triangleright \text{Local Model Updates})$$

Microservices believe the local model updates from fog nodes are authentic and securely encrypted.

- **D3:** From **M3**, **A1**, **A2**, **A3**, and **A4**:

$$C \triangleright (M \triangleright \text{Aggregated Model})$$

Cloud servers believe the aggregated model updates from microservices are authentic, securely computed, and encrypted.

- **D4:** From **M4**, **A1**, **A2**, and **A3**:

$$D \triangleright (C \triangleright \text{Global Model Update})$$

IoT devices believe the global model updates from cloud servers are authentic and securely transmitted.

Based on the foregoing explanation, when we make a BAN logic analysis, it is clear that the federated learning architecture applied to the IoT scenarios with microservice-based architecture and blockchain can provide a secure, robust, and privacy-preserving environment for model training. DABE, HE, and SMPC can be applied for authentication and integrity proof during data and model updates between IoT devices, fog nodes, microservices, and cloud servers, while the blockchain network can be used for trustworthy logging, leading to provable auditability of entire transactions. This combination of the technologies guarantees that both the entire learning process and the privacy of data can be provided securely to cater to reliable decentralized learning and gain the trust of all participants.

V. Analysis of Proposed Model

Our proposed federated learning framework utilizes blockchain technology and sophisticated cryptographic primitives such as Decentralised Attribute-Based Encryption (DABE), Homomorphic encryption, and Secure Multi-Party Computation (SMPC) to enhance data privacy and security during collaborative learning, from data contribution to model transmission and aggregation. The use of DABE can ensure that only authorized fog nodes and cloud servers with the right attributes can access and decrypt the data, thus preventing unauthorized access. It helps protect from data privacy attacks such as data poisoning, etc Homomorphic encryption can secure the model transmission and model aggregation, ensuring that computations on the data can be made without revealing the original data. SMPC can keep the raw data private during model aggregation by allowing encrypted exchanges between fog nodes and cloud servers.

Moreover, it resolves security issues inherent to centralized models by spreading the tasks across multiple entities using blockchain technology – a tamper-proof ledger that stores an immutable history of any transactions, model updates, and computations, thereby making it more transparent, secure and reducing a single point of failure. Meanwhile, the use of differential privacy in aggregating model weights ensures that the data would not leak and avoids data memorization, protecting users' privacy and preserving the accuracy of the model. These components seamlessly work together to create a robust federated and secure learning environment to counter the various data privacy and security threats present in IoT scenarios. FL-DABE-BC is a robust framework ensuring data privacy, integrity, complete transparency, and accountability in the system and ensuring secure and effective communication between the nodes. It is a trustworthy, reliable, and secure framework for collaborative learning.

The following analysis details how FL-DABE-BC holds up against various vulnerabilities and attacks:

A. Anonymity

Anonymity is built in the federated learning framework using the Decentralized Attribute-Based Encryption (DABE). In this framework, data coming from IoT devices is encrypted with DABE. Those that can decrypt the data are only those with the right attributes. Thus, any participant (IoT devices as data sources) is anonymous to any outsider (attacker) who has no right attribute. Blockchain also guarantees anonymity in recording all transactions without revealing the identities of the blockchain network and can engage in pseudonymous transactions.

B. Non-Traceable and Impersonation Attacks

Furthermore, the framework can also mitigate non-traceable and impersonation attacks through the use of Decentralised Attribute-Based Encryption (DABE) and blockchain. DABE will ensure that only users who hold the proper credentials can study data or be part of the distributed network, thus preventing impersonation or unauthorized access. Moreover, due to the inherent nature of federated learning, that is, staying on-device, the data source is untraceable, thus preventing data tracing. And, through blockchain's inherent immutable ledger, it becomes impossible for an attacker to impersonate a legitimate node without being detected. Moreover, the pure use of blockchain technology by itself guarantees that attackers will not be able to trace transactions back to their source as due to the use of secure cryptographic hashes, the whole blockchain ledger is protected.

C. Message Modification Attacks

The proposed framework protects against message modification attacks by leveraging homomorphic encryption (HE) and blockchain. With homomorphic encryption, model weights, and data remain encrypted throughout the training and aggregation processes, ensuring that even if an attacker intercepts the messages, they cannot modify the content without detection. Furthermore, the blockchain records every transaction in a tamper-proof ledger. Any attempt to modify a message or model update would require altering all subsequent blocks, which is computationally infeasible. This ensures the integrity of messages exchanged between IoT devices, fog nodes, and cloud servers.

D. Replay Attacks and Man in the Middle Attacks

The framework protects against replay and man-in-the-middle attacks using blockchain and SMPC. Because the ledger provided by the blockchain is unchangeable, the use of blockchain prevents replay attacks by establishing that every transaction is independently unique and cannot be copied without this uniqueness being detectable and unacceptable. Since the blockchain provides a secure communication channel between the clients that are generating the data to be aggregated, any attempts at man-in are detectable as the inputs must pass cryptographic checking before entering the blockchain and hence entering the aggregation protocol. Furthermore, the inputs are 'blinded' by the SMPC aggregation protocol so that, if an attacker were to capture the data during the aggregation, nothing useful could be discerned about the inputs so the computation process retains its confidentiality and integrity.

VI. Conclusion

The research proposed a novel federated learning framework based on blockchain, decentralized attribute-based encryption (DABE), homomorphic encryption, secure multi-party computation (SMPC), and differential privacy for enhanced data security, privacy, and decentralized authentication in IoT market spaces. DABE ensures that only the set of parties who possess the correct attributes can access and process the ciphertext of data, this results in superior data confidentiality and access control. Homomorphic encryption and SMPC help to maintain privacy for the aggregation and computation of the encrypted data without needing to access the individual data points of each contributing device. The blockchain enables transparency, immutability, and integrity; it securely logs all transactions, model updates, and operations on the blockchain on the network which promotes trust among every node on the network.

The proposed framework is highly secure, scalable, and efficient, with fog-layer microservices performing the data aggregation, real-time analytics, and communication. The modular design would enable the scaling of the functionality flexibly with the number of IoT devices and fog nodes, depending on the computational and data requirements. Differential privacy brings an additional useful functionality of shielding the information about individual contributions from leakage even after the aggregation. To summarise, a detailed framework for secure, decentralized, and privacy-preserving federated learning in IoT environments is proposed, which can be extended in the future.

Table 1: A Comparative Table of FL-DABE-BC Framework and Other Frameworks

Groups	Attacks	IFed [18]	BC/Smart Contract + FL [16]	Differential Privacy + FL [17]	IDS + FL [12]	Privacy-Preserving-Group-Signatures + FL [15]	Semi-Asynchronous-Hierarchical + FL [14]	Contextual-Client-Selection + FL [13]	FL-DABE-BC (proposed)
Security	DoS Attacks (Sybil)	Yes	Yes	No	No	No	Limited	Yes	Yes
	Spoofing Attacks	Yes	Limited	No	No	No	Yes	Yes	Yes
	Tampering Attacks	Yes	Yes	Limited	Limited	No	Limited	Limited	Yes
	Replay Attacks	Yes	Yes	Limited	Limited	-	Limited	Limited	Yes
	Byzantine Fault Tolerance Attack	Yes	Yes	-	-	-	-	No	Yes
	Backdoor attacks	Yes	Limited	No	-	-	-	No	Yes
	Centralized Server Compromise	No	Yes	No	Yes	No	Yes	No	Yes
	Masquerading Attacks	Yes	Limited	No	No	No	Yes	Yes	Yes
	Front Running Attack	No	-	Yes	No	No	No	-	Yes
	Message Modification	Yes	Yes	Limited	Limited	Yes	Limited	Yes	Yes
	Man in the Middle Attack	Yes	Yes	Limited	Limited	-	Limited	Limited	Yes
	Model Inversion	Yes	No	-	-	-	-	Limited	Yes
Privacy Preserving	Eavesdropping	Limited	Yes	Limited	Yes	Yes	Yes	Yes	Yes
	Location Pinpointing	Limited	No	No	Limited	Yes	Limited	Limited	Yes
	Anonymity	-	Yes	Yes	Yes	-	Yes	Yes	Yes
	Non-traceability and Impersonation Attacks	Yes	Limited	Yes	Yes	-	Yes	Yes	Yes
	Traffic Analysis	Limited	-	Limited	Limited	Yes	Limited	Limited	Yes
	Data Poisoning	Yes	-	Limited	-	-	Limited	Limited	Yes
	Side Channel Attack	Limited	No	Yes	No	No	-	-	Yes
	Collusion Attack	Yes	Limited	Yes	No	Yes	-	No	Yes

Note: In cases where specific details were not explicitly provided in the sources, the analysis has been interpreted subjectively.

VII. Future Scope

We propose a blockchain-based federated learning framework with advanced cryptographic techniques, opening new research avenues. Enhanced decentralized attribute-based encryption (DABE) algorithms could offer more secure, granular access control and reduce computational overhead for IoT devices. Improved differential privacy mechanisms might balance data leakage prevention with model accuracy. Optimizing homomorphic encryption and Secure Multi-Party Computation (SMPC) can boost aggregation efficiency and scalability for numerous nodes and complex models. The framework's adaptability could extend to smart healthcare and industrial IoT, with scalability tested in real-world settings. Automated tools for microservice management could ease deployment across diverse IoT environments.

REFERENCES

[1] Z. Ali, H. Ali, and M. Badawy, "Internet of things (iot): Definitions, challenges, and recent research directions," *International Journal of Computer Applications*, vol. 128, pp. 975–8887, 10 2015.

[2] S. Ben Atitallah, M. Driss, and H. Ben Ghezala, "Fedmicro-ida: A federated learning and microservices-based framework for iot data analytics," *Internet of Things*, vol. 23, p. 100845, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523001683

[3] A. Rabay'a, E. Schleicher, and K. Graffi, "Fog computing with p2p: Enhancing fog computing bandwidth for iot scenarios," in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2019, pp. 82–89.

[4] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950705121000381

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2011, pp. 568–588.

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[7] X. Yi, R. Paulet, E. Bertino, X. Yi, R. Paulet, and E. Bertino, *Homomorphic encryption*. Springer, 2014.

[8] R. Cramer, I. B. Damgård *et al.*, *Secure multiparty computation*. Cambridge University Press, 2015.

[9] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*. Springer, 2006, pp. 1–12.

[10] B. Liu, N. Lv, Y. Guo, and Y. Li, "Recent advances on federated learning: A systematic survey," *Neurocomputing*, vol. 597, p. 128019, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231224007902

[11] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2017. [Online]. Available: https://arxiv.org/abs/1610.05492

[12] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Computer Communications*, vol. 195, pp. 346–361, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366422003516

[13] R. Song, L. Lyu, W. Jiang, A. Festag, and A. Knoll, "V2x-boosted federated learning for cooperative intelligent transportation systems with contextual client selection," 05 2023.

[14] Q. Chen, Z. You, and H. Jiang, "Semi-asynchronous hierarchical federated learning for cooperative intelligent transportation systems," 10 2021.

[15] S. Kanchan, J. W. Jang, J. Y. Yoon, and B. J. Choi, "Efficient and privacy-preserving group signature for federated learning," *Future Generation Computer Systems*, vol. 147, pp. 93–106, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X23001528

[16] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: a systematic literature review," *Artificial Intelligence Review*, vol. 56, pp. 1–35, 09 2022.

[17] H. Batool, A. Anjum, A. Khan, S. Izzo, C. Mazzocca, and G. Jeon, "A secure and privacy preserved infrastructure for vanets based on federated learning with local differential privacy," *Information Sciences*, vol. 652, p. 119717, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025523013026

[18] C. Hui, S. Liu, R. Zhao, and X. Xiong, "Ifed: A novel federated learning framework for local differential privacy in power internet of things," *International Journal of Distributed Sensor Networks*, vol. 16, p. 155014772091969, 05 2020.

[19] R. Sharma, M. Wazid, and P. Gope, "A blockchain based secure communication framework for community interaction," *Journal of Information Security and Applications*, vol. 58, p. 102790, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212621000351

[20] C. So, K. Conway, X. Yu, S. Yao, and K. Wong, "opp/ai: Optimistic privacy-preserving ai on blockchain," 2024. [Online]. Available: https://arxiv.org/abs/2402.15006

[21] J. Sierra, J. Hernandez-Castro, A. Alcaide, and J. Torres, "Validating the use of ban logic." 01 2004, pp. 851–858.