

Blockchain-enabled Federated Learning for Security and Privacy in Consumer Electronics Devices

Debashis Das, Pushpita Chatterjee, Sourav Banerjee, Uttam Ghosh, and Mohammed S. Al-Numay

Abstract—Consumer electronics devices (CEDs) are becoming increasingly interconnected and integrated into our daily lives. Thus, the demand for seamless communication, enhanced security, and reliable performance has increased. However, the widespread adoption of these devices raises significant concerns regarding security and privacy in computing, especially when collecting and processing sensitive consumer data. To address these challenges, robust security mechanisms are necessary to protect this sensitive data. In response to these challenges, Blockchain-Enabled Federated Learning for Consumer Electronics Devices (BFLCED) is proposed to make CEDs more secure and privacy-preserving. The combination of blockchain and federated learning (FL) provides a robust solution for real-world CEDs where data privacy and security are most important. The proposed BFLCED ensures devices are authenticated and communicated securely to maintain data integrity and confidentiality during model training. It generates unique identities using the Lightweight Elliptic Curve Digital Signature Algorithm (LECDSA) and digital signatures for data integrity. Parallely, smart contracts are employed to verify device identities & data integrity automatically and enable secure communication among devices. Data privacy is maintained during model aggregation by securely aggregating updates using encryption and multi-party computation (MPC). In the end, a security analysis is conducted to evaluate the effectiveness of the proposed mechanisms in safeguarding CEDs against potential threats and vulnerabilities. Furthermore, the proposed BFLCED transforms automation and personalization by securely connecting CEDs to our daily lives.

Index Terms—Consumer Electronic Devices, Secure Communication, Attack Resistance, Data Privacy, Decentralized Learning, Secure Aggregation.

I. INTRODUCTION

IN our increasingly connected world, the role of consumer electronics devices (CEDs) has become more prominent. From smartphones to smart home devices, these gadgets have been woven into the fabric of our daily lives to make them more convenient and efficient. These devices facilitate seamless communication, entertainment, and productivity in our lives. Consumers increasingly rely on these devices to store and transmit sensitive personal information, such as financial data, health records, and browsing habits [1]. However, inadequate security protocols are significant vulnerabilities inherent in the design and operation of systems that handle sensitive data. As the connected ecosystems expand, the complexity

D. Das, P. Chatterjee, and U. Ghosh are with the Department of CS and DS, Meharry Medical College, Nashville, TN, USA. (e-mail: debashis.das@ieee.org, pushpita.c@ieee.org, ghosh.uttam@ieee.org).

S. Banerjee is with the Department of CSE, Kalyani Government Engineering College, Kalyani, WB, India (e-mail: mr.sourav.banerjee@ieee.org).

M. S. Al-Numay is with the Department of Electrical Engineering, King Saud University, Riyadh, Saudi Arabia (e-mail: alnumay@ksu.edu.sa).

Corresponding author: Debashis Das.

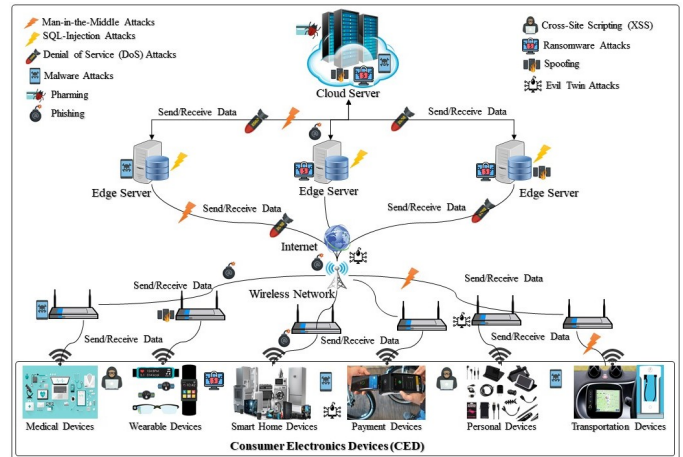


Fig. 1. Potential cyberattacks in CEDs.

and interconnectedness of these devices increase the potential attack surface. Moreover, the limited computational and energy resources of CEDs constrain the implementation of robust security measures. The current phase of CEDs suffers from various challenges, such as security and privacy threats from external attackers and inherent vulnerabilities within the devices themselves [2].

Challenges: In recent years, ransomware attacks have become increasingly prevalent and target CEDs [3]. According to Startups magazine, data security is a major worry for CEDs, with up to one in three Americans facing data breaches yearly [4]. A 2024 survey by U.S. News 360 Reviews found that 80% of U.S. adults have had data breaches [4] and CEDs are facing an increasing number of cyberattacks [5]. A UK consumer organization reported over 12,000 attempts to compromise smart home products in just one week [4]. As we connect more technologies, these attacks are expected to rise as shown in Fig. 1. Many devices collect sensitive data or make critical decisions that make them vulnerable to attacks on privacy, security, and even identity [6]. On the other hand, denial-of-service (DoS) attacks disrupt the normal functioning of CEDs, degrade service performance, and cause outages [7]. Man-in-the-middle (MITM) attacks intercept and manipulate communications between CEDs and external servers [7]. Attackers eavesdrop on sensitive data exchanged between devices, and they compromise the confidentiality and integrity of CED systems [8]. They lack robustness in verifying the identity of users or devices [9]. Traditional methods (e.g., encryption, authentication, access control, etc.) have proven to be insufficient to address these challenges [10]. Without robust encryption measures, data is left vulnerable to interception

and exploitation by malicious actors. Thus, weak encryption practices create a gateway for unauthorized access to severe such vulnerabilities. This distrust could slow CEDs industry innovation and impede growth. Manufacturers may fail to provide timely security updates or patches where devices are susceptible to known exploits and malware infections [11], [12]. Therefore, there is a need for a multifaceted approach to mitigate security and privacy issues stemming from these vulnerabilities.

Motivation: Meanwhile, blockchain is a distributed ledger technology that enables secure and transparent record-keeping across a network of decentralized nodes [13]. The data structure of blockchain ensures that transactions cannot be altered once recorded [14], which is lacking in traditional systems. In the context of CEDs, blockchain can enhance security and trust in various aspects. Manufacturers can establish secure device authentication protocols where unique device identifiers are recorded on the blockchain. So, authenticated devices can interact with the network to mitigate the risk of unauthorized access or tampering [15]. On the other hand, Federated Learning (FL) enables model training to be performed across distributed devices to preserve data privacy [16]. It ensures that sensitive information remains private and secure by keeping the data on the CEDs that collect sensitive consumer data to safeguard unauthorized access [17].

Our Approach: In light of these challenges and benefits of the hybrid combination, this paper proposes a secure and privacy-preserving approach named Blockchain-Enabled Federated Learning for Consumer Electronics Devices (BFLCED) that combines blockchain [18] with FL [16] to enhance the security and privacy of CEDs. This hybrid approach establishes a secure and efficient model for device authentication, data integrity, and privacy-preserving model updates in CEDs [19]. In our proposed work, data is stored across multiple nodes, which makes it difficult for any single entity to tamper with the information [20]. The transparent nature of blockchain raises concerns about data exposure and confidentiality as transactions are visible to anyone [21]. Thus, FL is considered to address these privacy issues in the blockchain network [22]. In addition, the Lightweight Elliptic Curve Digital Signature Algorithm (LECDSA) is designed to authenticate CEDs for generating digital signatures based on elliptic curve cryptography (ECC) [23], which provides equivalent security strength with significantly smaller key sizes compared to traditional algorithms. This compactness reduces the computational overhead for resource-constrained devices with limited processing power, memory, and energy. Besides, multi-party computation enables collaborative computation across multiple devices or entities without revealing their inputs. It is used in this work to enhance the privacy and security of operations performed by CEDs. Furthermore, the proposed BFLCED aims to establish a robust, secure, and efficient framework for CEDs.

Contribution: The primary contributions of this paper are outlined below:

- The paper presents a secure communication algorithm for identity generation and authentication of CEDs by utilizing the LECDSA algorithm.

- A privacy-preserving method for securely aggregating model updates is proposed in the BFLCED approach using blockchain, FL, and MPC to ensure privacy protection.
- The paper conducts a security analysis to evaluate the proposed mechanisms' effectiveness in protecting CEDs from threats and vulnerabilities.
- The paper conducts experiments to validate the efficacy and performance of the proposed approach.

Organization: The rest of the paper is organized as follows: Section II reviews and discusses related works in detail. The proposed methodology is outlined and demonstrated in Section III. In Section IV the security analysis of the proposed method is discussed. Section V presents the experimental setup and results with an in-depth discussion of the results and the proposed method. Finally, Section VI concludes the paper and provides related future research directions.

II. RELATED WORKS

Numerous approaches have been proposed to secure FL using blockchain. For instance, some studies introduced blockchain-based FL frameworks but faced issues with high computational overhead and limited scalability. Others optimized consensus mechanisms to improve efficiency but still struggled with storage inefficiencies. Some focused on enhancing the privacy of FL but did not adequately address execution complexity. Traditional authentication methods like passwords and biometrics are vulnerable to attacks such as brute force, password guessing, and spoofing. Centralized authentication systems pose risks of single points of failure and potential data breaches. Kwon et al. [24] proposed a lightweight digital signature scheme tailored for resource-constrained IoT devices. They addressed the computational overhead by optimizing cryptography operations and reducing memory requirements. However, their approach faces challenges in balancing security and efficiency. Another study by Shukla et al. [25] explored the use of ECC for digital signatures in CEDs and demonstrated the feasibility of ECC in reducing computational overhead while maintaining security. Nonetheless, challenges remain in terms of key management and scalability, especially in large-scale deployment scenarios. Gong et al. [26] proposed a blockchain-based authentication framework for IoT devices. They addressed scalability challenges by employing sharding techniques and optimizing consensus algorithms. However, managing private keys securely remains a challenge. Hwaitat et al. [27] presented a blockchain-based authentication scheme for smartphones to manage user authentication and access control. However, the overhead of executing smart contracts on resource-constrained devices was a concern. Khalil et al. [28] introduced a blockchain-based authentication protocol for CEDs by employing zero-knowledge proofs. However, the computational overhead of zero-knowledge proofs was a limitation. Liu et al. [29] developed a blockchain-based authentication mechanism for smart home devices. They employed decentralized identity management and verifiable credentials. However, the proposed approach still faces the challenges of reliability in decentralized identity sources and

TABLE I
USEFUL NOTATIONS AND THEIR DEFINITION

Notation	Description
M	Message to be signed or validated
SK	Private key used for signing
PK	Public key used for signature verification
G	Generator point on the elliptic curve
d	Random scalar for signature generation
r, s	Signature components generated using LE-CDSA
$H(M)$	Hash of the message M
p	Curve parameter in modular arithmetic
n	Order of the elliptic curve
x_P	x-coordinate of the elliptic curve point P
$\mathbb{S}E_i$	Securely aggregated encrypted local model update of device D_i
\mathbb{G}	Decrypted aggregated global model update
u_1, u_2	Intermediate values for signature validation
P	Point on the elliptic curve used in LE-CDSA
T_{iter}	Time taken for an iteration of model training without encryption.
T_{enc}	Time required for encrypting each model update.
T_{dec}	Time required for decrypting the aggregated model update.
T_{comm}	Communication delay due to the increased size of encrypted messages.
T_{agg}	Time required for secure aggregation of encrypted updates.
N	Number of devices participating in FL.
λ_0	Convergence rate without encryption.
λ_{enc}	Convergence rate with encryption.
$Attack_{D_i}$	Represents an attack targeting device D_i
\mathcal{V}_{D_i}	Set of vulnerabilities present in device D_i
\mathcal{T}_{D_i}	Represents the level of threats targeting device D_i
S_{D_i}	Security mechanism deployed on device D_i to mitigate vulnerabilities and threats.
\mathcal{P}_{D_i}	Privacy mechanism implemented on device D_i to safeguard user data and prevent unauthorized access.
$\neg\mathcal{V}_{D_i}$	Absence of vulnerabilities in device D_i .
$\neg\mathcal{T}_{D_i}$	Absence of threats targeting device D_i .
\mathcal{D}_{D_i}	Amount of data stored centrally for device D_i .
\mathcal{U}_{D_i}	Number of model updates sent (as opposed to raw data) for device D_i in FL.
\mathcal{R}_{D_i}	Risk of data breach for device D_i .
\mathcal{A}_{D_i}	Size of the attack surface related to authentication of device D_i .
\mathcal{C}_{D_i}	Complexity of authentication mechanisms for device D_i .
S_{D_i}	Security strength of authentication for device D_i .
\max_C	Maximum possible complexity of authentication mechanisms.
\max_S	Maximum possible security strength.
$\max_{\mathcal{H}}$	Maximum possible hash strength.

managing revocation. Wu et al. [30] proposed a blockchain-based authentication mechanism for connected vehicles to securely manage vehicle identities and access control for secure communication between vehicles and infrastructure. However, the main challenge of the proposed work is the lack of real-time authentication. yang et al. [31] provided a blockchain-based authentication framework for smart home devices to establish a decentralized trust management system by utilizing secure device authentication and access control. However, the work suffered because of the overhead of blockchain transactions. These blockchain-based mechanisms address specific security needs but face challenges such as reliability, real-time authentication, and transaction overhead.

III. PROPOSED BFLCED METHOD

The proposed BFLCED consists of several components with specific functionalities to achieve the desired goals. The key components (listed below) of the BFLCED are mainly blockchain integration with secure identity generation and communication between devices, smart contract deployment, and blockchain-enabled FL for secure aggregation. However, Table I shows the required symbols used in this paper and their definitions.

CEDs act as nodes, the participants in the system, and compute model updates based on their local data, which preserves privacy by ensuring raw data never leaves the device. To secure their communications, CEDs generate a public-private key pair using the LECDSA. This cryptographic step establishes a secure foundation for encrypted communications. Once the updates are computed, they are encrypted to maintain confidentiality and signed digitally to provide a verifiable identity for each sender. CEDs also verify the authenticity and integrity of received data to ensure only valid updates contribute to the system.

The central server secures aggregating model updates received from multiple CEDs. It securely aggregates encrypted model updates received from multiple CEDs using MPC, which prevents exposure of individual contributions. The aggregated updates are used to refine and update the global model. The central server processes encrypted data without needing access to the raw inputs.

Blockchain is the most important component of the proposed system. Its role is defined by its core properties of immutability, transparency, and integrity, which ensure the system's reliability and trustworthiness. The blockchain is a tamper-proof ledger that records transactions, including key exchanges, model updates, and verification events. Once added to the blockchain, these records cannot be altered or deleted. It allows all participants to view and verify the recorded transactions and secures its records using cryptographic techniques to make unauthorized modifications in the proposed system nearly impossible.

Smart contracts automate and secure key operations without requiring trust between parties. These contracts facilitate secure and tamper-proof public key exchanges between CEDs and the central server using blockchain. To prevent unauthorized access, smart contracts verify the authenticity of participating CEDs. This validation process confirms that only legitimate devices with proper credentials can contribute updates or participate in the system. It strengthens the overall security framework by blocking malicious entities from infiltrating the system to maintain the quality and integrity of the system's learning process.

A. Decentralized Identity Management for CEDs

In this proposed work, a blockchain network maintains a decentralized ledger to record all identities and interact among CEDs with the edge cloud. As shown in Fig. 2, blockchain is integrated with an edge-cloud server to create a robust and secure platform for handling CEDs. Edge resources are deployed closer to the devices to reduce latency and improve response times. This enables efficient data processing and analysis at the edge.

1) *Identity Generation of CEDs*: Algorithm 1 is designed using the lightweight LECDSA to minimize the computational burden and ensure optimal performance on resource-constrained devices. It guarantees robust digital signatures for upholding the integrity and authenticity of transactions within the proposed blockchain system for CEDs. It generates a unique digital signature (r, s) for a given message M

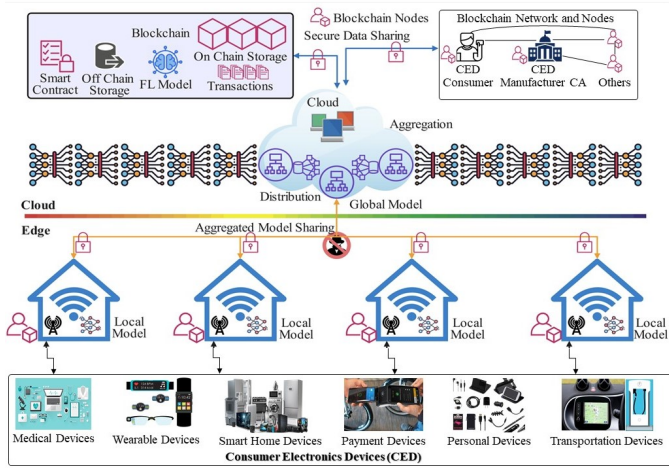


Fig. 2. Proposed BFLCED framework.

using a private key SK and a curve parameter p . Therefore, the algorithm computes a point P on the elliptic curve by multiplying the base point G by the secret scalar d , (i.e., $P = d \times G$). This point represents a unique identifier derived from the private key and is used in the signature generation process. Therefore, this algorithm calculates the x-coordinate x_P of the computed point P . This x-coordinate is reduced modulo p to ensure it falls within the finite field defined by the curve parameter p . If the computed x-coordinate r equals zero (indicates an invalid signature), the algorithm rejects the current scalar d and repeats the process by choosing another random scalar d . Once a valid x-coordinate r is obtained, the algorithm proceeds to compute the signature component s : $d^{-1}(H(M) + SK \times r) \pmod{n}$. Finally, the algorithm returns the computed unique signature (r, s) for the given message M .

2) *Identity Validation of CEDs*: To ensure the authenticity of identities generated using *Algorithm 1*, a validation process is necessary, which is presented in *Algorithm 2*. It confirms that the signature associated with an identity is valid and can be trusted. The first step is to compute the hash of the original message M using the same cryptography hash function employed during the signature generation process. This ensures consistency between the message used for signature generation and the one used for validation. Two intermediate

values, u_1 and u_2 , are computed using *Equations 1* and *2*. These intermediate values are essential for reconstructing a point on the elliptic curve. Utilizing the public key PK and computed intermediate values u_1 and u_2 , a point P on the elliptic curve is reconstructed. Then, from the reconstructed point P , the x-coordinate x_P is extracted. This x-coordinate is compared with the signature component r . The extracted x-coordinate x_P is compared with r modulo the curve parameter p . If the signature is valid, it confirms the identity's authenticity. Upon successful authentication, the generated identity is validated and made trustworthy within the proposed BFLCED framework.

$$u_1 = H(M) \times s^{-1} \pmod{n} \quad (1)$$

$$u_2 = r \times s^{-1} \pmod{n} \quad (2)$$

3) *Smart Contracts for Secure Communication*: Smart contracts deployed on the blockchain verify the authenticity of device identities using *Algorithms 1* and *2*. Assume that each device (A and B) generates a unique public-private key pair using the LECDsa algorithm. Device A possesses its public key PK_A and private key SK_A , while Device B holds its public key PK_B and private key SK_B . Devices A and B securely exchange their public keys through trusted channels or store them on the blockchain. Now, Device A initiates secure communication with Device B. Before transmission, Device A signs the message with its private key SK_A by producing a digital signature (r, s) using *Algorithm 1*. Then, Device A transmits the message along with the digital signature (r, s) and its public key PK_A to Device B. Upon receiving the message, Device B interacts with a smart contract to further validate Device A's identity. The smart contract verifies the signature (r, s) against Device A's public key PK_A using *Algorithm 2*. If the signature is valid, the smart contract confirms Device A's identity and approves the communication request. With Device A's identity confirmed and the message authenticated, Device B processes the received message and responds accordingly. In this way, smart contracts provide an additional layer of security by validating device identities and ensuring message integrity. *Algorithm (3)* ensures robust and efficient secure communication between CEDs and resolves potential vulnerabilities during the key exchange process.

Algorithm 1: Identity Generation Using LECDsa

Input: M, SK, p

Output: Signature (r, s)

- 1 Choose d randomly such that $1 < d < p$;
 - 2 Compute $P = d \times G$ on the elliptic curve;
 - 3 Compute $r \equiv x_P \pmod{p}$, where x_P is the x-coordinate of P ;
 - 4 **if** $r = 0$ **then**
 - 5 | Choose a d and repeat the process;
 - 6 Compute $s \equiv d^{-1}(H(M) + SK \times r) \pmod{n}$;
 - 7 **if** $s = 0$ **then**
 - 8 | Choose another d and repeat the process;
 - 9 **return** Signature (r, s)
-

Algorithm 2: Identity Validation Using LECDsa

Input: $M, (r, s), PK, p$

Output: Validation result

- 1 Compute $u_1 \leftarrow H(M) \times s^{-1} \pmod{p}$;
 - 2 Compute $u_2 \leftarrow r \times s^{-1} \pmod{p}$;
 - 3 Reconstruct point $P \leftarrow u_1 \times G + u_2 \times PK$;
 - 4 Extract x_P from P ;
 - 5 **if** $r \equiv x_P \pmod{p}$ **then**
 - 6 | **return** *True* ; // Signature is valid
 - 7 **end**
 - 8 **return** *False* ; // Signature is invalid
-

Algorithm 3: Secure Communication Between Device A and B

Data: PK_A, SK_A, PK_B, SK_B

Result: Successful communication

- 1 Generate keys: $PK_A, SK_A \leftarrow$ form **Algorithm 1**;
 $PK_B, SK_B \leftarrow$ LECDSA_KeyGeneration();
 - 2 Exchange keys securely: $PK_A \leftrightarrow PK_B$;
 - 3 Device A signs message: $(r, s) \leftarrow$ Sign(M, SK_A);
 - 4 Transmit: $(M, (r, s), PK_A)$;
 - 5 Verify: Verify($M, (r, s), PK_A$);
 - 6 Verify: SmartContractVerify($PK_A, (r, s)$);
 - 7 Establishing Communication: Process message: M ;
-

B. Secure Model Aggregation

The next critical aspect is ensuring privacy and integrity in collaborative learning environments by creating secure identity management and communication protocols established for CEDs. This section discusses how secure model aggregation in FL facilitates combining model updates from multiple devices to enhance the global model and safeguard data privacy. Initially, the device D_i generates a local model update $\theta_{\text{local}}^{(t+1)}(D_i)$ at iteration $(t + 1)$, as shown in *Algorithm 4*. Device D_i encrypts its local model update $\theta_{\text{local}}^{(t+1)}(D_i)$ using its public key PK_i . This encryption process ensures that the individual updates remain confidential and inaccessible to unauthorized parties. Once the local updates are encrypted, they are securely aggregated using MPC protocols to compute an aggregated update denoted as \mathbb{SE} .

$$\mathbb{SE}_i = \text{Enc}(\theta_{\text{local}}(t + 1)^{(D_i)}, PK_i) \quad (3)$$

Thus, the actual model updates remain private throughout the aggregation process. After the aggregation process, the resulting securely aggregated update \mathbb{SE} is decrypted using *Equation 4*.

$$\mathbb{G}_i = \text{Dec}(\mathbb{SE}_i, SK_i) \quad (4)$$

This decryption step allows the aggregation point to obtain the aggregated update \mathbb{G}_i , which represents the collective contribution of all devices to the global model. Finally, the decrypted aggregated update \mathbb{G}_i is used to update the global model $\theta_{\text{Global}}^{(t+1)}$. Each device's contribution is considered, and the updated global model (see *Equation 5*) is computed as the average of the decrypted updates from all participating devices. Thus, each device's model updates remain confidential during aggregation.

$$\theta_{\text{global}}^{(t+1)} = \frac{1}{N} \sum_{i=1}^N \theta_{\text{local}}^{(t+1)}(D_i) \quad (5)$$

However, the process of encrypting each local model update can introduce additional time delays. These delays are associated with encryption overhead (T_{enc}) and decryption overhead (T_{dec}). The increased time for each iteration due to these operations can slow down the overall convergence rate of the model. Encrypted model updates \mathbb{SE}_i are typically larger than

their plaintext versions due to added cryptographic metadata and padding. This increased size can lead to higher transmission times and affect the communication latency (T_{comm}). Longer communication times can delay the synchronization of model updates and impact the speed of convergence. The secure aggregation process using MPC also introduces additional computational steps. This delay can also influence the convergence rate by extending the time required to aggregate and synchronize model updates. To address these effects in the model convergence analysis, we provide the convergence rate λ to account for encryption impacts in *Equation 6*.

$$\lambda_{\text{enc}} = T_{\text{iter}} + T_{\text{enc}} + T_{\text{comm}} + T_{\text{agg}} \quad (6)$$

To address the impact of encryption on model convergence rates in FL, various time components are introduced by encryption and secure aggregation. The total time T_{total} for each iteration in encryption can be expressed as:

$$T_{\text{total}} = T_{\text{iter}} + N \cdot T_{\text{enc}} + T_{\text{dec}} \cdot N + T_{\text{comm}} + T_{\text{agg}} \quad (7)$$

The convergence rate λ is defined as the inverse of the total time required per iteration. Therefore, for the system with encryption, the convergence rate λ_{enc} is:

$$\lambda_{\text{enc}} = \frac{1}{T_{\text{total}}} = \frac{1}{T_{\text{iter}} + N \cdot T_{\text{enc}} + T_{\text{dec}} \cdot N + T_{\text{comm}} + T_{\text{agg}}} \quad (8)$$

For comparison, the convergence rate without encryption λ_0 is:

$$\lambda_0 = \frac{1}{T_{\text{iter}}} \quad (9)$$

To evaluate the impact of encryption, we compute the ratio of the convergence rates:

$$\text{Ratio} = \frac{\lambda_{\text{enc}}}{\lambda_0} = \frac{T_{\text{iter}}}{T_{\text{iter}} + N \cdot T_{\text{enc}} + T_{\text{dec}} \cdot N + T_{\text{comm}} + T_{\text{agg}}} \quad (10)$$

This ratio indicates how the presence of encryption affects the convergence rate relative to the non-encrypted case. Therefore, it can reduce the (T_{enc}) and (T_{dec}). Thus, λ_{enc} can be reduced, and the impact of encryption on convergence rates can be minimized in an efficient FL process.

Algorithm 4: Secure Model Aggregation in BFLCED

Data: Encrypted model updates $\mathbb{E}_1, \mathbb{E}_2, \dots, \mathbb{E}_N$

Result: Decrypted aggregated model update \mathbb{G}

- 1 Initialization: Set $\mathbb{SE} = \emptyset$;
 - 2 **for** $i \leftarrow 1$ **to** N **do**
 - 3 Perform encryption:
 $\mathbb{E}_i \leftarrow$ Encrypt($\theta_{\text{local}}(t + 1)^{(D_i)}, PK_i$);
 - 4 Add \mathbb{E}_i to securely aggregated updates:
 $\mathbb{SE} \leftarrow \mathbb{SE} \cup \mathbb{E}_i$;
 - 5 **end**
 - 6 Perform secure aggregation: $\mathbb{G} \leftarrow \mathbb{D}(\mathbb{SE}, SK_j)$;
-

IV. SECURITY ANALYSIS OF THE PROPOSED METHOD

Conducting a security analysis of the proposed method is essential to ensure that it effectively addresses vulnerabilities and threats within the system. The analysis verifies whether the proposed method can withstand various attacks.

A. Attack and vulnerability Analysis

This subsection aims to identify potential security weaknesses and vulnerabilities in CEDs that can be exploited by attackers. By analyzing these vulnerabilities, we can determine specific attack vectors and prioritize implementing robust countermeasures to enhance device security and privacy.

Attack and vulnerability: This analysis focuses on finding weaknesses in CEDs (for instance D_i). If the set of vulnerabilities \mathcal{V}_{D_i} is non-empty (i.e., $\mathcal{V}_{D_i} \neq \emptyset$), it means there are security flaws in the device D_i . This also indicates that an attack Attack_{D_i} targeting these vulnerabilities is possible. These vulnerabilities compromise the security of device D_i . Therefore, the proposed BFLCED addresses device vulnerabilities using the LECDSA, where a digital signature is generated and verified to ensure only legitimate devices participate.

Reduction of Vulnerabilities (\mathcal{V}_{D_i}) using BFLCED: Let $\mathcal{A}_{D_i}^{\text{before}}$ represent the attack surface size before blockchain integration and $\mathcal{A}_{D_i}^{\text{after}}$ after blockchain integration. Blockchain integration provides a decentralized ledger and uses cryptographic hashes to reduce vulnerabilities. The attack surface size can be modeled as:

$$\mathcal{A}_{D_i}^{\text{after}} = \mathcal{A}_{D_i}^{\text{before}} \cdot \left(1 - \frac{\mathcal{H}_{D_i}}{\max_{\mathcal{H}}}\right) \quad (11)$$

This implies $\mathcal{A}_{D_i}^{\text{after}}$ is smaller due to increased security from hashing and thereby reduces vulnerabilities: $\mathcal{A}_{D_i}^{\text{after}} < \mathcal{A}_{D_i}^{\text{before}}$. Now, Let $\mathcal{R}_{D_i}^{\text{before}}$ represent the risk of a data breach before FL, and $\mathcal{R}_{D_i}^{\text{after}}$ after FL. It reduces the amount of raw data (\mathcal{D}_{D_i}) that is sent and stored centrally. The risk can be modeled as a function of the amount of data stored centrally and the number of updates sent. We can express the risk reduction as:

$$\mathcal{R}_{D_i}^{\text{after}} = \mathcal{R}_{D_i}^{\text{before}} \cdot \left(1 - \frac{\mathcal{U}_{D_i}}{\mathcal{D}_{D_i} + \max_{\mathcal{U}}}\right) \quad (12)$$

This indicates that as the proportion of updates \mathcal{U}_{D_i} relative to the total data \mathcal{D}_{D_i} increases as well as the risk \mathcal{R}_{D_i} decreases. Therefore: $\mathcal{R}_{D_i}^{\text{after}} < \mathcal{R}_{D_i}^{\text{before}}$.

B. Threat Level Assessment

This section evaluates the likelihood and severity of potential attacks targeting a device by assessing its threat level. Based on this assessment, devices with higher threat levels will be prioritized for immediate countermeasures and mitigation strategies to reduce the risk of compromise.

Threat Level \mathcal{V}_{D_i} Assessment The threat level Threat_{D_i} is the likelihood and severity of potential attacks targeting device D_i . If \mathcal{T}_{D_i} is high (i.e., $\mathcal{T}_{D_i} > \text{threshold}$), then there exists Threat_{D_i} with a high probability of targeting device D_i . This assessment helps prioritize the mitigation strategies for resources and attention to the most critical

threats. When Threat_{D_i} exceeds the threshold, the proposed BFLCED deploys patches or countermeasures to D_i based on its logged vulnerabilities. These countermeasures are verified cryptographically before execution. This is achieved through dynamic prioritization, secure aggregation, private communication channels, and automated patch deployment.

Reduction of Threats (\mathcal{T}_{D_i}) Let $\mathcal{T}_{D_i}^{\text{before}}$ represent the likelihood of threats before blockchain-based authentication and usage of smart contracts, and $\mathcal{T}_{D_i}^{\text{after}}$ after. Blockchain integration increases the complexity and security of authentication mechanisms, and smart contracts ensure secure and predefined interactions. Therefore, the size of the attack surface decreases as the complexity and security strength increase, as follows:

$$\mathcal{T}_{D_i}^{\text{after}} = \mathcal{T}_{D_i}^{\text{before}} \cdot \left(1 - \frac{\mathcal{C}_{D_i}}{\max_{\mathcal{C}}}\right) \cdot \left(1 - \frac{\mathcal{S}_{D_i}}{\max_{\mathcal{S}}}\right) \quad (13)$$

and

$$\mathcal{T}_{D_i}^{\text{after}} = \mathcal{T}_{D_i}^{\text{before}} \cdot \left(1 - \frac{\mathcal{S}_{D_i} \cdot \mathcal{F}_{D_i}}{\max_{\mathcal{S}} \cdot \max_{\mathcal{F}}}\right) \quad (14)$$

Here, $\left(1 - \frac{\mathcal{C}_{D_i}}{\max_{\mathcal{C}}}\right)$ reflects the reduction in the attack surface due to increased complexity. Higher complexity \mathcal{C}_{D_i} reduces the attack surface to make successful attacks less. On the other hand, $\left(1 - \frac{\mathcal{S}_{D_i}}{\max_{\mathcal{S}}}\right)$ captures the effect of increased security strength. Higher security strength \mathcal{S}_{D_i} reduces the likelihood of successful attacks, and more secure and frequent interactions decrease the risk of threats. Therefore we can write: $\mathcal{T}_{D_i}^{\text{after}} < \mathcal{T}_{D_i}^{\text{before}}$. Thus, the attack surface \mathcal{A}_{D_i} is minimized, and the complexity \mathcal{C}_{D_i} and security strength \mathcal{S}_{D_i} are enhanced to a decreased likelihood of successful threats to authentication. Therefore, the BFLCED approach minimizes vulnerabilities and threats by enhancing security mechanisms through blockchain and FL integration by strengthening authentication and communication through smart contracts.

V. RESULTS AND DISCUSSION

In this work, we evaluated the performance of the proposed BFLCED framework through a series of experiments. These experiments aimed to assess key performance metrics, including transaction costs, execution times, and the security of FL model training. Our analysis focused on the effects of varying the number of transactions, comparing different Ethereum Virtual Machine (EVM) versions, and examining the impact on model accuracy and privacy during FL rounds. The experimental setup incorporated Remix version 0.53.0, Solidity compiler version 0.8.25, and Python version 3.12.2.

Transaction Cost Analysis: The analysis of transaction costs (as shown in Fig. 3c) revealed that as the number of transactions increased from 100 to 1000, both transaction and deposit costs increased proportionally. However, an important observation was that the average transaction cost remained relatively stable, even with the increase in transaction volume. This stability indicates that the BFLCED framework is capable of maintaining consistent transaction efficiency under higher transaction loads.

Execution Cost Analysis: Execution cost is the computational cost associated with running the smart contracts and

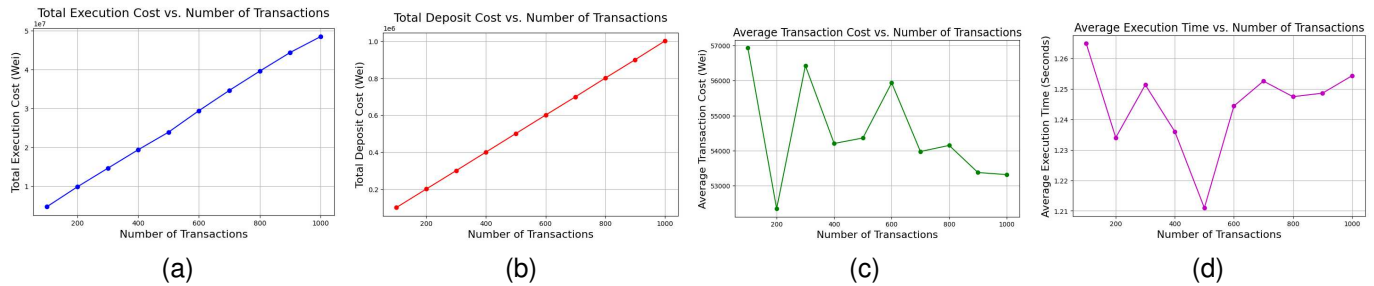


Fig. 3. Smart contracts cost analysis results. (a) Total execution cost. (b) Total deposit cost. (c) Average transaction cost. (d) Average execution time.

performing cryptographic operations required for the BFLCED framework. This includes costs for operations such as encryption, decryption, key management, and the execution of FL updates. Our experiments tracked the execution cost, particularly with the number of transactions and the complexity of the operations performed. As shown in Fig. 3a, execution costs increased as the transaction count increased. However, the increase in execution costs was not as steep as the increase in transaction volume, which indicates that the system was efficient in terms of executing the required operations for each transaction. Our proposed framework mitigated the computational burden of cryptographic operations using LECDSA to reduce execution costs while maintaining a high level of security.

Deposit Cost Analysis: Deposit cost is the cost associated with securing funds or gas fees for smart contract execution required for interactions with the blockchain. In our experiments, deposit costs were tracked alongside transaction costs, with both rising in proportion to the number of transactions. As shown in Fig. 3b, while deposit costs increased with the number of transactions, they exhibited more variability compared to transaction costs. This variability was due to the changing gas prices and the dynamic nature of the blockchain network. The fluctuating gas fees influenced the deposit amounts required to execute smart contracts, particularly in high-demand periods. Interestingly, despite these fluctuations, our proposed BFLCED framework maintained stable performance with relatively consistent deposit costs when compared to the transaction volume.

Average Execution Time: As shown in Fig. 3d, when the number of transactions increased, the execution times also increased, which is expected since more transactions take

longer to process. However, the BFLCED framework managed the increased load efficiently, and the execution times didn't rise too quickly as the number of transactions grew. This shows that the system can handle more transactions without becoming too slow, which is important for keeping the system quick and efficient.

Comparison of Different EVM Versions: The performance of the system was further analyzed by comparing different EVM versions—EVM v1 (Mainnet fork), EVM v2 (London), EVM v3 (Cancun), and EVM v4 (Berlin). These versions were evaluated based on varying gas prices and gas limits, which directly affect both transaction costs and execution times. The results, depicted in Fig. 4, highlight the trade-offs between cost-efficiency and performance for each EVM configuration. Gas prices and gas limits influence the overall transaction cost, with higher gas prices and limits leading to increased transaction costs but possibly improving execution efficiency, as shown in Fig. 4a. On the other hand, the comparison revealed that different EVM versions exhibit significant variations in execution times, as shown in Fig. 4b. EVM v3 (Cancun) and EVM v4 (Berlin) demonstrated more efficient processing of transactions compared to earlier versions and suggested that newer EVM configurations may be better suited for the BFLCED framework. This analysis is important for identifying the optimal EVM configuration for deploying smart contracts. By selecting the appropriate version, we can optimize the cost and performance of the BFLCED framework to improve its overall efficiency.

FL Process and Model Performance: The next aspect of our analysis focused on the FL process, as shown in Fig. 5. We monitored critical metrics such as model accuracy, privacy loss, and data leakage over multiple training rounds. These metrics are essential for evaluating the effectiveness of the BFLCED framework in balancing security and performance. Fig. 5a shows the FL process aimed to ensure that the model's accuracy remained high across all rounds. We closely tracked privacy loss to ensure that it stayed within acceptable thresholds throughout the training rounds (see Fig. 5b). The BFLCED framework showed resilience in maintaining strong privacy protections and mitigating risks of data leakage from individual devices. Data leakage is another critical metric monitored throughout the FL process. The analysis shown in Fig. 5c demonstrated that the BFLCED framework effectively safeguarded against potential data leakage so that sensitive information remained secure, even when aggregated for global model training. The goal of this analysis is to demonstrate

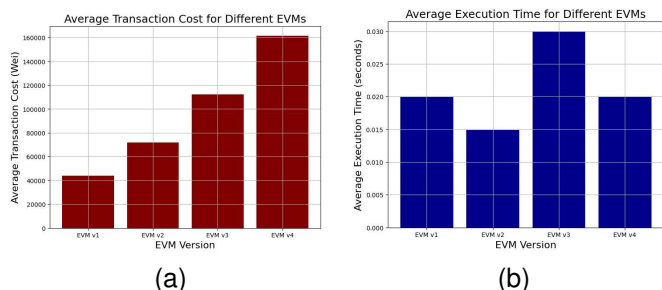


Fig. 4. Smart contract cost analysis for different EVMs. (a) Average transaction cost. (b) Average execution time.

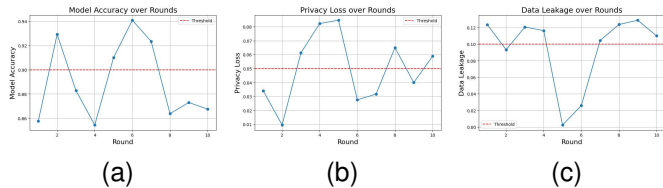


Fig. 5. FL model training analysis results. (a) Model accuracy. (b) Privacy loss. (c) Data Leakage.

the robustness of the BFLCED framework in maintaining both model performance and privacy over time. The results confirmed that the framework is effective at balancing these factors so that privacy-preserving methods do not significantly degrade the quality of the model or compromise data security.

Performance Analysis of BFLCED Framework The proposed BFLCED framework can introduce computational and communication overhead during the encryption of FL rounds. The overhead primarily arises from the added time and resource requirements for encrypting model updates before transmission and decrypting them upon receipt. This process can introduce delays in both local model training and global model aggregation, which impacts the overall system's efficiency. To mitigate these impacts, the paper incorporates secure aggregation protocols that aggregate encrypted model updates in a manner that reduces the overall encryption burden. The proposed BFLCED also optimizes the frequency of communication rounds to balance the need for frequent updates and the overhead introduced by encryption. Furthermore, lightweight encryption is considered to balance security with performance. These strategies are crucial to minimize the encryption-induced overhead for ensuring secure FL operations. Table II highlights key features and metrics relevant to evaluating blockchain-based solutions for CEDs within smart environments. In contrast, other approaches, like multi-factor authentication (MFA) [31] and blockchain authentication [26], [29], [27] introduce more complexity, which may not be ideal for low-power CEDs. The proposed BFLCED framework sets the foundation for future advancements in several domains in securely managing interconnected CEDs in smart environments. By balancing security, performance, and resource constraints, this approach provides a more practical and scalable solution for CEDs compared to other blockchain-based authentication and privacy-preserving methods. Overall, our experiments show that the BFLCED framework achieves a balance between transaction cost, execution cost, deposit cost, execution time, and FL model security. These findings underscore the practical feasibility of implementing the BFLCED framework in real-world scenarios for secure and privacy-preserving machine learning on CEDs.

CED Applications: The proposed method is highly effective for environments like hospitals and clinics where devices must be both energy-efficient and secure, which is not typically addressed by other frameworks that focus only on one of these aspects. For instance, in healthcare systems, multiple devices and healthcare providers need to communicate securely as they use thousands of devices to generate large amounts of data. The BFLCED framework is ideal for healthcare CEDs because

TABLE II
COMPARISON OF BFLCED AND EXISTING APPROACHES

Metric / Method	BFLCED	[29]	[27]	[31]	[26]
Algorithm Efficiency	High	High	Moderate	Moderate	High
System Complexity	Low	Low	High	High	Moderate
Resource Efficiency	High	High	Moderate	Moderate	High
Smart Contract Optimization	High	Moderate	Moderate	High	High
Storage Complexity	Low	Moderate	Moderate	High	Moderate
Communication Overhead	Optimized	Moderate	High	High	Moderate
Scalability	High	High	Moderate	Moderate	High
Adaptability	High	Moderate	Moderate	Low	Moderate
Privacy Preservation	Strong	Basic	High	High	Moderate

it combines strong security, decentralized trust, efficiency, and real-time threat mitigation. The use of encryption and secure aggregation ensures that sensitive medical data is protected during the FL process. It is particularly well-suited for the complex, resource-constrained, and highly sensitive nature of healthcare environments with scalable and secure solutions for healthcare interconnected devices.

VI. CONCLUSION

The proposed BFLCED framework provides a robust and secure solution for managing CEDs in decentralized environments. By integrating blockchain with FL, the framework effectively enhances both data privacy and device security and addresses common vulnerabilities and threats in CED networks. It employs secure aggregation protocols and lightweight cryptographic techniques to address common concerns, such as the computational and communication overheads associated with encryption during FL model updates. Its lightweight and efficient design, combined with robust security features and high scalability, makes it more suitable compared to more complex blockchain-based alternatives. The experimental results demonstrate the efficiency and robustness of the BFLCED framework across different layers of the system, from transaction processing to smart contract deployment. These findings validate the proposed solution's effectiveness in real-world consumer applications with a solid foundation for secure, scalable, and privacy-preserving operations in decentralized environments like CEDs. Overall, the BFLCED framework is a major step forward in secure and efficient decentralized environments for improving privacy and security. However, future work could address energy consumption concerns and boost privacy and security in BFLCED systems by integrating homomorphic encryption techniques.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation under Grant numbers 2219741 and 2401928. The work of Mohammed S. Al-Numay was also supported by the Researchers Supporting Project Number (RSP2024R150), King Saud University, Riyadh, Saudi Arabia.

REFERENCES

- [1] P. Chatterjee, D. Das, and D. B. Rawat, "Federated learning empowered recommendation model for financial consumer services," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2508–2516, 2024.
- [2] J. Wu, J. Zhang, M. Bilal, F. Han, N. Victor, and X. Xu, "A federated deep learning framework for privacy-preserving consumer electronics recommendations," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2628–2638, 2024.
- [3] D. Palmer, "Wannacry ransomware attack at lg electronics takes systems offline," <https://www.zdnet.com/article/wannacry-ransomware-attack-at-lg-electronics-takes-systems-offline/>, 2017, [Online; Accessed on Mar. 28, 2024].
- [4] P. West, "The biggest threat to consumer electronics is data security," <https://startupsmagazine.co.uk/article-biggest-threat-consumer-electronics-data-security/>, 2024, [Online; Accessed on Mar. 28, 2024].
- [5] B. R. Amin, M. Hossain, A. Anwar, and S. Zaman, "Cyber attacks and faults discrimination in intelligent electronic device-based energy management systems," *Electronics*, vol. 10, no. 6, p. 650, 2021.
- [6] P. Certified, "New report shows that consumers are concerned about device security," <https://www.psacertified.org/blog/consumers-are-concerned-about-device-security/>, 2023, [Online; Accessed on Mar. 28, 2024].
- [7] M. Sayad Haghghi, F. Farivar, A. Jolfaei, A. B. Asl, and W. Zhou, "Cyber attacks via consumer electronics: Studying the threat of covert malware in smart and autonomous vehicles," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 825–832, 2023.
- [8] F. Wahab, I. Khan, T. Hussain, A. Amir *et al.*, "An investigation of cyber attack impact on consumers' intention to purchase online," *Decision Analytics Journal*, vol. 8, p. 100297, 2023.
- [9] J. Su, Z. Hong, L. Ye, T. Liu, S. Liang, S. Ji, G. S. Aujla, R. Beyah, and Z. Wen, "Trustworthy iap: An intelligent applications profiler to investigate vulnerabilities of consumer electronic devices," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4605–4616, 2024.
- [10] A. S. George, T. Baskar, and P. B. Srikanth, "Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors," *Partners Universal International Innovation Journal*, vol. 2, no. 1, pp. 51–75, 2024.
- [11] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.
- [12] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M. A. Khan, A. Amir, K. V. Vuda, and A. I. Sarwat, "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure," *Sensors*, vol. 23, no. 8, 2023.
- [13] X. Yu, C. Tang, P. Palensky, and A. W. Colombo, "Blockchain: What does it mean to industrial electronics?: Technologies, challenges, and opportunities," *IEEE Industrial Electronics Magazine*, vol. 16, no. 2, pp. 4–14, 2021.
- [14] Y. Djenouri, A. Yazidi, G. Srivastava, and J. C.-W. Lin, "Blockchain: Applications, challenges, and opportunities in consumer electronics," *IEEE Consumer Electronics Magazine*, vol. 13, no. 2, pp. 36–41, 2024.
- [15] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151 054–151 089, 2019.
- [16] P. Chatterjee, D. Das, and D. B. Rawat, "Next generation financial services: Role of blockchain enabled federated learning and metaverse," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. IEEE, 2023, pp. 69–74.
- [17] S. Banabilah, M. Aloiaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications," *Information processing & management*, vol. 59, no. 6, p. 103061, 2022.
- [18] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor, and U. Biswas, "Design of an automated blockchain-enabled vehicle data management system," in *2022 5th International Conference on Signal Processing and Information Security (ICSPIS)*, 2022, pp. 22–25.
- [19] D. Das, S. Banerjee, K. Dasgupta, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain enabled sdn framework for security management in 5g applications," in *Proceedings of the 24th International Conference on Distributed Computing and Networking*, ser. ICDCN '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 414–419. [Online]. Available: <https://doi.org/10.1145/3571306.3571445>
- [20] S. Banerjee, D. Das, P. Chatterjee, B. Blakely, and U. Ghosh, "A blockchain-enabled sustainable safety management framework for connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2023.
- [21] D. Das, S. Banerjee, and U. Biswas, "Cloud-based smart iot architecture and various application domains," *Trends in Cloud-based IoT*, pp. 199–226, 2020.
- [22] U. Ghosh, D. Das, P. Chatterjee, and N. Shillingford, "Federated edge-cloud framework for heart disease risk prediction using blockchain," in *IFIP International Internet of Things Conference*, 2023, pp. 309–329.
- [23] S. Datta and S. Namasudra, "Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4026–4036, 2024.
- [24] H. Kwon, J. Ahn, and J. Ko, "Lightcert: On designing a lighter certificate for resource-limited internet-of-things devices," *Transactions on emerging telecommunications technologies*, vol. 30, no. 10, 2019.
- [25] S. Shukla, S. Thakur, and J. G. Breslin, "Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2021, pp. 261–266.
- [26] L. Gong, D. M. Alghazzawi, and L. Cheng, "Bcot sentry: A blockchain-based identity authentication framework for iot devices," *Information*, vol. 12, no. 5, p. 203, 2021.
- [27] A. K. Al Hwaitat, M. A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, "A new blockchain-based authentication framework for secure iot networks," *Electronics*, vol. 12, no. 17, 2023.
- [28] U. Khalil, O. A. Malik, S. Hussain *et al.*, "A blockchain footprint for authentication of iot-enabled smart devices in smart cities: state-of-the-art advancements, challenges and future research directions," *IEEE Access*, vol. 10, pp. 76 805–76 823, 2022.
- [29] B. Liu, X. Yao, K. Guo, and P. Zhu, "Consortium blockchain based lightweight message authentication and auditing in smart home," *IEEE Access*, 2023.
- [30] A. Wu, Y. Guo, and Y. Guo, "A decentralized lightweight blockchain-based authentication mechanism for internet of vehicles," *Peer-to-Peer Networking and Applications*, vol. 16, no. 3, pp. 1340–1353, 2023.
- [31] H. Yang, Y. Guo, and Y. Guo, "Blockchain-based cloud-fog collaborative smart home authentication scheme," *Computer Networks*, 2024.