Journal of Computing and Communication Vol.4, No.1, PP. 1-18, 2025

Chain of Things (CoT): A Blockchain-based Framework for Securing Internet of Things Applications

Essam H. Houssein*[a,b], Mohamed Reda[a], Yasser M. Wazery[a], Mina Younan[a]

[a] Faculty of Computers and Information, Minia University, Minia, Egypt.
[b] Minia National University, Minia, Egypt.

*Corresponding Author: Essam H. Houssein [***essam.halim@mu.edu.eg***]

ARTICLE DATA

Article history:
Received 24 December 2024
Revised 26 January 2025
Accepted 28 January 2025
Available online

***Keywords*:**
Internet of Things (IoT),
Chain of Things (CoT),
Blockchain, Security,
Decentralization,
Smart Contracts,
Data Integrity

ABSTRACT

The rapid growth of the Internet of Things (IoT) has introduced significant challenges related to security, data integrity, and trustworthiness in distributed systems. Traditional IoT security mechanisms often fail to address vulnerabilities caused by centralized architecture, exposing IoT applications exposed to cyberattacks and unauthorized access. This paper proposes Chain of Things (CoT), a blockchain-based framework designed to enhance the security of IoT applications. By leveraging blockchain's decentralized, immutable, and transparent properties, CoT ensures secure communication, reliable data sharing, and tamper-proof logging of IoT transactions. The proposed framework incorporates smart contracts for automated policy enforcement and scalability, addressing IoT's dynamic and heterogeneous environment. CoT implementation and performance analysis demonstrate its effectiveness in mitigating threats such as data breaches and unauthorized manipulation while maintaining operational efficiency. The proposed framework establishes a robust foundation for securing next-generation IoT systems, promoting trust and resilience in diverse application domains.

1. Introduction

Internet of Things (IoT) is a network of everything that can communicate over the internet to autonomously represent their status [1]. Things are equipped with sensors to convert them into Smart Things (SThs) [2]. Billions of SThs connected to IoT networks generate real-time data to create transformative opportunities across industries [3] [4]. IoT is essential for modern applications, due to characteristics such as automation and interconnectivity, which allow seamless communication among devices, creating collaborative networks [5]. Real-time operation enables instant monitoring and feedback, providing timely alerts and better control [6]. Scalability of IoT allows systems to adapt from small setups to large-scale deployments, accommodating technological growth [7]. Additionally, automation reduces manual intervention by executing tasks based on predefined rules, improving productivity, and minimizing errors [8]. Together, these features establish IoT as a foundational technology for creating smart environments [9].

IoT is transforming various sectors by revolutionizing how services are delivered and managed. For instance, in healthcare, wearable enables doctors to follow and remotely monitor patients, so that they can present accurate medical services to their patients [10]. Smart city initiatives leverage IoT for intelligent traffic management, energy-efficient infrastructure, and automated waste disposal, enhancing urban living standards [11] [12]. In agriculture, IoT-powered smart farming systems enable precision agriculture through real-time crop monitoring, automated irrigation, and environmental sensing, boosting productivity [13]. Industrial IoT (IIoT), a cornerstone of Industry 4.0, benefits from IoT through predictive maintenance, real-time production monitoring, and supply chain optimization [1] [14]. Similarly, home automation systems featuring smart thermostats, lighting controls, and security cameras enhance comfort, convenience, and safety [15].

IoT faces significant security challenges that hinder its widespread adoption [1]. Data breaches are a primary concern, often resulting from insufficient encryption and insecure storage mechanisms that expose sensitive information to cybercriminals [16]. Privacy risks arise from the continuous data collection and

sharing practices inherent in IoT systems, potentially exposing personal and confidential information [17]. Network vulnerabilities exacerbate these issues, as interconnected devices can become entry points for malware or targets of distributed denial-of-service (DDoS) attacks [18]. Furthermore, the limited computational capabilities of SThs restrict the implementation of conventional security protocols, so lightweight effective solutions are required for enabling secure and reliable deployment of IoT applications across various domains [19].

Blockchain is a decentralized and distributed ledger that securely and transparently records transactions across a peer-to-peer network [20]. Its key features such as decentralization, immutability, transparency, and trustworthiness make it an effective solution for enhancing security in digital ecosystems and data-sensitive environments such as IoT [21]. Consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) are used in blockchain to validate transactions and maintain system integrity [22]. Blockchain decentralized architecture eliminates single-point-failure [23] [24], and its immutability ensures data integrity and authenticity [25]. Smart contracts, embedded within the blockchain, automate device authentication and access control, reducing the risks of unauthorized access and identity spoofing [26]. Furthermore, blockchain's cryptographic encryption mechanisms protect sensitive IoT data from unauthorized disclosure while maintaining privacy [27]. Its consensus algorithms facilitate secure and verified data exchanges between devices, preventing fraudulent transactions [28]. By integrating blockchain into IoT architectures, a secure, scalable, and trust-driven ecosystem is created where devices can interact autonomously while ensuring confidentiality, data integrity, and operational reliability [23] [29]. This integration offers a comprehensive security solution that mitigates existing vulnerabilities in IoT applications, making blockchain an ideal technology for enhancing IoT system security [30].

Main contributions of this paper are summarized as follows. First, it provides a detailed analysis of IoT, focusing on its applications and addressing challenges such as security, scalability, and trust issues. Second, it explores blockchain, emphasizing its features (decentralization, immutability, and transparency) and its potential to enhance IoT security. Third, it examines the integration of blockchain with IoT, highlighting solutions for secure data sharing, trusted communication, and access control, while addressing scalability and resource constraints. Fourth, this paper introduces a Chain of Things (CoT), a blockchain-based framework designed to tackle IoT security challenges through secure communication, tamper-proof data logging, and enhanced trust. Finally, it simulates the CoT framework, demonstrating its effectiveness and efficiency in addressing IoT security concerns in real-world scenarios.

The remainder of the paper is organized as follows. Section 2 presents related work followed by Integration between IoT and blockchain technologies in Section 3. Section 4 introduces the proposed CoT framework. Section 5 presents CoT implementation. Section 6 evaluates CoT performance and discusses its limitations proposing future improvements. Finally, Section 7 concludes the paper.

2. Related Work

Traditional identity management systems face significant challenges, due to centralized structures, reliance on trusted third parties, and vulnerabilities to data breaches. IoT and blockchain integration offers a promising solution to enhance security, transparency, and reliability [1]. To address these issues, researchers have developed various frameworks, models, and architectures to address IoT security challenges. Younan et al. [23] introduced Quantum Chain of Things (QCoT) paradigm to highlight importance of integrating such promising technologies in IoT. In [31], a blockchain-based solution was developed to address privacy and scalability challenges in large-scale IoT networks. By combining permissioned blockchain with homomorphic encryption, efficient data management and decentralized verification could be achieved. Security threats could be identified and mitigated in real-time by integrating distributed ledger technology with Ethereum smart contracts [32].

Wazid et al. [33] proposed a framework-based blockchain for AI-enabled IoT drone-aided healthcare systems to address communication vulnerabilities, such as replay and impersonation attacks. Integrating blockchain, secures drone operations and demonstrates improved performance in tasks like medical supply delivery and sample collection. For IIoT, a hybrid blockchain framework has been designed in [34] to secure

multinational operations. It defends against threats like DoS and DDoS attacks while minimizing authentication delays. Simulations show the framework achieves 94% efficiency in enhancing IIoT security and reliability. In smart farming, blockchain has been employed to ensure data security and integrity. For IoT-driven smart cities, a privacy-preserving and secure framework (PPSF) was introduced in [35]. PPSF secures data transmission using two-level blockchain privacy scheme and integrates a Gradient Boosting Anomaly Detector for intrusion detection. Using blockchain-IPFS Fog-Cloud architecture, PPSF addresses centralization, scalability, and privacy challenges, outperforming existing solutions in securing IoT infrastructures.

A framework-based blockchain presented in [36] focuses on enhancing security, transparency, and efficiency for enabling secure Public Emergency Services (PES) in supply chain management. This framework employs edge computing servers and an optimal queue management system to improve processing speed and reduce delays in PES operations. A novel RF-PO algorithm optimizes the supply chain parameters, ensuring efficient resource utilization and scalability. A blockchain-based SDN framework for IoT networks integrates an SDN-Blockchain Classifier to mitigate malicious traffic and enhance transaction trustworthiness. In [37], a framework employs Ethereum with a PoS consensus mechanism is proposed to achieve superior performance in terms of energy efficiency, latency, and network throughput.

Sharma et al. [38] proposed a decentralized framework based on IoT and blockchain to improve privacy, security and efficiency of electronic health records (EHRs), supporting real-time patient monitoring. This framework ensures data integrity, anonymity, and interoperability through secure encryption techniques, surpassing traditional healthcare systems in service quality and data monitoring. Rani et al [39] introduced a decentralized IoT framework integrating SDN and blockchain to enhance scalability, security, and performance. The system achieved a 12.75% improvement in network efficiency by addressing bandwidth, response time, and scalability challenges. Similarly, Satapathy et al. [40] proposed a Hyperledger Fabric-based framework to secure IoT communications, tackling issues like data leakage and unauthorized access while ensuring privacy and data integrity. Veeramakali et al. [41] developed the ODLSB framework, combining blockchain with deep learning for IoT healthcare. This system achieved high diagnostic accuracy (93.68%) using advanced encryption and optimization techniques. Shankar and Maple [42] introduced the SSCI-BDL framework for IoT-enabled smart cities, integrating blockchain and deep learning to achieve 99.5% security and low latency (4.1%), optimizing resource usage in smart city infrastructure. Padma and Ramaiah [43] proposed SecPrivPreserve framework for IoT smart cities, utilizing Hyperledger Fabric, encryption, and OTP mechanisms to enhance data protection and privacy, demonstrating superior computational efficiency. Baker et al. [44] presented a fog-oriented blockchain framework for vehicular transportation systems, leveraging fog computing and 5G technologies to improve responsiveness, latency, and energy efficiency in urban transportation."

Caro et al. [45] proposed a blockchain-based traceability system for the agri-food supply chain, leveraging Ethereum to enhance transparency, immutability, and trustworthiness. The system securely tracks food products from production to consumption, demonstrating its practical application in improving food safety and traceability within supply chain management. Chen et al. [46] introduced AgriTalk, an IoT-based platform designed for precision soil farming, with a focus on turmeric cultivation. By integrating IoT sensors, the platform monitors soil conditions and enables automatic control switching for irrigation and other agricultural tasks. The study highlights its effectiveness in boosting agricultural productivity and resource efficiency. Rehman et al. [47] presented a blockchain-based framework for secure cloud services in IoT applications. Using the Ethereum blockchain, the system ensures data integrity, confidentiality, and decentralized access. However, the study reported significant latency on the public Ethereum network, emphasizing the need for private blockchain solutions to meet the demands of real-time IoT environments.

Table 1 summarizes key blockchain-based frameworks in this section that are tailored for IoT applications. The diversity of approaches underscores the flexibility and potential of blockchain in various IoT domains.

TABLE 1: A Summary for Blockchain-based Frameworks in Related Work

Ref	Year	IoT App	Blockchain	Technologies	Key Contributions
[36]	2024	Supply Chain Management	Private Blockchain	Blockchain, IoT, Edge Computing	• Proposed a framework-based blockchain to improve transparency and security in PES. • Proposed an optimized RF-PO algorithm and employed a queueing model to improve service quality.
[38]	2024	Healthcare	Decentralized Blockchain	Blockchain, IoT	• Proposed a decentralized framework based on IoT and blockchain, ensuring data integrity and interoperability.
[43]	2024	Smart cities	Hyperledger Fabric	Blockchain, IoT, OTP Mechanisms	• Developed the SecPrivPreserve framework for IoT-enabled smart cities, demonstrating improved computational efficiency and data protection.
[42]	2023	Smart cities	Hybrid Blockchain	Blockchain, IoT, Deep Learning	• Introduced the SSCI-BDL framework, combining blockchain and deep learning • Achieve 99.5% security and 4.1% latency.
[32]	2023	Smart agriculture	Public Blockchain	Blockchain, IoT, Smart Contracts	• Presenting a smart farming blockchain framework for attack prevention, real-time notifications, and improved system execution.
[31]	2023	6G IoT networks	Permissioned Blockchain	Blockchain, IoT	• Introduced a trust-aware IoT security approach for 6G-enabled IoT with enhanced algorithms for biometric and industrial data (Homomorphic Encryption).
[48]	2022	IoT security and identity management	Federated Blockchain	Blockchain, Smart Contracts	• Designed a blockchain-based IoT ID management model with smart contracts and a proof-of-concept prototype.
[37]	2022	Energy	Public Blockchain	Blockchain, SDN, PoS, IDS-based Security Tool.	• Developed an SDN-Blockchain Classifier to mitigate malicious traffic. • Utilized Ethereum's PoS mechanism to secure data communication.
[39]	2022	IoT networks	Private Blockchain	Blockchain, SDN, IoT	• Proposed a decentralized framework integrating SDN and blockchain, achieving 12.75% improvement in network performance.
[44]	2022	Smart transportation	Fog-Based Blockchain	Blockchain, IoT, Fog Computing	• Proposed a lightweight blockchain framework for vehicular IoT systems, improving latency, responsiveness, and energy efficiency using fog computing and 5G.
[41]	2021	Healthcare	Private Blockchain	Blockchain, IoT AI, Deep Learning	• Proposed the ODLSB framework, integrating blockchain and deep learning for secure IoT healthcare • Achieve 93.68% diagnostic accuracy.
[35]	2021	Smart cities	Hybrid Blockchain	Blockchain, ML, PCA, IoT	• Proposed 2-level privacy scheme using PoW and PCA. • Designed an anomaly detector. • Integrated blockchain with fog-cloud.
[34]	2021	IIoT and supply chain	Private Blockchain	Blockchain, IoT	• Developed a blockchain architecture to secure records, ensure transparency, and reduce overhead.
[33]	2020	Healthcare	Private Blockchain	Blockchain, AI, IoT	• Proposed a private blockchain framework, designed for attack resilience.
[40]	2019	IoT communication	Hyperledger Fabric	Blockchain, IoT	• Developed a secure communication framework for IoT applications in healthcare and smart cities.
[47]	2019	IoT Cloud Services	Public Blockchain	Blockchain, IoT	• Presented a secure framework for cloud-based IoT services using Ethereum. • Highlighted the need for private blockchain due to high latency in public blockchain networks.
[46]	2019	Precision Farming	Public Blockchain	Blockchain, IoT	• Introduced AgriTalk, an IoT platform for precision soil farming. • Enhanced agricultural productivity and resource efficiency.
[45]	2018	Agri-Food Supply Chain Management	Public Blockchain	Blockchain, IoT	• Proposed a blockchain-based traceability system leveraging Ethereum. • Improved transparency, immutability, and trustworthiness in the agri-food supply chain.

3 The Internet of Things and Blockchain Integration

IoT enhances quality of life by promoting innovation, reducing operational costs, and driving sustainable development [49]. It converts things into SThs and enables real-time sensing, monitoring, processing, and decision-making.

3.1. IoT Challenges and Blockchain Solutions

As mentioned previously, IoT applications penetrate almost all fields improving productivity in variety fields such as healthcare, agriculture, and transportation [11] [50]. On the other hand, IoT faces several challenges [1]. Table 2 summarizes the key challenges of IoT in different applications.

TABLE 2: Main Challenges of the IoT in Variety of Applications

Ref	Year	Challenge	Description
[51]	2023	Regulations	Compliance with varying laws and regulations across regions adds complexity.
[52]	2022	Energy Consumption	IoT devices often face limitations in battery life and energy efficiency.
[53]	2022	Interoperability	Lack of standardization results in difficulty in communication between SThs.
[54]	2021	Scalability	Managing an increasing number of devices and vast data volumes
[55]	2021	Security	Vulnerabilities lead to risks of hacking and data breaches.
[56]	2020	Privacy	sensitive user data raises concerns about unauthorized access and misuse.
[57]	2020	Data Management	Processing, storing, and analyzing large data sets require advanced solutions.
[58]	2020	Latency	Time delays in data transmission can hinder real-time applications.
[59]	2020	Reliability	Ensuring consistent performance and reducing downtime
[60]	2019	Cost	High costs of deploying IoT infrastructure can deter widespread adoption.
[61]	2018	Connectivity	Limited or unreliable network infrastructure affects performance and coverage.

Blockchain is integrated with the IoT to improve data security, transparency, and trust by enabling authorized access, immutable record-keeping, and fraud prevention through smart contracts and decentralized validation [32] [62]. As shown in Figure 1-(a), in the blockchain life cycle, stakeholders first register and verify their credentials using a secure blockchain-based system, ensuring authorized access. After identifying appropriate use cases, smart contracts initiate transactions that are securely recorded on the blockchain. Transactions are grouped into blocks, validated by network nodes to ensure accuracy and prevent fraud, then appended to the blockchain, creating an immutable record. Using such a system, stakeholders can generate reliable insights and maintain continuously updated records.

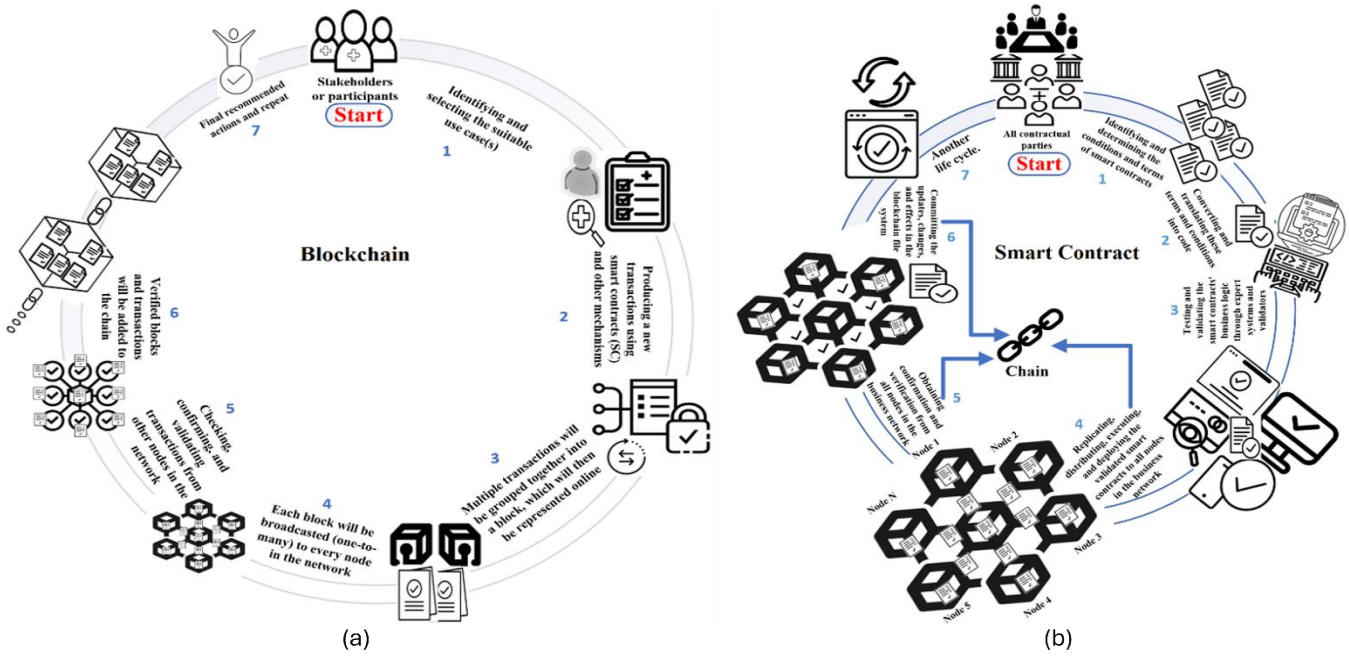

FIGURE 1. Data Flow Diagram: (a) Blockchain - (b) Smart Contract

Figure 1-(b) illustrates the life cycle of smart contracts in IoT applications, where the process begins with the involvement of all relevant parties to define contract terms and conditions. These terms are encoded into executable contracts on the blockchain. Before deployment, the contracts are rigorously tested to ensure they are error-free and accurately implement the intended business logic. Once validated, the contracts are distributed across network nodes, ensuring decentralized enforcement. Each node verifies the contracts through consensus, ensuring their legitimacy. Any modifications or updates to the contracts are permanently recorded on the blockchain, guaranteeing transparency and immutability.

Blockchain addresses key challenges in IoT systems through three main types: public, private, and consortium blockchains, each offering unique benefits. Public blockchains like Ethereum and Bitcoin ensure transparency and decentralization, making them suitable for open-access IoT applications such as environmental monitoring [63]. Private blockchains, including Hyperledger Fabric, provide secure and restricted data management, ideal for sensitive applications like healthcare and smart homes [64]. Consortium blockchains, governed by trusted entities like Corda, balance transparency and controlled participation, benefiting sectors such as industrial automation and energy management [65]. The choice of blockchain depends on specific IoT needs, balancing trade-offs in transparency, privacy, scalability, and control to ensure optimal performance and security. Table 3 summarizes key IoT applications and their recommended blockchain types based on specific needs.

TABLE 3: Blockchain Recommendations for IoT Applications

Ref	Year	IoT App	Blockchain	Brief Description
[66]	2024	Energy and Utilities	Consortium Blockchain	IoT optimizes smart grids. Blockchain supports secure, decentralized energy trading and fault detection.
[67]	2024	Telemedicine	Private Blockchain	IoT facilitates remote care; blockchain ensures secure, auditable interactions between patients and providers.
[68]	2024	Autonomous Vehicles	Consortium Blockchain	IoT supports V2V and V2I communication. Blockchain ensures secure data exchange among connected vehicles.
[69]	2022	Agriculture	Private Blockchain	IoT supports precision farming. Blockchain secures records and ensures traceability in supply chains.
[70]	2021	Smart Cities	Consortium Blockchain	IoT optimizes urban management. Blockchain ensures trusted data sharing and smart contract execution for public services.
[71]	2021	Industrial Automation	Consortium Blockchain	IoT enables predictive maintenance and tracking. Blockchain provides tamper-proof transaction records for industrial systems.
[72]	2021	Home Automation	Private Blockchain	IoT enhances energy efficiency. Blockchain provides secure data sharing and user control.
[62]	2020	Healthcare	Private Blockchain	IoT enables real-time health monitoring. Blockchain ensures secure, immutable health records with controlled access.
[73]	2020	Transportation	Consortium Blockchain	IoT optimizes fleet tracking. Blockchain ensures traceability and reliable data for logistics and supply chains.
[74]	2020	Retail	Private Blockchain	IoT improves inventory and customer experience. Blockchain secures transactions and inventory records.

3.2. Blockchain-IoT Integration Challenges

However, Blockchain-IoT integration enhances security, transparency and data integrity, it introduces significant energy consumption challenges, particularly for SThs with restricted resources (e.g., battery life) [23]. Energy optimization for SThs focuses on reducing energy consumption while maintaining security and performance. Traditional cryptographic algorithms are unsuitable for IoT devices capabilities, as they require high computational resources [75]. Similarly, traditional blockchain protocols like Proof of Work (PoW) require high energy, which is incompatible with the constraints of most IoT devices [76] [77]. Many IoT devices lack the energy and processing capacity to participate directly in energy-intensive consensus processes [78]. Additionally, frequent and continuous data exchanges between IoT devices and blockchain nodes increase energy consumption, as devices often maintain prolonged connectivity for real-time data transmission [24].

To overcome these limitations, lightweight cryptographic techniques have been developed, aiming to simplify encryption and decryption processes, use smaller key sizes while maintaining security, and

optimize memory usage for devices with limited storage [79]. Lightweight block ciphers like AES-128, stream ciphers like Grain, and elliptic curve cryptography, enable secure communication with reduced overhead [80]. PoS and Delegated Proof of Stake (DPoS) can significantly lower energy demands [81]. Off-chain solutions like state channels and sidechains further minimize on-chain transaction energy use [82]. Integrating edge computing allows edge nodes to process and aggregate data locally, reducing the computational and communication burden on IoT devices [83]. Adaptive techniques such as data compression and aggregation optimize data transmission, conserving energy during communication [84]. Additionally, lightweight smart contracts optimized for efficient execution can reduce energy use in interactions between IoT devices and blockchain networks [85]. By adopting these strategies, blockchain-IoT integration can become more sustainable and practical, supporting its application across diverse domains while ensuring efficiency and reliability.

To sum up, implementing lightweight cryptographic techniques and energy-efficient consensus mechanisms enable IoT systems to balance energy efficiency and robust security. This is particularly beneficial for sustainable operation in constrained environments, such as remote monitoring systems, smart agriculture, and healthcare applications.

4. The Proposed Chain of Things (CoT) Framework

The proposed Chain of Things (CoT) framework represents an advanced model for securing IoT applications by integrating blockchain to ensure secure data storage, transfer, and management. This framework leverages IoT sensors to generate real-time data across various domains such as healthcare, smart cities, agriculture, and logistics. Blockchain plays a central role in CoT to store, validate, and secure IoT data through decentralized systems and smart contracts, ensuring transparency, tamper resistance, and trustworthiness. Also, CoT implements authentication and encryption mechanisms to enhance data integrity and confidentiality. As shown in Figure 2, CoT integrates four layers: sensing, networking, blockchain, and application layer to create a robust and secure IoT applications.

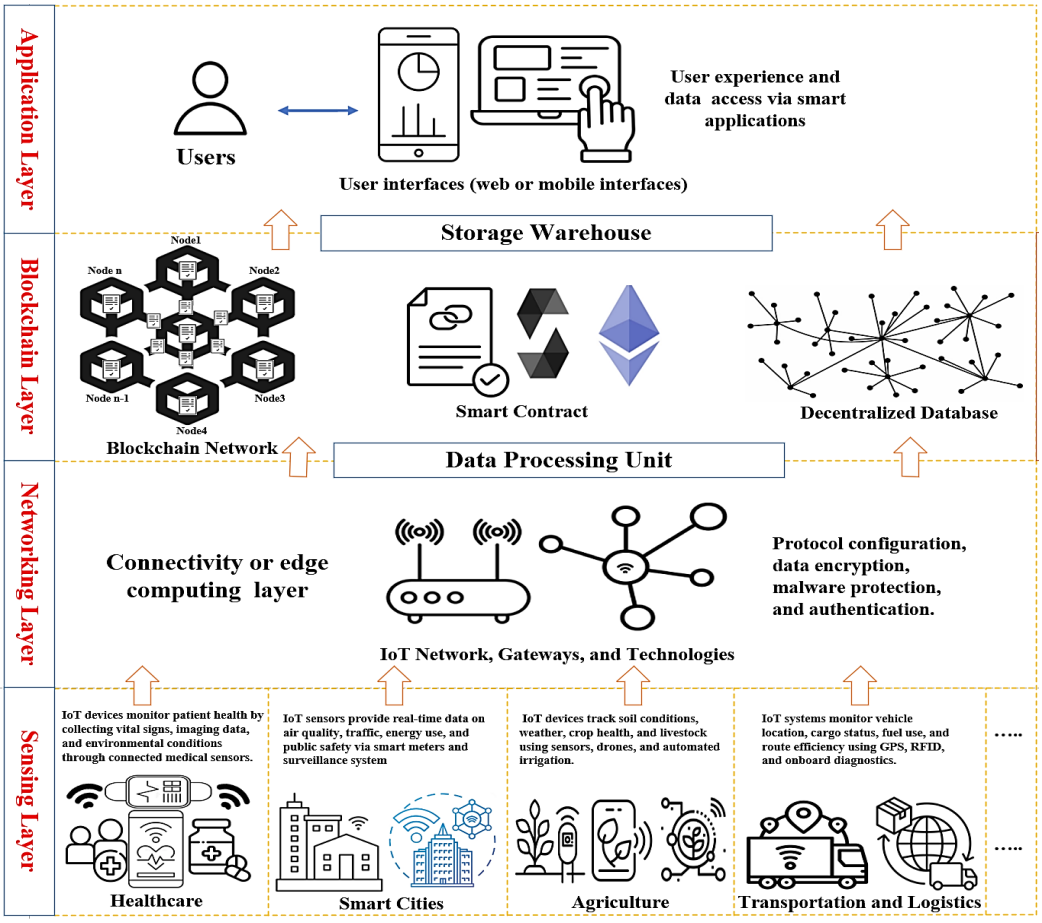

FIGURE 2. The Proposed CoT Framework

A brief overview of each layer is presented in the following points:

1. **The Sensing Layer:** the lower layer, where SThs gather real-time data, for example, sensing patient vital signs in healthcare application. This layer acts as the data generation hub, collecting environmental and operational data for further processing.
2. **The Network Layer:** IoT networks, edge computing, and gateways are used to route the collected data to subsequent layers. At this stage, protocols, data encryption, and security mechanisms such as authentication are configured to safeguard data integrity during transmission. This layer connects the sensing and blockchain layers, enabling the flow of IoT-generated data in real-time.
3. **The Blockchain Layer:** provides the security backbone of the CoT framework. This layer is known as cloud layer in IoT architecture. It stores IoT data securely using decentralized blockchain networks and smart contracts. Data blocks are cryptographically validated, ensuring immutability and transparency. Smart contracts automate processes, such as data access and validation, while decentralized databases prevent single points of failure. This layer ensures that all IoT data is trustworthy and tamper-proof.
4. **The Application Layer:** is user-centric, providing access to IoT data and interfaces through web or mobile applications. Users, such as patients, farmers, stakeholders, administrators, or others based on IoT applications, can retrieve, monitor, and analyze IoT data based on specific needs. This layer enhances user experience by enabling secure access to alerts, reports, and real-time information generated by IoT devices.

Simplicity of CoT architecture and seamless interaction between its layers facilitate seamless data flow and enable user-friendly access to IoT data. As shown in Figure 3, in the first, SThs (e.g., wearable in healthcare) join sensing layer. Collected sensory data is sent through the network layer to be routed to the blockchain layer. In the next step, the blockchain layer securely stores critical IoT data in balance with cloud layer. This layer ensures balance in data storage, processing overheads, and data security. Finally, the application layer grants stakeholders, such as patients or other stakeholders, access to the data, enabling retrieval, insights analysis, and real-time alerts. Implementing IoT-based blockchain applications following such workflow could achieve data security, integrity, reliability and efficiency.

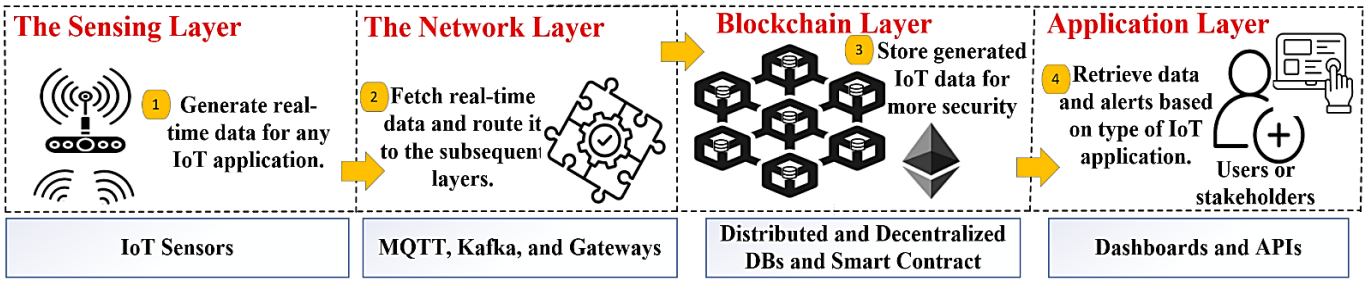

FIGURE 3. CoT: Layers, and Data Flow

5. CoT Implementation

Scenario (**Agriculture Sector – Private Network**): Assume that a 100-acre farm is equipped with IoT sensors that continuously monitor key parameters such as soil moisture, temperature, and humidity. The farm management system leverages real-time data to automate irrigation schedules, optimizing water usage and crop health. The collected sensory data is securely transmitted to a private blockchain network to maintain data integrity and availability. Farmers can then access real-time farm conditions, receive irrigation alerts, and analyze crop health trends through a mobile application, enabling informed decision-making and efficient farm management.

This scenario is implemented and tested on a laptop with the following specification: Intel® Core™ i7-2640M processor, 8 GB of RAM, a 180 GB SSD, and Windows 10 Pro (64-bit). Figure 4 highlights the primary tools and technologies utilized in this experiment, which are detailed in the subsections below.

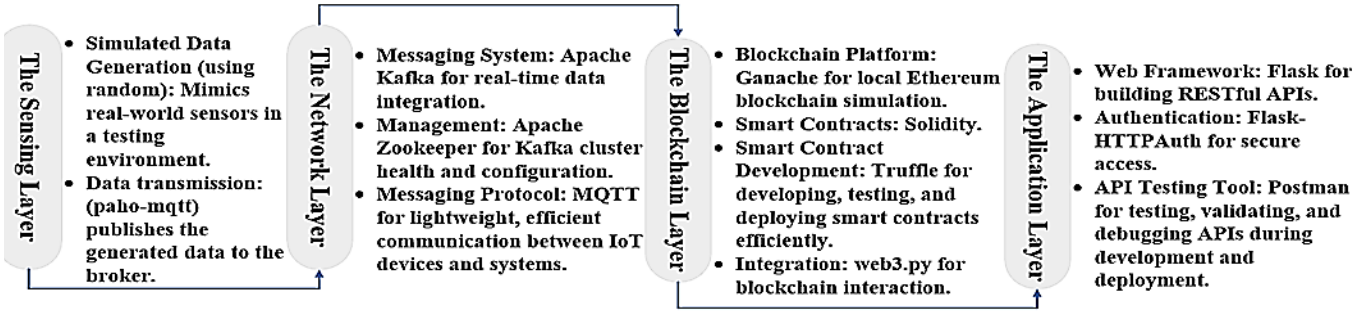

FIGURE 4. Technologies and tools implemented at each CoT layer

1. **The Sensing Layer:** includes soil moisture, temperature, and humidity sensors, simulate real-time environmental and crop conditions. Simulated data generation is handled using Python, utilizing libraries like random to produce realistic sensor readings. Algorithm 1 is used to simulate and generate agriculture data. The generated IoT data has the following format.

```
Publishing: {"soil_moisture": 63, "temperature": 19, "humidity": 70, "timestamp":
1734469585.3593047}
```

Algorithm 1 Sensing Layer: Data Generation

```
Input: MQTT broker, and topic.
Begin
Initialize MQTT client and connect to MQTT broker.
while true do
    Generate agriculture_data.
    if !Valid(agriculture_data) then
        Discard agriculture_data and log error.
    else
        Publish agriculture_data to MQTT topic.
    end if
    Wait for 1 second.
end while
End
```

2. **The Network Layer:** sensory data is transmitted via the MQTT protocol to a Kafka streaming platform. This ensures efficient, low-latency data transfer to downstream systems while maintaining reliable connectivity. Algorithm 2 is used to simulate and generate agriculture data. The format of the data received and published to the previously created Kafka topic "agriculture-data".

```
Received and published data to Kafka topic: agriculture-data: {'sensor_id':
'Sensor1', 'data_type': 'Agriculture', 'data_value': '{"soil_moisture": 63,
"temperature": 19, "humidity": 70, "timestamp": 1734469585.3593047}', 'timestamp':
```

Algorithm 2 Network Layer: MQTT to Kafka Bridge

```
Input: MQTT topic, Kafka broker, Kafka topic.
Begin
Initialize Kafka producer and MQTT client.
Subscribe to MQTT topic.
while true do
    if MQTT message received then
        Decode and validate MQTT message.
        Format message as Kafka payload.
        Publish payload to Kafka topic.
    end if
end while
End
```

3. **The Blockchain Layer:** The collected data is stored securely on a private blockchain. This layer ensures data integrity, protects against tampering, and provides controlled access to authorized parties. The blockchain is implemented using Truffle and Ganache, with smart contracts developed in Solidity to manage data storage and access permissions. Algorithm 3 ensures secure agricultural data storage on a blockchain by validating transactions, recording details, and retrying failed operations to maintain data integrity. Algorithm 4 utilizes a smart contract to manage agricultural data efficiently, enabling structured data storage, retrieval, and transparent updates through event notifications. Figure 5 shows Ganache execution output. The list box below displays the format of data stored in the blockchain.

```
Stored in blockchain:
0x2be11302b845d7f92673d4907b5b138a3bcf6e082d5c57dd325fe327a3eed855
```

Algorithm 3 Blockchain Layer: Data Storage

Input: IoT data from Kafka.
Begin
Initialize smart contract and connect to blockchain.
Retrieve data from Kafka topic.
while data available **do**
  if `!Valid(data)` **then**
    Discard data and log error.
  else
    Call `addAgricultureRecord()` in smart contract.
  end if
end while
End

Algorithm 4 Smart Contract: Agriculture Data Management

Input: Sensor ID, data type, data value.
Begin
function ADDAGRICULTURERECORD
  Validate inputs.
  Create new agriculture record.
  Emit `NewAgricultureRecord` event.
  Increment record count.
end function
function GETAGRICULTURERECORD(RECORDID)
  Validate `recordId`.
  Return agriculture record details.
end function
End

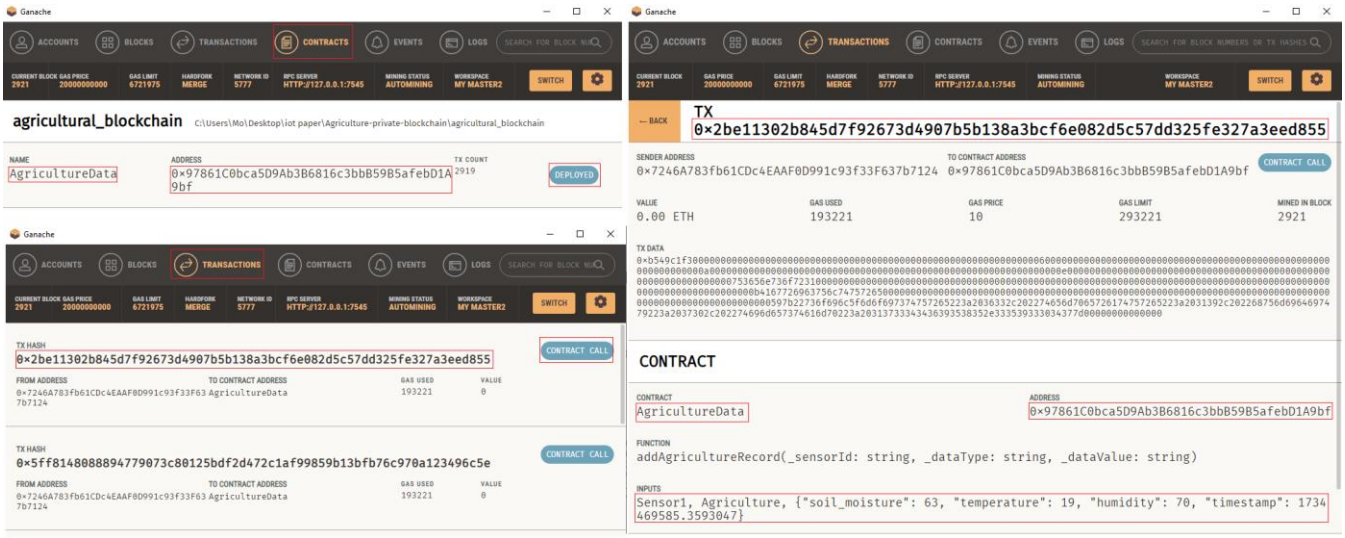

FIGURE 5. Ganache Execution: Implementation of agriculture data storage and generation of result outputs.

4. **The Application Layer:** A Flask-based web dashboard offers farmers and stakeholders real-time sensor data visualization, access to historical blockchain records, and alerts for critical environmental changes. The application is tested using Postman (Figure 6).

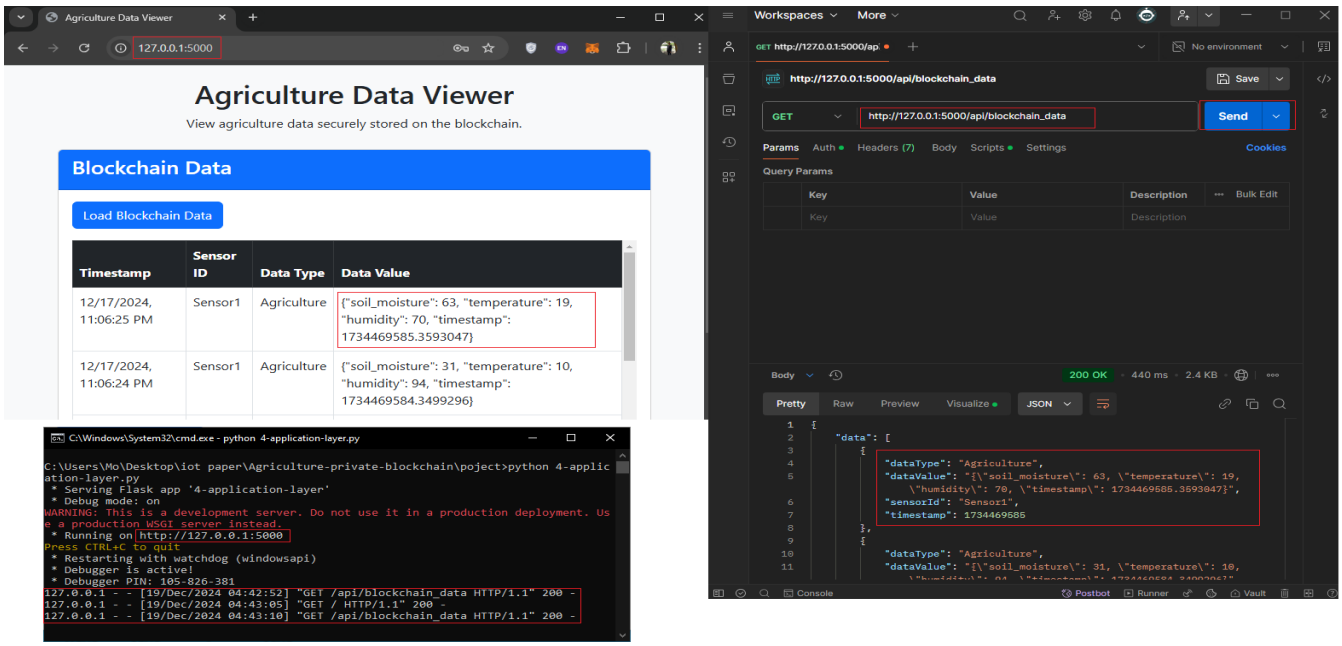

FIGURE 6. API Integration and User Interface: Execution and result validation using Postman and Flask.

As a result, this layered architecture could ensure continuous data generation, secure storage, and actionable insights, enabling agricultural management to be effective. CoT is implemented in this section in agriculture; however, it could be expanded to be implemented in numerous fields like healthcare and industrial automation. In healthcare, CoT could improve diagnostic accuracy by analyzing patient symptoms step-by-step and assist in personalized treatment planning by considering factors like genetics and medication compatibility. In industrial automation, it could optimize predictive maintenance by evaluating sensor data to foresee equipment failures and support adaptive manufacturing by adjusting production parameters in real time.

6. CoT Performance Analysis and Evaluation

The proposed CoT framework is evaluated using 2000 messages, which are transmitted at a rate of one message per second (Message/Second). The evaluation analyzes CoT performance across its layers based on the following equation:

Throughput Eq (1): The rate at which messages are processed over time.

$$\text{Throughput} = \frac{\text{Total Messages}}{\text{Elapsed Time (Seconds)}} \quad \text{Eq (1)}$$

Latency Eq (2): The average time required to process a single message.

$$\text{Average Latency} = \frac{\sum_{i=1}^{n} \text{Latency}_i}{\text{Total Messages}} \quad \text{Eq (2)}$$

6.1 CoT Performance Analysis

1. **The Sensing Layer:** This layer captures and processes real-time data from IoT devices. With an average latency of 0.0029 seconds, the system demonstrates a fast response time for generating real-time data. However, the overall throughput of 0.99 messages/second suggests that data collection is relatively slow, indicating possible bottlenecks in message generation or system workload limits.

--- Overall Metrics ---
Total Messages Processed: 2000
Total Time Elapsed: 2023.59 seconds
Overall Throughput: 0.99 messages/second
Average Latency (Real-Time Data Generation): 0.0029 seconds

2. **The Network Layer:** This layer manages the data transfer from the sensing layer using protocols like MQTT and Kafka. An average latency of 0.0028 seconds reflects an efficient transfer mechanism with minimal delays. However, the overall throughput of 0.98 messages/second mirrors the sensing layer's performance, suggesting that data transfer keeps pace with data generation but doesn't exceed it, ensuring real-time communication consistency.

--- Overall Metrics ---
Total Messages Processed: 2000
Total Time Elapsed: 2034.52 seconds
Overall Throughput: 0.98 messages/second
Average Latency (MQTT to Kafka): 0.0028 seconds

3. **The Blockchain Layer**: This layer processes transactions with a significantly higher throughput of 4.14 transactions/second, indicating that it can handle transactions faster than data is generated and transmitted from the previous layers. However, the average latency of 0.2418 seconds reveals that transaction confirmation is slower compared to the sensing and network layers due to the computational overhead of blockchain operations like transaction validation and block creation.

--- Overall Metrics ---
Total Transactions Processed: 2000
Total Time Elapsed: 2027.17 seconds
Overall Throughput: 4.14 transactions/second
Average Latency: 0.2418 seconds

4. For the **Application Layer**, the time taken to fetch agriculture data from the blockchain is a critical metric for application performance. The first-time fetch took 0.52 seconds, reflecting initialization overhead, while the average fetching time across 100 queries was 0.414 seconds, indicating consistent and efficient performance. These metrics highlight the application layer's ability to retrieve the last ten records of agriculture data from the blockchain in near-real-time, ensuring responsiveness and reliability. This level of performance is suitable for applications requiring secure and timely data access, such as precision agriculture and IoT-based farming systems, with opportunities for further optimization to reduce initialization delays.

These metrics reveal a well-optimized system where the blockchain layer outperforms the sensing and network layers in throughput. However, reducing the sensing and network layers' throughput bottlenecks could enhance end-to-end system performance. Additionally, optimizing blockchain transaction latency through advanced blockchain scaling solutions like sharding or layer-2 protocols could further improve the system's scalability. Compared to most relevant related work, none of them provide a fully integrated, end-to-end solution equivalent to CoT. **Table 4** highlights a comparison of CoT's latency and throughput performance with these frameworks.

TABLE 4: Performance Analysis for Most Relevant Blockchain-based Frameworks Compared to CoT

Framework	Latency	Throughput	Key Features
AgriBlockIoT [45]	16.55	Not reported	Ethereum-based traceability in agri-food.
AgriTalk [46]	<0.2	Not reported	IoT platform for precision soil farming.
Cloud based Blockchain [47]	272	Not reported	Cloud-based IoT service with Ethereum.
Drone-Aided Healthcare [33]	0.355	2.82	Framework simulation for adding blocks and transactions into the blockchain
CoT: (the proposed framework)	0.2418	4.14	Scalable IoT security framework using private blockchain (Ethereum)

Caro et al. [45] introduced a blockchain-based traceability framework for agri-food supply chains using Ethereum, reporting a transaction latency of 16.55 seconds, which is significantly higher than CoT by 16.3082 seconds. This improvement is due to CoT optimized private blockchain configuration and efficient consensus mechanism. Similarly, Chen et al**.** [46] developed AgriTalk, an IoT platform for precision farming, achieving lower message delays of less than 0.2 seconds. However, while AgriTalk excels in agricultural use cases, CoT provides a broader and more adaptable solution for diverse IoT environments. Rehman et al. [47] used the public Ethereum network for a cloud-based IoT service framework, reporting a transaction latency of 272 seconds. CoT outperforms this framework, achieving much faster latency thanks to its private blockchain design. Likewise, Wazid et al. [33] proposed a private blockchain framework for AI-enabled IoT-based healthcare services, achieving a block latency of 0.307 seconds, a transaction latency of 0.355 seconds, and a throughput of 2.82 transactions per second.

6.2. CoT Limitations and Proposed Solutions for Future Enhancement

While CoT demonstrates significant potential in addressing IoT security challenges, it has significant limitations as well that need to be acknowledged and addressed in future work. The limitations of CoT framework are summarized as follows:

- **Scalability Challenges:** While the CoT framework demonstrates efficiency in small- to medium-scale IoT networks, its scalability in large-scale, real-time environments remains constrained by the computational overhead of blockchain operations, such as consensus mechanisms and transaction validation.
- **Energy Consumption:** The integration of blockchain may result in high energy consumption, limiting its feasibility for resource-constrained IoT devices.
- **Regulatory and Ethical Considerations:** Implementing blockchain in critical applications (e.g., healthcare) may raise concerns regarding data privacy compliance (e.g., GDPR) and ethical implications of decentralized data sharing.
- **Latency in Data Processing:** Although blockchain provides secure data storage, the added latency during transaction validation and block creation can hinder real-time applications where immediate responses are critical.

Concerning latency, the performance analysis presented early shows that the blockchain layer has higher latency (0.2418 seconds on average) compared to the sensing and network layers, primarily due to the computational overhead of transaction validation and block creation. To address this, the following optimizations are proposed:

- **Advanced Consensus Mechanisms:** Transitioning from PoW [86] to efficient mechanisms like PoS [87] and DPoS [88] to reduce computational complexity and enhance transaction throughput.
- **Implementing Blockchain Scaling Techniques: (a) Sharding** [89] to handle a subset of transactions independently, to reduce computational burden and increase transaction capacity [90] [91]. (b) **Layer-2 Protocols** [92]**:** Processing transactions off-chain using techniques like state channels or rollups, with only summaries recorded on the main chain, significantly lowering latency and improving processing speed [93] [94].
- **Efficient Smart Contract Optimization** [95]**:** Streamlining smart contract code to minimize unnecessary computations and optimize storage access, reducing execution time and improving performance.
- **Asynchronous Transaction Processing:** Using asynchronous techniques to process transactions in parallel and optimize operation order to alleviate bottlenecks during periods of high transaction volume [96].

Integrating AI-based anomaly detection will enhance the real-time threat identification and mitigation capabilities of the CoT framework. AI models will analyze real-time data from the sensing layer to detect patterns and anomalies, such as unauthorized access or device malfunctions. In the agricultural scenario,

AI-based anomaly detection improves security and operational resilience by continuously monitoring sensor data streams. Machine learning algorithms can identify unusual patterns, like abnormal soil moisture or temperature spikes, which may signal sensor tampering, hardware failures, or cyberattacks targeting IoT devices or the blockchain layer.

7. Conclusion

Chain of Things (CoT) framework is proposed to integrate blockchain with IoT to enhance the security, trust, and reliability of IoT applications. By leveraging blockchain's decentralized, immutable, and transparent properties, CoT addresses the vulnerabilities associated with traditional centralized IoT systems, such as unauthorized access, data tampering, and single points of failure. The integration of smart contracts enables automated policy enforcement and scalability, ensuring secure communication and tamper-proof logging within dynamic IoT environments. Experimental results and performance evaluations of CoT demonstrate its effectiveness in mitigating security threats, while maintaining operational efficiency. As a result, CoT architecture could establish a robust foundation for securing next-generation IoT systems. In the future work, CoT will be extended to address scalability challenges in large-scale IoT networks by exploring advanced blockchain solutions, such as sharding and layer-2 protocols. Also, we plan to integrate AI-driven anomaly detection mechanisms to enhance real-time threat identification and response. In addition, further investigations will focus on optimizing energy consumption and resource management for IoT devices operating in constrained environments. Finally, the proposed framework will be tested and realized on a real application to validate its adaptability and performance.

References

[1] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial internet of things: A comprehensive review," *Measurement, vol. 151, p. 107198, 2020..*

[2] O. Vermesan, A. Bröring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, C. Gallicchio, A. Micheli, M. Dragone, A. Saffiotti and others, "Internet of robotic things–converging sensing/actuating, hyperconnectivity, artificial intelligence and IoT platforms," in *Cognitive hyperconnected digital transformation*, River Publishers, 2022, p. 97–155.

[3] M. Younan, M. Elhoseny, A. E.-m. A. Ali, and E. H. Houssein, "Data reduction model for balancing indexing and securing resources in the internet of things applications," *IEEE Internet of Things Journal, 2020. https://doi.org/10.1109/JIOT.2020.3035248.*

[4] R. S. Jha and P. R. Sahoo, "Internet of things (IoT)–enabler for connecting world," in *ICT for competitive strategies*, CRC Press, 2020, p. 1–7.

[5] A. Uzoka, E. Cadet and P. U. Ojukwu, "The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications," *Comprehensive Research and Reviews in Science and Technology,* vol. 2, p. 055–073, 2024.

[6] W. Villegas-Ch, J. García-Ortiz and S. Sánchez-Viteri, "Towards Intelligent Monitoring in IoT: AI Applications for Real-Time Analysis and Prediction," *IEEE Access,* 2024.

[7] P. Deivendran, S. Ilaiyaraja, S. Selvakanmani and K. S. Raghuram, "Scalability and security requirements for the Internet of Things architecture," in *Artificial Intelligence for Internet of Things*, CRC Press, 2022, p. 109–147.

[8] H. Chegini, R. K. Naha, A. Mahanti and P. Thulasiraman, "Process automation in an IoT–fog–cloud ecosystem: A survey and taxonomy," *IoT,* vol. 2, p. 92–118, 2021.

[9] M. Younan, S. Khattab, and R. Bahgat, "From the wireless sensor networks (wsns) to the web of things (wot): an overview," *J. Intell. Syst. Internet Things, vol. 4, no. 2, pp. 56–68, 2021..*

[10] C. Li, J. Wang, S. Wang and Y. Zhang, "A review of IoT applications in healthcare," *Neurocomputing,* vol. 565, p. 127017, 2024.

[11] E.H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in Smart Cities: Comprehensive Review, Open Issues and Challenges," *IEEE INTERNET OF THINGS JOURNAL,* pp. 1-12, 2024.

[12] M. E. E. Alahi, A. Sukkuea, F. W. Tina, A. Nag, W. Kurdthongmee, K. Suwannarat and S. C. Mukhopadhyay, "Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends," *Sensors,* vol. 23, p. 5206, 2023.

[13] C. Liang and T. Shah, "IoT in agriculture: The future of precision monitoring and data-driven farming," *Eigenpub Review of Science and Technology,* vol. 7, p. 85–104, 2023.

[14] G. Kiradoo, "The prominence of IoT in enhancing business success in the context of industry 4.0," *Recent Progress in Science and Technology,* vol. 6, p. 188–204, 2023.

[15] C. Stolojescu-Crisan, C. Crisan and B.-P. Butunoi, "An IoT-based smart home automation system," *Sensors,* vol. 21, p. 3784, 2021.

[16] A. N. Lone, S. Mustajab and M. Alam, "A comprehensive study on cybersecurity challenges and opportunities in the IoT world," *Security and Privacy,* vol. 6, p. e318, 2023.

[17] V. Demertzi, S. Demertzis and K. Demertzis, "An Overview of Privacy Dimensions on the Industrial Internet of Things (IIoT)," *Algorithms,* vol. 16, p. 378, 2023.

[18] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Computers & Security,* vol. 127, p. 103096, 2023.

[19] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh and H. Arshad, "A review on the security of the internet of things: Challenges and solutions," *Wireless Personal Communications,* vol. 119, p. 2603–2637, 2021.

[20] S. Dong, K. Abbas, M. Li and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Computer Science,* vol. 9, p. e1705, 2023.

[21] V. Ali, A. A. Norman and S. R. B. Azzuhri, "Characteristics of blockchain and its relationship with trust," *Ieee Access,* vol. 11, p. 15364–15374, 2023.

[22] D. P. Oyinloye, J. S. Teh, N. Jamil and M. Alawida, "Blockchain consensus: An overview of alternative protocols," *Symmetry,* vol. 13, p. 1363, 2021.

[23] M. Younan, M. Elhoseny, A. A. Ali, and E. H. Houssein, "Quantum chain of things (qcot): A new paradigm for integrating quantum computing, blockchain, and internet of things," *in 2021 17th International Computer Engineering Conference (ICENCO). IEEE, 2021, pp. 101–106.*

[24] A. Al Sadawi, M. S. Hassan and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEe Access,* vol. 9, p. 54478–54497, 2021.

[25] G. R. Mounika and N. V. Lakshmi, "Blockchain Applications in Cybersecurity: Strengthening Data Integrity and Authentication," *Library Progress International,* vol. 44, p. 16624–16633, 2024.

[26] M. R. Hasan, A. Alazab, S. B. Joy, M. N. Uddin, M. A. Uddin, A. Khraisat, I. Gondal, W. F. Urmi and M. A. Talukder, "Smart contract-based access control framework for internet of things devices," *Computers,* vol. 12, p. 240, 2023.

[27] M. Qi, Z. Wang, Q.-L. Han, J. Zhang, S. Chen and Y. Xiang, "Privacy protection for blockchain-based healthcare IoT systems: A survey," *IEEE/CAA Journal of Automatica Sinica,* 2022.

[28] A. R. Kairaldeen, N. F. Abdullah, A. Abu-Samah and R. Nordin, "Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms," *Wireless Communications and Mobile Computing,* vol. 2021, p. 4401809, 2021.

[29] A. P. Delladetsimas, S. Papangelou, E. Iosif and G. Giaglis, "Integrating Blockchains with the IoT: A Review of Architectures and Marine Use Cases," *Computers,* vol. 13, p. 329, 2024.

[30] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah and others, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain," *Internet of Things,* vol. 23, p. 100888, 2023.

[31] 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, p. 3618, 2023.

[32] A. A. Aliyu and J. Liu, "Blockchain-Based Smart Farm Security Framework for the Internet of Things," *Sensors,* vol. 23, p. 7992, 2023.

[33] M. Wazid, B. Bera, A. Mitra, A. K. Das and R. Ali, "Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services," in *Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond*, 2020.

[34] G. Rathee, F. Ahmad, R. Sandhu, C. A. Kerrache and M. A. Azad, "On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things," *Information Processing & Management,* vol. 58, p. 102526, 2021.

[35] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu and N. N. Xiong, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Transactions on Network Science and Engineering,* vol. 8, p. 2326–2341, 2021.

[36] A. Y. B. Ahmad, N. Verma, N. Sarhan, E. M. Awwad, A. Arora and V. O. Nyangaresi, "An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model," *IEEE Access,* 2024.

[37] M. A. Al Ghamdi, "An optimized and secure energy-efficient blockchain-based framework in IoT," *IEEE Access,* vol. 10, p. 133682–133697, 2022.

[38] A. Sharma, S. Kaur and M. Singh, "A secure blockchain framework for the internet of medical things," *Transactions on Emerging Telecommunications Technologies,* vol. 35, p. e4917, 2024.

[39] S. Rani, H. Babbar, G. Srivastava, T. R. Gadekallu and G. Dhiman, "Security framework for internet-of-things-based software-defined networks using blockchain," *IEEE Internet of Things Journal,* vol. 10, p. 6074–6081, 2022.

[40] U. Satapathy, B. K. Mohanta, S. S. Panda, S. Sobhanayak and D. Jena, "A secure framework for communication in internet of things application using hyperledger based blockchain," in *2019 10th international conference on computing, communication and networking technologies (ICCCNT)*, 2019.

[41] T. Veeramakali, R. Siva, B. Sivakumar, P. C. Senthil Mahesh and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing,* vol. 77, p. 9576–9596, 2021.

[42] A. Shankar and C. Maple, "Securing the Internet of Things-enabled smart city infrastructure using a hybrid framework," *Computer Communications,* vol. 205, p. 127–135, 2023.

[43] A. Padma and M. Ramaiah, "Blockchain based an efficient and secure privacy preserved framework for smart cities," *IEEE Access,* 2024.

[44] T. Baker, M. Asim, H. Samwini, N. Shamim, M. M. Alani and R. Buyya, "A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems," *Computer Networks,* vol. 203, p. 108676, 2022.

[45] M. P. Caro, M. S. Ali, M. Vecchio and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," in *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, 2018.

[46] W.-L. Chen, Y.-B. Lin, Y.-W. Lin, R. Chen, J.-K. Liao, F.-L. Ng, Y.-Y. Chan, Y.-C. Liu, C.-C. Wang, C.-H. Chiu and others, "AgriTalk: IoT for precision soil farming of turmeric cultivation," *IEEE Internet of Things Journal,* vol. 6, p. 5209–5223, 2019.

[47] M. Rehman, N. Javaid, M. Awais, M. Imran and N. Naseer, "Cloud based secure service providing for IoTs using blockchain," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019.

[48] S. Venkatraman and S. Parvin, "Developing an IoT identity management system using blockchain," *Systems,* vol. 10, p. 39, 2022.

[49] J. O. Gidiagba, N. K. Nwaobia, P. W. Biu, C. A. Ezeigweneme and A. A. Umoh, "Review on the evolution and impact of iot-driven predictive maintenance: assessing advancements, their role in enhancing system longevity, and sustainable operations in both mechanical and electrical realms," *Computer Science & IT Research Journal,* vol. 5, p. 166–189, 2024.

[50] A. R. Anarbayevich, "EXPLORING THE PRACTICAL APPLICATIONS OF IoT TECHNOLOGIES," *International Journal of Advance Scientific Research,* vol. 4, p. 88–100, 2024.

[51] J. Li, A. Maiti and J. Fei, "Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things," *Future Internet,* vol. 15, p. 256, 2023.

[52] R. Mishra, B. K. R. Naik, R. D. Raut and M. Kumar, "Internet of Things (IoT) adoption challenges in renewable energy: A case study from a developing economy," *Journal of Cleaner Production,* vol. 371, p. 133595, 2022.

[53] S. S. Albouq, A. A. Abi Sen, N. Almashf, M. Yamin, A. Alshanqiti and N. M. Bahbouh, "A survey of interoperability challenges and solutions for dealing with them in IoT environment," *IEEE Access,* vol. 10, p. 36416–36428, 2022.

[54] A. Alrehaili, A. Namoun and A. Tufail, "A comparative analysis of scalability issues within blockchain-based solutions in the internet of things," *International Journal of Advanced Computer Science and Applications,* vol. 12, 2021.

[55] M. Azrour, J. Mabrouki, A. Guezzaz and A. Kanwal, "Internet of things security: challenges and key issues," *Security and Communication Networks,* vol. 2021, p. 5533843, 2021.

[56] N. Hasan, A. Chamoli and M. Alam, "Privacy challenges and their solutions in IoT," *Internet of Things (IoT) Concepts and Applications,* p. 219–231, 2020.

[57] B. Diène, O. Diallo, J. J. P. C. Rodrigues, E. H. M. Ndoye and C. Teodorov, "Data management mechanisms for IoT: Architecture, challenges and solutions," in *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, 2020.

[58] M. T. A. Bakar and A. A. Jamal, "Latency issues in internet of things: A review of literature and solution," *International Journal,* vol. 9, 2020.

[59] L. Xing, "Reliability in Internet of Things: Current status and future perspectives," *IEEE Internet of Things Journal,* vol. 7, p. 6704–6721, 2020.

[60] L. F. Osako, M. O. Matsubayashi, S. M. Takey, P. A. Cauchick-Miguel and E. Zancul, "Cost evaluation challenges for internet of things (iot) based product/service-systems (pss)," *Procedia CIRP,* vol. 84, p. 302–306, 2019.

[61] I. Petruţ and M. Oteşteanu, "The IoT connectivity challenges," in *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2018.

[62] K. Anitha Kumari, R. Padmashani, R. Varsha and V. Upadhayay, "Securing Internet of Medical Things (IoMT) using private blockchain network," *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm,* p. 305–326, 2020.

[63] V. Dedeoglu, R. Jurdak, A. Dorri, R. C. Lunardi, R. A. Michelin, A. F. Zorzo and S. S. Kanhere, "Blockchain technologies for iot," *Advanced applications of blockchain technology,* p. 55–89, 2020.

[64] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM computing surveys (CSUR),* vol. 52, p. 1–34, 2019.

[65] P. Koukaras, K. D. Afentoulis, P. A. Gkaidatzis, A. Mystakidis, D. Ioannidis, S. I. Vagropoulos and C. Tjortjis, "Integrating Blockchain in Smart Grids for Enhanced Demand Response: Challenges, Strategies, and Future Directions," *Energies,* vol. 17, p. 1007, 2024.

[66] S. Khalid, I. Ahmad and H. Lei, "A Consortium Blockchain-Based Approach for Energy Sharing in Distribution Systems," *IEEE Transactions on Network and Service Management,* 2024.

[67] C. V. B. Murthy and M. L. Shri, "Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine," *IEEE Access,* 2024.

[68] B. Liu, H. Tian, Z. Shen, Y. Xu and W. Dou, "A Consortium Blockchain-Based Edge Task Offloading Method for Connected Autonomous Vehicles," *ACM Transactions on Autonomous and Adaptive Systems,* 2024.

[69] B. Bera, A. Vangala, A. K. Das, P. Lorenz and M. K. Khan, "Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment," *Computer Standards & Interfaces,* vol. 80, p. 103567, 2022.

[70] Y. Bai, Q. Hu, S.-H. Seo, K. Kang and J. J. Lee, "Public participation consortium blockchain for smart city governance," *IEEE Internet of Things Journal,* vol. 9, p. 2094–2108, 2021.

[71] Y. Feng, W. Zhang, X. Luo and B. Zhang, "A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT," *IEEE Transactions on Industrial Informatics,* vol. 18, p. 2840–2848, 2021.

[72] M. Ammi, S. Alarabi and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Information Processing & Management,* vol. 58, p. 102482, 2021.

[73] D. Wang and X. Zhang, "Secure data sharing and customized services for intelligent transportation based on a consortium blockchain," *IEEE Access,* vol. 8, p. 56045–56059, 2020.

[74] J. Chen, T. Cai, W. He, L. Chen, G. Zhao, W. Zou and L. Guo, "A blockchain-driven supply chain finance application for auto retail industry," *Entropy,* vol. 22, p. 95, 2020.

[75] M. Rana, Q. Mamun and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems,* vol. 129, p. 77–89, 2022.

[76] D. Chembakassery, "Proof of Computational Power: An Innovative Consensus Algorithm for Blockchain Systems," in *The International Conference on Recent Innovations in Computing*, 2023.

[77] M. Rukhiran, S. Boonsong and P. Netinant, "Sustainable Optimizing Performance and Energy Efficiency in Proof of Work Blockchain: A Multilinear Regression Approach," *Sustainability,* vol. 16, p. 1519, 2024.

[78] A. Jahid, M. H. Alsharif and T. J. Hall, "The convergence of Blockchain, IoT and 6G: potential, opportunities, challenges and research roadmap," *Journal of Network and Computer Applications,* vol. 217, p. 103677, 2023.

[79] M. A. Qasem, F. Thabit, O. Can, E. Naji, H. A. Alkhzaimi, P. R. Patil and S. B. Thorat, "Cryptography algorithms for improving the security of cloud-based internet of things," *Security and Privacy,* vol. 7, p. e378, 2024.

[80] R. Mathews and D. V. Jose, "Hybrid homomorphic-asymmetric lightweight cryptosystem for securing smart devices: A review," *Transactions on Emerging Telecommunications Technologies,* vol. 35, p. e4866, 2024.

[81] A. Sharma, "Consensus Mechanisms in Blockchain Networks: Analyzing Various Consensus Mechanisms Such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT)," *Blockchain Technology and Distributed Systems,* vol. 1, p. 1–11, 2021.

[82] S. C.-K. Chau, N. Wang and S. Karumba, "EnergiPay: Off-chain Payment Channel for Blockchain-enabled Peer-to-peer Energy Trading," in *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems*, 2024.

[83] F. Firouzi, S. Jiang, K. Chakrabarty, B. Farahani, M. Daneshmand, J. Song and K. Mankodiya, "Fusion of IoT, AI, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine," *IEEE Internet of Things Journal,* vol. 10, p. 3686–3705, 2022.

[84] A. M. Hussein, A. K. Idrees and R. Couturier, "Distributed energy-efficient data reduction approach based on prediction and compression to reduce data transmission in IoT networks," *International Journal of Communication Systems,* vol. 35, p. e5282, 2022.

[85] V. Maurya, V. Rishiwal, M. Yadav, M. Shiblee, P. Yadav, U. Agarwal and R. Chaudhry, "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," *Peer-to-Peer Networking and Applications,* vol. 18, p. 1–35, 2025.

[86] B. Sriman, S. Ganesh Kumar and P. Shamili, "Blockchain technology: Consensus protocol proof of work and proof of stake," in *Intelligent Computing and Applications: Proceedings of ICICA 2019*, 2021.

[87] V. Buterin, Proof of stake: The making of Ethereum and the philosophy of blockchains, Seven Stories Press, 2022.

[88] Q. Hu, B. Yan, Y. Han and J. Yu, "An improved delegated proof of stake consensus algorithm," *Procedia Computer Science,* vol. 187, p. 341–346, 2021.

[89] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access,* vol. 8, p. 14155–14181, 2020.

[90] Y. Li, J. Wang and H. Zhang, "A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces," *Journal of Network and Computer Applications,* vol. 217, p. 103686, 2023.

[91] F. Hashim, K. Shuaib and N. Zaki, "Sharding for scalable blockchain networks," *SN Computer Science,* vol. 4, p. 2, 2022.

[92] C. Sguanci, R. Spatafora and A. M. Vergani, "Layer 2 blockchain scaling: A survey," *arXiv preprint arXiv:2107.10881,* 2021.

[93] M. B. Saif, S. Migliorini and F. Spoto, "A Survey on Data Availability in Layer 2 Blockchain Rollups: Open Challenges and Future Improvements," *Future Internet,* vol. 16, p. 315, 2024.

[94] M. Stipsits, *Scalable Integration of Ethereum in a Microservice based Application through Layer 2 Rollups,* University of Applied Sciences, 2023.

[95] B. Y. K. Kasula, "Optimizing Smart Contracts with Machine Learning Techniques in Blockchain," *International Journal of Creative Research In Computer Technology and Design,* vol. 2, 2020.

[96] F. Marcos Solis, S. E. Pomares Hernandez, J. R. Pérez Cruz and L. M. Rodríguez Henríquez, "Concurrency Conflict Modeling for Asynchronous Processing in Blockchain-Based Transactive Energy Systems," *Mathematics,* vol. 12, p. 3968, 2024.