Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 6, pp. 5649–5671, DOI 10.12694/scpe.v25i6.2936

B-ERAC : BLOCKCHAIN-ENABLED ROLE-BASED ACCESS CONTROL FOR SECURE IOT DEVICE COMMUNICATION

NEELAM SALEEM KHAN[*] ROOHIE NAAZ MIR[†] MOHAMMAD AHSAN CHISHTI[‡] AND MAHREEN SALEEM[§]

Abstract. Security risks are increasingly concerning as the Internet of Things (IoT) expands. Authentication, access control, and authorization present significant challenges for resource-constrained IoT devices. Traditional authentication methods often require enhancements for these devices, but Blockchain technology presents a potential solution. Decentralized and distributed, Blockchain eliminates a single point of failure and relies on Elliptic Curve Cryptography (ECC) for robust security.

We have introduced a cutting-edge solution to fortify communication security within IoT devices across supply chain ecosystems. By harnessing the power of Blockchain technology, our framework incorporates smart contracts, adheres to ES256 encryption standards, and seamlessly integrates with Infura API. These components establish stringent access controls, ensure data integrity, and enhance transparency throughout supply chain processes. The framework's robust architecture facilitates swift and secure transactions, bolsters traceability efforts, and effectively mitigates potential security risks. With its scalable design and reliable functionality, this framework emerges as a pivotal asset for optimizing IoT device communication within dynamic supply chain environments. The use of ProVerif in our analysis provides a formal guarantee of the correctness of our access control mechanisms.

Key words: IoT, Blockchain, Security, Cloud Computing, Infura, Ethereum, Ganache, Metamask

1. Introduction. Devices are becoming more ubiquitous as they strive to fulfill our needs, make life easier, and add value to the tasks we perform every day. The web is now connected to all gadgets, including those used in domestic automation, industrial automation, and smart city infrastructure. The IoT is altering many aspects of the society we live in, including how we shop, how we drive, and even how we obtain electricity for our homes. If handled improperly, the personal data gathered by IoT devices poses a privacy risk. Hence, protecting the Internet of Things is crucial. In order to prevent device hijacking and the spread of botnets, management of the devices should also require effective authentication. Thus, innovations should be created with security in mind to protect the user and the company data acquired by IoT devices. A "defense in depth" strategy is necessary overall, even with the deployment of security layers [47]. The 2020 Indian data breach, which came at a hefty expense of USD 1.9 million, serves as a reminder of the possible monetary losses connected to data breaches. The 2013 US military data breach is a prime example of the dire repercussions of unauthorized access to sensitive data, as it exposed the personal information of millions of government workers, including military personnel [36]. Introducing secure and robust technologies like Blockchain has greatly improved security, privacy, and access control.

Blockchain technology based on cryptographically protected, immutable distributed ledger technology and consensus might improve IoT structures with more mechanized asset optimization and inborn security [8].

Blockchain technology was created as a distributed ledger technology by Satoshi Nakamoto, the person who invented Bitcoin [1]. Blockchain provides reliable and authorized identity registration, tracking of goods and assets, ownership, and product monitoring [35]. A public ledger of all Bitcoin transactions, going back to the first, is called Blockchain. Since new blocks are constantly being added, the Blockchain is a continually improving technology. A computer connected to the network processes the transactions recorded in the Blockchain. These computers are commonly referred to as "nodes." Being a decentralized technology, Blockchain has nodes all over the world. Everything on the network typically occurs, and each block in the Blockchain is added to the chain in the proper order. As all network nodes are part of the same community and are not restricted by

[*]Department of Computer Science & Engineering, NIT Srinagar, J&K, India (neelam_02phd17@nitsri.ac.in).
[†]Department of Computer Science & Engineering, NIT Srinagar, J&K, India (naaz310@nitsri.ac.in).
[‡]Department of Computer Science & Engineering, NIT Srinagar, J&K, India (ahsan@nitsri.ac.in).
[§]Department of Information Technology, NIT Srinagar, J&K, India (mehkhan27@gmail.com).

any specific substance or material, Blockchain technology was developed to be durable and permanent. The network has no single point of failure thanks to its decentralized design.

1.1. IoT Security Dangers. The Internet of Things (IoT) has become an integral part of modern civilization, offering numerous opportunities with its rapidly expanding network of connected devices. However, this growth also brings serious security risks. Some of the prominent IoT security dangers include:

Hijacking of Connected Devices for Botnets and Spam: IoT devices, sharing similar functionalities as smartphones and tablets, can be hijacked by attackers to form botnets for distributed denial-of-service (DDoS) attacks or used to send spam messages.

Leaking of IP/Physical Addresses by Unsecured Devices: Unsecured IoT devices can inadvertently expose the IP and physical addresses of homes or offices, which attackers can exploit or sell to malicious parties.

Advanced Persistent Threats (APT): Cybercriminals can gain unauthorized access to IoT networks and remain passive to gather sensitive information over an extended period.

Remote Vehicle Hijacking: The rise of self-driving cars and trucks brings the risk of remote hijacking despite manufacturers' efforts to mitigate such threats.

Ransomware Attacks: IoT devices like thermostats can be vulnerable entry points for ransomware attacks where attackers encrypt crucial data and demand ransom for its release.

Remote Recording and Surveillance: IoT devices, including cameras and microphones, can be exploited by intelligence agencies and cybercriminals to conduct remote surveillance and record conversations.

Denial-of-Service (DoS) Attacks: Unverified devices connected to the network can launch simple yet malicious DoS attacks .

Authentication Challenges: Traditional authentication methods may not be sufficient for IoT devices with limited resources, calling for more efficient, secure, and scalable strategies [47].

Public Key Infrastructure (PKI) Management: Supporting secure communications in IoT requires managing the complex PKI infrastructure [65].

Location-Based Service Privacy Concerns: Cloud-based IoT users' daily habits can be exposed through location-based services, necessitating safeguarding privacy, trust, and authentication [71].

Resource Limitations: IoT devices often have limited resources, requiring energy-efficient and lightweight protocols, posing computation and energy management challenges.

Single Point of Failure: IoT-based services can suffer from single points of failure due to the heterogeneous network infrastructure, necessitating fault-tolerant implementations [46].

Privacy and Communication Challenges: Significant privacy issues with IoT communication have prompted research into cutting-edge solutions like hardware security, transparent gateways, and end-to-end encryption [38].

Addressing these security dangers is crucial to ensuring IoT devices and networks' safe and reliable operation in various domains. In our work, we employ the key characteristics of Blockchain technology to propose a secure framework for communication in an IoT environment. The key characteristics of Blockchain, including smart contracts, peer-to-peer systems, speed, and capacity, play a crucial role in providing a solution for Blockchain-Enabled Secure Supply Chain IoT Framework for secure IoT device communication. Here is how these characteristics contribute: [2].

- *Smart Contracts:* Smart contracts are self-executing contracts with the terms of the agreement directly written into the code. In the context of our system, smart contracts enforce access control policies by defining and automating the rules governing device communication. These contracts can specify who can access specific IoT devices, under what conditions, and what actions they can perform. Smart contracts provide transparency, immutability, and tamper-proof execution of access control rules, enhancing the security and reliability of IoT device communication.
- *Peer-to-Peer System:* Blockchain operates on a peer-to-peer network, where nodes interact directly without relying on a centralized authority. This decentralized nature eliminates the need for intermediaries and central points of control, making the system more resilient to single points of failure and reducing the risk of unauthorized access or manipulation. In our system, a peer-to-peer system ensures access control policies and decisions are distributed across the network, allowing devices to communicate securely without relying on a centralized access control authority.

- *Speed:* Blockchain technology has evolved to address early implementations' scalability and speed limitations. While traditional public Blockchains like Bitcoin and Ethereum may have slower transaction speeds, newer Blockchain platforms and protocols offer faster transaction processing and higher throughput. These advancements in Blockchain technology enable faster verification and execution of access control policies in our system, ensuring timely and efficient communication between IoT devices without compromising security.
- *Capacity:* Blockchain's capacity refers to its ability to store and process large transactions and data. Our framework requires a robust and scalable system to securely handle the access control requirements of numerous IoT devices. Blockchain's distributed and append-only nature allows for storing access control policies, device identities, and communication logs in a tamper-proof and auditable manner. By leveraging the capacity of Blockchain, our framwork can accommodate the growing number of IoT devices and their access control needs while maintaining the integrity and security of the system.

In addition, every phase of an IoT device's supply chain and life cycle is properly managed, administered, and tracked through the use of the Blockchain. By ensuring that data is cryptographically encrypted and signed by the authorized sender, blockchain ensures data integrity and authentication. Smart contracts on blockchain technology enable privacy and authentication. Every IoT device will have a unique GUID (globally unique identifier) and symmetric key pair once installed and connected to the Blockchain network; this removes the need for distribution and key management. Lightweight security protocols are therefore applied. These compact protocols would satisfy and organize the IoT devices' computing and memory resources needs. The maintenance of immutable records of authorized transactions is guaranteed by Blockchain technology. Moreover, as stated by [60], the Internet of Things leverages Blockchain to store sensor data, control device settings, and enable micropayments.

Supply chains that employ IoT can greatly increase resilience by tackling several issues. Blockchain technology combined with IoT provides secure data frameworks for networked supply chain management systems [17]. By tracking product information across various nodes, this integration makes it possible to create robust supply chain management systems that guarantee scalable and safe operations [20]. Furthermore, supply chains are made more resilient by the decentralized nature of blockchain technology, which solves security and data reliability problems in IoT networks [18]. Moreover, IoT and blockchain technology highlight the potential for boosting supply chain resilience by improving pharmaceutical supply chain operations' efficiency, visibility, flexibility, and transparency, particularly during disruptive times like the COVID-19 pandemic [19]. Supply chains can become more resilient, secure, and capable of handling various situations by utilizing blockchain and IoT, ultimately increasing overall operational resilience. The main contribution of our work is as follows:

- A comprehensive literature review that underscores the growing interest in leveraging Blockchain technology to enhance security and access control in IoT environments. The survey highlights the potential of Blockchain-driven solutions to fortify IoT security while pointing towards promising avenues for further research and development
- Proposing a Blockchain-Enabled Role-Based Access Control for Secure IoT Device Communication. This framework leverages Blockchain technology's security features, such as tamper-proof ledgers, cryptographic encryption, and decentralized consensus, to establish a highly secure access control mechanism for IoT devices. This enhances the overall security posture of IoT networks, reducing the risk of unauthorized access and data breaches.
- The proposed system includes a supply chain use case, enabling secure and transparent communication within the supply chain. This can lead to improved efficiency, reduced fraud, and enhanced accountability in supply chain operations.

2. Literature Review. The literature on Blockchain, IoT and supply chain management offers valuable insights into various aspects of access control, security, and privacy in IoT environments.

2.1. A review of the literature on Blockchain and IoT. Several studies have explored the integration of Blockchain technology with IoT and highlighted its advantages and challenges.

Mayra Samaniego et al. [60] emphasized the challenge of finding suitable hosting locations for Blockchain deployment, considering computing resources, bandwidth, and power conservation. Their findings suggest that deploying Blockchain on resource-constrained IoT devices is not recommended. In comparison, our proposed

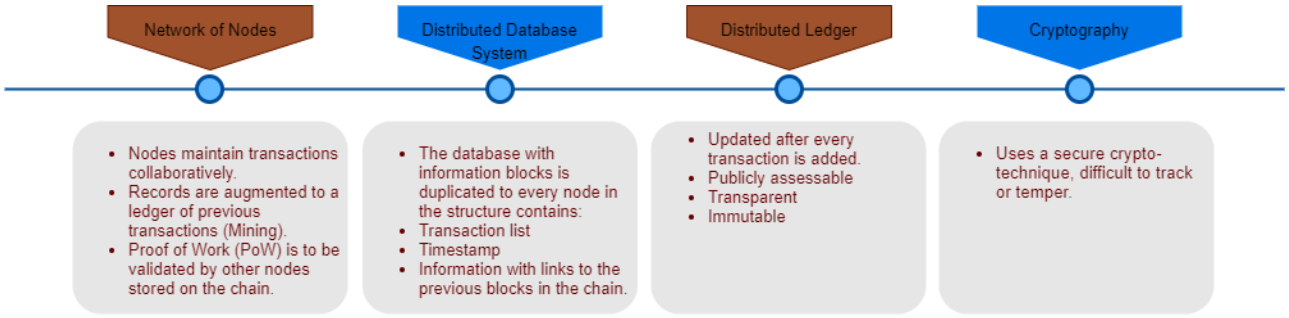

Fig. 2.1: Four Components of Blockchain Technology.

Table 2.1: Threate Identified using STRIDE[70][63] model

Threat	Effect
Spoofing	A malicious management hub could pose as a legitimate management hub.
Tamper	The access control information sent to IoT devices can be changed.
Repudiate	It is possible for a device to say that it hasn't done anything.
DoS	Degrade data sent to an IoT device or expose IoT device data that hasn't been permitted.

system addresses this challenge by leveraging a distributed peer-to-peer system, where the computational and storage burden is distributed among network participants, ensuring efficient and scalable access control for IoT devices. Figure 2.1 illustrates the four components of blockchain, which are discussed by Dr. B. V. Ramana Reddy [68].

Oscar Novo [37] highlighted the advantages of IoT access control, particularly in creating a single, smart contract representing policy norms and enabling larger IoT devices to be part of the access control framework. However, the proposed framework needed more time for access control information release, affecting performance. In contrast, our proposed system leverages the efficiency and speed of Blockchain transactions, ensuring real-time access control management for IoT devices without compromising scalability.

The STRIDE [63] model discovered many threats in the suggested solution, as shown in Table 2.1. The model is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. Their research also indicates that providing a Certification Authority (CA) is a solution to address security challenges. The IoT devices can use this procedure to verify the legitimacy of the management hub as the CA signs the hub nodes.

In their study, Ouaddah et al. [53] presented FairAccess, a decentralized authorization management system based on Blockchain. Their architecture generated a unique smart contract for each resource-requester pair's access control policy. Similarly, our proposed system leverages Blockchain technology to ensure decentralized access control for secure IoT device communication. However, our system goes beyond access control and incorporates role-based access control (RBAC) for more granular and flexible authorization management. Nallapaneni Manoj Kumara et al. [49] discussed the security vulnerabilities in IoT intercommunication and highlighted the challenges of integrating Blockchain technology with IoT. The authors point out that centralized data management servers (CDMS) pose a risk of exposing sensitive data sections to the outside world via fake authentication and device spoofing. The three main topics of the paper are Analytical and Computing Engines (ACE), Raw Information and Processed Data Storage (RI-PDS), and Things with Networked Sensors and Actuators (TNSA). While their study focuses on security and privacy concerns, our proposed system addresses these challenges by providing a secure and decentralized framework for role-based access control in IoT device communication. Other studies, such as Friese et al. [40], Slock.it [13], TransActive Grid, and Filament, have explored the use of Blockchain technology in various IoT applications. These studies highlight the potential of Blockchain for secure and decentralized communication between IoT devices. Our proposed system focuses on

role-based access control, providing a fine-grained and flexible authorization mechanism for secure IoT device communication. Bahga et al. [28] developed BPIIOT, a decentralized peer-to-peer system for Industrial IoT that utilizes Blockchain technology. The BPIIOT framework enables trustless peer-to-peer connections without needing a trusted intermediary, allowing for developing various peer-to-peer and distributed industrial applications. Christidis et al. [34] and Pureswaran et al. [56] described using smart contracts on the Blockchain to facilitate the exchange of services between IoT devices and autonomous workflows.

In the healthcare domain, Matthias Mettler et al. [44] and Asaph Azaria et al. [26] explored the applications of Blockchain technology in managing electronic health records (EHRs) and user-centered medical research. While these studies address security and privacy concerns in healthcare, our proposed system extends the benefits of Blockchain-enabled access control to secure IoT device communication in various domains beyond healthcare. Furthermore, [70] discussed using Blockchain in PSN-based healthcare, where an upgraded version of the IEEE 802.15.6 protocol is being developed to establish secure links. Zyskind et al. [72] presented a platform for securing personal data using Blockchain technology as an access control moderator, and Nabil Rifi et al. [59] proposed a publisher-subscriber mechanism for data access using Blockchain and smart contracts. The system's last component utilizes the off-chain database IPFS [9]. Our proposed system incorporates similar principles of access control and data privacy, but focuses specifically on role-based access control for secure IoT device communication. Several studies have also discussed the limitations and challenges of existing approaches. For instance, Seyoung Huh et al. [43] highlighted the transaction time and storage limitations of Blockchain, which may not be suitable for time-sensitive domains and resource-constrained IoT devices. Similarly, Sayed Hadi Hashemi et al. [15] discussed different access techniques in Blockchain-based IoT systems. In contrast, our proposed system addresses these limitations by leveraging Blockchain technology's speed and capacity advantages, ensuring efficient and secure role-based access control for IoT device communication.

In articles [27] [55], authors presented a solution to minimize the amount of data stored on Blockchain by employing other consensus mechanisms [5], [42], [48], and different graph topologies [30], [12]. Leemon Baird et al. [30] suggested Hedera, a distributed ledger platform and organization that addresses the issues that prevent mass adoption of public DLT(Distributed Ledger Technology). A data structure called a hash graph and a consensus algorithm create a unique platform for delivering consensus in a distributed setup. The contrasts between Blockchain and hash graphs are also highlighted in this study. The hashgraph works well; it is fast, equitable, compliant with ACID, inexpensive, effective, time-stamped, Byzantine, and resistant to DoS attacks.

Serguei Popov [12] discussed the tangle, which is made up of a directed acyclic graph (DAG) for recording transactions, as the next evolutionary step in the Blockchain. In their article, Xiaoqi Li et al. [50] outlined various security vulnerabilities with Blockchain technology. Their study examined every potential risk and vulnerability in Blockchain and their likely origins and implications. Their research also revealed certain real-world Blockchain assaults, focusing on the exploited weaknesses that lead to such attacks. Blockchain technology is increasingly growing as an influential framework for COVID-19 management, according to [3]. Since October 2019, the Chinese government has been focusing on Blockchain. Following the outbreak of the 2020 coronavirus, Chinese hospitals have begun experimenting with Blockchain technology in various applications, including electronic health records and insurance claims. Popular pharmaceutical businesses have collaborated on Blockchain technologies with SAP SE of Walldorf, Germany, to follow supply chains and detect false drug identities. As COVID-19 vaccines and treatments are tested, Blockchain can be used to certify the studies.

According to [4], the COVID-19 pandemic has revealed the shortcomings of current healthcare surveillance systems for quickly responding to public health emergencies. Attention is growing to Blockchain technology as a potential tool to help with various outbreak containment aspects. In order to access electronic health records, a secure infrastructure, entity authentication, identity verification, and persistent representation of authorization are required, according to interoperability guidelines published by the Office of the National Coordinator for Health Information Technology of the US Department of Health and Human Services. These goals may be achieved by the decentralized architecture of the Blockchain thanks to important characteristics like robustness, immutable audit trails, and data provenance. Additionally, while upholding rules for data privacy and security, the various nodes of a permissioned Blockchain can instantly share and report crucial information.

Blockchain can aid disease prevention and control by enhancing various public health activities, such as early

epidemic detection, faster tracking of medication trials, and better management of outbreaks and treatments. During the COVID-19 pandemic, there was a clear surge in demand for electronic medical records (EMRs). Health records are highly sought-after but challenging to implement, given Blockchain's security, privacy, and transparency benefits. In times of crisis, such as COVID-19, research initiatives in this area are encouraged to be implemented nationally and globally [11].

Jayasree et al. [61] categorize security breaches in the Internet of Things into four main groups: physical, network, software, and data attacks. They also provide potential countermeasures for each category. Their analysis also covers the development of Blockchain technology and its benefits when integrated with IIoT and IoT. Their poll addressed security issues regarding Blockchain technology and conventional solutions for the Internet of Things and Industrial Internet of Things, requiring in-depth research.

The paper [69] advances IoT security by addressing information security issues and suggesting a solution utilizing Blockchain-based smart contracts. The limitations of the MQTT protocol in offering secure authentication to Internet of Things devices are brought to light. It illustrates how Blockchain technology can guarantee privacy, accountability, and trust in Internet of Things networks by presenting an Ethereum-based authentication system. The suggested solution hopes to increase user acceptance and uptake by improving security services in IoT networks. In summary, this paper adds to the knowledge about IoT network security and emphasizes how Blockchain can help reduce security risks in the IoT domain.

The paper [22] advances IoT security and suggests Blockchain protocols for secure communication and authentication. It presents the Authenticated Device Transmission Protocol (ADP) for secure communication inside the overlay network and the Authenticated Devices Configuration Protocol (ADCP) for authentication and building a secure overlay network. These protocols improve data integrity and IoT network security by storing authentication records in a distributed Blockchain database. The formal analysis shows their resistance to different attacks, shedding light on how useful Blockchain is for Internet of Things security. Furthermore, the paper presents numerical results confirming its security enhancement, taking into account a stochastic threat model.

The paper [47] presents an overview of security landscape of Fog computing, challenges, and, existing solutions. They outline major authentication issues in IoT, map their existing solutions and further tabulate Fog and IoT security loopholes. Furthermore this paper presents Blockchain, a decentralized distributed technology as one of the solutions for authentication issues in IoT.

The literature survey highlights the increasing interest in leveraging Blockchain technology to enhance security, privacy, and efficiency in IoT environments. Studies have demonstrated the potential of Blockchain to offer decentralized access control, improve data integrity, and address security challenges. Despite scalability and transaction time challenges, proposed solutions include optimized consensus mechanisms and novel cryptographic protocols. Future research should focus on addressing remaining challenges and validating solutions in real-world settings. By leveraging Blockchain's strengths, IoT systems can achieve enhanced security, privacy, and interoperability, fostering a more connected and secure digital ecosystem.

2.2. A review of the literature on Supply Chain Management.. Blockchain's impact reaches various domains such as healthcare and farming by enhancing supply chain management through robust frameworks for data management and secure communication. Table 2.2 provides a comparative analysis of various studies on supply chain management using IoT and Blockchain technology, highlighting the advantages of our proposed supply chain framework.

3. Preliminaries. This section overviews the preliminary concepts and technologies for building secure communication between IoT devices using Blockchain technology. Here is a summary of the key points covered:

3.1. Understanding Blockchain at its core. Blockchain is a public ledger that records all Bitcoin transactions, continually growing as more blocks are added. Transactions are processed by nodes, decentralized computers spread across the network. Ethereum, a programmable Blockchain, allows developers to build decentralized applications (dApps). We focus on Ethereum due to its suitability for decentralized applications. We will be working on the Ethereum Blockchain.The Ethereum Blockchain was developed with decentralized applications in mind, according to [7]. Ethereum ushered in a new era for the internet: i) payments and money are integrated; ii) users own their data, and apps are unable to steal or snoop on it; iii) anyone can now access

Table 2.2: Comparative Analysis of Supply Chain Management Research

Citation	**Method Used**	**Contribution**	**Findings**
[58]	RFID technology	Enhances traceability in fishery supply chains	RFID improves traceability, supply chain visibility, quality control, and regulatory compliance, contributing to sustainability and safety.
[57]	Hyperledger Blockchain and IoT technology	Addresses challenges in chili farming supply chain	Proposes solutions like demand prediction, stock analysis, and building trusted networks, enhancing transparency and security.
[41]	Stylized models and quantitative approaches	Evaluates accountability in IoT supply chains	Introduces accountability measures, contract design, and cyber insurance to mitigate risks and encourage supplier honesty.
[25]	Machine learning models (linear, DenseNet121, ResNet152)	Compares performance of ML models and proposes IoT smart healthcare system	Finds ResNet152 most effective for COVID-19 detection and highlights blockchain-based pharmaceutical system for efficiency and security.
[20]	Ethereum-based Solidity blockchain	Enhances supply chain transparency and scalability	Introduces IoT-Ethereum framework with RFID, highlighting blockchain's role in transparency and scalability despite challenges.
[21]	IoT and blockchain technologies	Enhances resilience in pharmaceutical supply chain post-pandemic	Proposes a model for real-time monitoring, secure data sharing, and improved visibility, flexibility, and transparency.
[51]	Blockchain and Physical Unclonable Functions (PUFs)	Enhances IoT security	Proposes a new authentication algorithm, improving performance with reduced computational overhead and latency.
[64]	Machine learning classifiers	Develops intrusion detection system for IoT supply chain	Creates classifiers detecting 99.99% of intrusions, demonstrating reliable results against various cyberattacks.
[29]	Modified Raft consensus protocol	Enhances blockchain adoption in IoT supply chains	Proposes mRAFT, improving throughput and latency, demonstrating applicability with Hyperledger Caliper.
[52]	Data mining approaches	Tracks evolution of blockchain in smart manufacturing	Proposes a roadmap for intelligent blockchain technology, emphasizing future research and knowledge gaps.
[24]	Review approach	Examines IoT's potential in transforming SCM	Highlights IoT's role in enhancing visibility, efficiency, cost-effectiveness, and risk management, advocating for interconnected and intelligent supply chains.
[54]	Layered security approach	Secures IoT devices and logistics	Explores blockchain for validating logistics, security in decentralized energy trading, and privacy in Bitcoin transactions.
[62]	IoT integration	Solves SCM issues across industries	Discusses solutions for security, tracking, traceability, and warehouse issues in various supply chains.
[66]	Blockchain and IoT integration	Enhances precision farming and smart farms	Proposes blockchain-based solutions for IoT issues, advocating for decentralized and secure data processing and storage.
[45]	Blockchain with IoT	Improves food supply chain transparency and trust	Demonstrates blockchain's influence on food supply chains, highlighting technological adoption and research areas.
[23]	Scalable blockchain protocol	Eases ownership transfer in supply chains	Proposes protocol for IoT devices, enabling secure batch ownership transfers and reducing transaction costs.
[67]	NFC, RFID, GPS technology	Automates and digitizes SCM processes	Highlights IoT's role in real-time monitoring, tracking shipments, and calls for systematic literature reviews in IoT-based SCM.
Our Proposed Scheme	Blockchain-enabled secure communication framework	Establishes secure communication between IoT devices in supply chains	Uses Ethereum Blockchain, ES256 encryption, and smart contracts for secure transactions and item management, enhancing transparency, traceability, and data integrity.

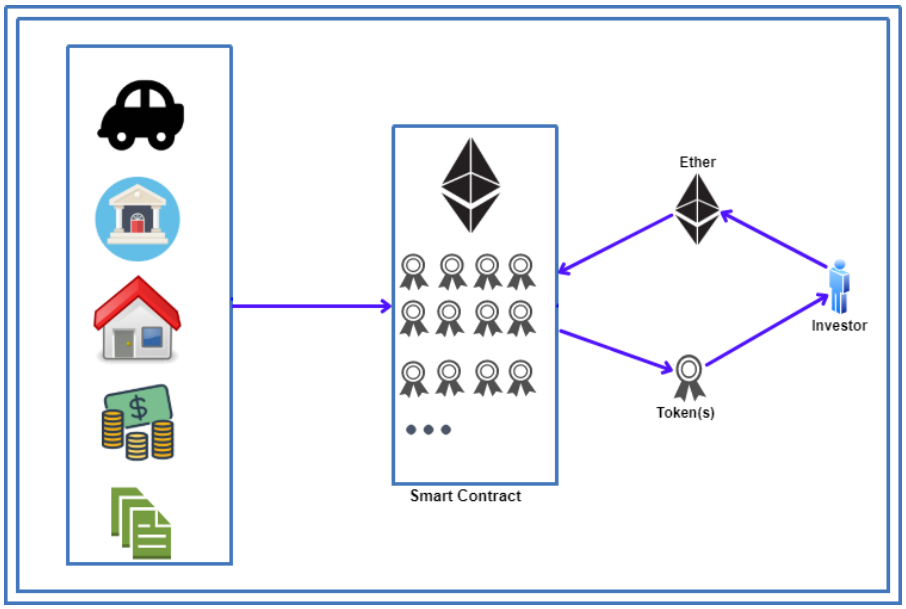

Fig. 3.1: Smart city applications integrated with Ethereum Blockchain through programmable smart contracts

an open financial system; and iv) no one entity is in control, and the system is built on neutral, open-access infrastructure. Figure 3.1 illustrates the Ethereum Blockchain. Transactions on Blockchain networks require signatures using private keys for verification. Each node in the network stores a copy of the Blockchain, and miners create new blocks.

Different types of Blockchain networks exist, such as public (e.g., Ethereum), consortium (e.g., G0-Ethereum), and private (e.g., Multichain). We focus on Ethereum for our work.

3.1.1. Transaction Signatures and Genesis Blocks. Transactions on open Blockchains like Ethereum require signatures for user anonymity and security. Updates must be applied to every node, making it computationally intensive. The initial block of a Blockchain is the genesis block, which is duplicated on each node. Full nodes hold the entire Blockchain, and miners create new blocks in the mining process.

3.1.2. Smart Contracts:. A contract is a legally binding agreement between two or more people. Contracts are socially adaptable because they can be entered and executed without the presence of a third party. The value of contracts is not that an outsider is always available, but that one can be found if necessary. That fallback option is sufficient for establishing confidence between strangers. By replacing the component of trust with enforceable guarantees, contracts increase work division and provide dependability to our globe, which are the foundations of monetary advancement. A smart contract is an agreement between two parties enforced, verified, and performed over a distributed system such as Bitcoin. The sequence of steps to create a Smart Contract is shown in Figure 3.2.

3.1.3. KECCAK function. KECCAK is a versatile cryptographic function for authentication, encryption, and pseudo-random number creation. It is best known as a hash function. Internally, it uses the innovative KECCAK F cryptographic permutation [10], and the structure is simple sponge construction. A wide random function or random permutation is required for sponge formation. It allows" absorbing" any measure of information and yielding/squeezing any information while going about as a pseudo-random function concerning all previous inputs, leading to great flexibility. Keccak-256 Produces a 56-bit hash and is currently used by Ethereum.

3.1.4. Accounts. Ethereum has two types of accounts: external accounts (individuals) and contract accounts (bound by code). Contract wallets, managed by code with a master account, receive, send, and store

Fig. 3.2: Steps to establish a Smart Contract.

Ether. These wallets incur gas costs for creation, represented in ethers.

The address of an external account is determined by its public key. Contract accounts' location is determined during creation based on the creator's address and nonce. Whether they contain code or not, both account types are treated the same by the EVM. Storage is a persistent key-value store, and each account has an Ether balance, where one Ether equals 10**18 Wei, modifiable through Ether-related transactions.

3.2. Strength of Blockchain. Blockchain's address space is 160 bits, while IPV6's 128 bits has an address length of 20 bytes and a public key-generated 160-bit ECDSA hash [68]. ECC is a good option for securing IoT devices in our suggested solution because it provides several benefits. Among these benefits are:

- Strong Security: ECC provides robust security with shorter key lengths compared to traditional encryption methods such as RSA. This is particularly important in resource-constrained IoT environments where computational power and memory are limited.
- Efficient Performance: ECC offers faster encryption and decryption compared to other encryption algorithms. Its computational efficiency makes it suitable for IoT devices, which often have limited processing capabilities.
- Lower Bandwidth and Storage Requirements: ECC requires smaller key sizes, resulting in reduced bandwidth and storage requirements for transmitting and storing cryptographic data. This is advantageous in IoT scenarios where minimizing data transfer and storage overhead is desirable.
- Scalability: ECC is well-suited for scalable deployments in IoT networks due to its efficient use of computational resources. It allows for secure communication and authentication even with a large number of devices.

The basic set of steps in realizing the strength of the Ethereum Blockchain is described in algorithm 1:

The above sequence of steps verifies the authenticity of the Ethereum transaction. It is feasible to confirm that the underlying private key used to sign the transaction and create the transaction signature matches the account used in the transaction "from field". Because of this, every node that participates in a transaction using Blockchain can instantly ascertain its validity. Figure 3.3 shows the complete method. The blocks are connected via cryptographic hashing [14]. To guarantee that the transactions in the Blockchain are in the right order, each block includes the hash of the block before it. The inclusion of previous block hashes guarantees the integrity of the transaction. All blocks that follow are impacted by modifications to a block's transaction(s). Any transaction a hacker tries to alter must be altered in that block and every other block in the Blockchain.

3.3. Interfaces with the Ethereum Blockchain.

3.3.1. Infura. To connect to Blockchain by a hosted Block channel, infura is utilized. It is a bunch of tools for anybody to make an application that interfaces with the Ethereum Blockchain. It interacts with the Ethereum Blockchain and runs nodes on behalf of its users. Metamask, Crypto kitties, Uport, Truffle use it.

Algorithm 1 Transaction Signing and Verification algorithm

Input: Ethereum Transaction
Output: Verifies the authenticity of the Ethereum transaction

I From a wallet, the user sends the Ethereum transaction Ti (say metamask).

II The user has a 32-byte private key Pr and a 64-hex character string that is randomised. A safe randomizer can create private keys at the user's end.

III Pr is transmitted using the ECDSA function (Elliptic curve digital signature Algorithm). This function generates a 64-byte public key named Pk. Pk can be produced from Pr in ECDSA, while Pr cannot be created from Pk in ECDSA. That is Blockchain's strength.

IV Using the Keccak-hash(Pk) function, create a hash of the Pk and extract the final 20 bytes, i.e., B96.....255. That would be the Ethereum Account (the transaction's 'from' field).

V Ti is signed by Pr. Tis is the output, which is a signed transaction.

VI The Tis is passed through ECRECOVER function. The outputs are Pk and the Ethereum Account (the transaction's from' field).

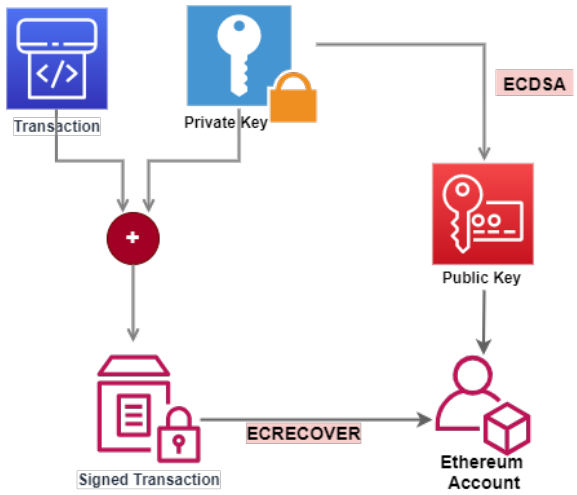

Fig. 3.3: Transaction signing and verification using ECDSA and ECRecover functions.

Infura gives enterprises and developers reliable access to Web3 tools and frameworks.

3.3.2. Truffle. Truffle is an Ethereum Virtual Machine (EVM)-based development, testing, and asset pipeline for Blockchains that makes a developer's life easier [6]. With Truffle, we get built-in Smart contract compilation, linking, deployment, and binary management.

3.3.3. Ganache. Ganache is a personal Blockchain designed to enable swift development of distributed applications on the Ethereum and Corda networks. Its functionality can be leveraged throughout the development process, from coding to deployment and testing, in a secure and predictable environment [6]. Ganache is available as both a desktop application, Ganache UI, and a command-line tool called ganache-cli (previously known as TestRPC) for Ethereum. It supports multiple operating systems including Windows, Mac, and Linux. Developers can interact with Ganache via its API, which is accessible through an RPC server. To transfer ethers between accounts in Ganache, Web3.js library can be used.

3.4. Working of a Blockchain node. Blockchain node communicates with a node with the help of:

1. *RPC:* Remote Procedure Call (Classical HTTP request to interact with API)
2. *IPC:* Inter-Process Communication

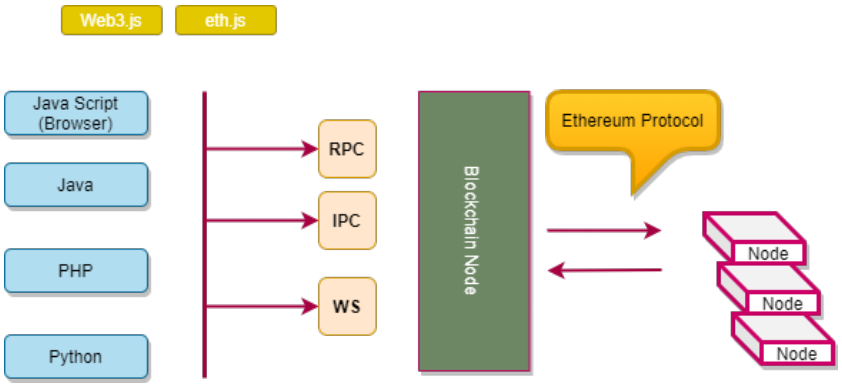

Fig. 3.4: Working of a Blockchain node

3. *WS:* Web Sockets protocol (where a server can send messages to a client)

Figure 3.4 illustrates the entire scenario.

The communication between Blockchain nodes within the Ethereum network occurs through the proprietary Ethereum protocol. A Blockchain node typically provides three methods of connection and control: RPC interface, IPC file, and Web Sockets protocol. The RPC interface sends traditional HTTP requests, similar to those made to interact with APIs or websites. The IPC file permits sending commands to a running process, while the Web Sockets protocol maintains an open connection between the server and client, allowing for bidirectional full-duplex communication. Unlike traditional RPC, the server can transmit messages to the client through the Web Sockets protocol. While typically accomplished through a browser using JavaScript, connecting to a Blockchain node can be achieved using any language with libraries available for popular languages such as Java, PHP, Python, Rust, and . NET. Depending on the system's architecture, these libraries support various connection methods, such as RPC, IPC, or WS.

To implement our proposed model, the components that our required are illustrated in figure 3.5.

The process is initialized by invoking a Metamask wallet to communicate with Infura. We also initiate a faucet(browser) for communication with the back end. For each new transaction that is emitted, block explorer (ropstan.etherscan.io on the Ropsten Test Network and Goerli.etherscan.io on the Goerli Test Network) can be explored for visualizing the transaction events being updated on the Ethereum Blockchain.

Furthermore, we used web3.py to encode and decode requests to connect smoothly with our Blockchain node with a smart contract, which is the architecture we have employed.

3.5. Zerynth Studio. Zerynth Studio is a platform for programming microcontrollers in Python and connecting them to Cloud infrastructures [16]. It enables the creation, signing, and sending of transactions from microcontrollers, facilitating interaction with smart contracts and eliminating centralized passages and points of disappointment. The Zerynth Ethereum library exploits the JSON-RPC interface to cooperate with an Ethereum hub and send an exchange. For the hashing and signs, the Zerynth crypto module is utilized. The primary class accessible is RPC. From an RPC object, bringing network status data and making transactions is feasible.

Zerynth Studio supports Python programming, communication protocols, and features like device emulation and OTA firmware updates. Additionally, Zerynth Studio supports a range of communication protocols, including Wi-Fi, Bluetooth, LoRa, and Sigfox, enabling developers to create IoT applications that can communicate with other devices and services.

Zerynth provides an IoT framework with the following features [16]:

1 Simple to utilize full IoT framework for interfacing new and existing items.
2 Zerynth IoT framework will utilize exclusive requirement security highlights to ensure full data assurance.
3 Top tier group of IoT specialists and devoted support to guarantee a speedy and effective venture.

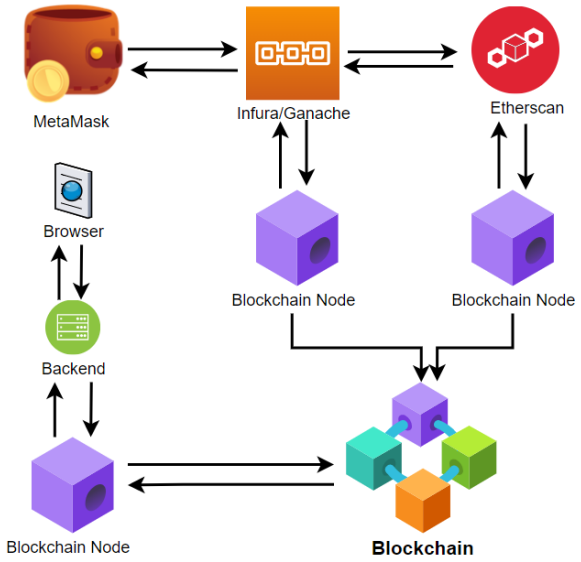

Fig. 3.5: Various components for node interaction in Blockchain based framework.

The Internet of Things revolves around extracting pertinent data from myriad interconnected devices, presenting a challenge in managing device security, application flexibility, and data integrity.

3.5.1. Advantages of using Zerynth instead of using a Raspberry Pi or Arduino.

- Zerynth offers an end-to-end platform for developing secure and connected IoT and industrial applications.
- It provides a Python-enabled operating system, hardware modules, and a device management system.
- Zerynth's integration enables lower power consumption, lower hardware costs, and scalability.

3.6. ProVerif. ProVerif is an automatic cryptographic protocol verifier designed to analyze the security of cryptographic protocols. Developed by Bruno Blanchet and his colleagues, ProVerif supports a wide range of cryptographic primitives, including symmetric and asymmetric encryption, digital signatures, hash functions, and non-interactive zero-knowledge proofs [32]. Key features include:

- *Security Analysis:* ProVerif can prove reachability properties, correspondence assertions, and observational equivalence, making it a powerful tool for verifying secrecy, authentication, privacy, traceability, and verifiability.
- *Protocol Modeling:* It uses the typed pi calculus to represent concurrent processes and interactions over communication channels.
- *Attack Reconstruction:* When a property cannot be proved, ProVerif attempts to reconstruct an execution trace that falsifies the desired property, providing insights into potential vulnerabilities.

ProVerif is a command-line tool that can be installed via OPAM (OCaml Package Manager), from sources, or binaries. It supports integration with text editors like Emacs and Atom for ease of use [31].

4. Framework Implementation and Evaluation of Blockchain-Enabled Role-Based Access Control for Secure IoT Device Communication. This section discusses the proposed solution for establishing secure communication between IoT devices by utilizing Blockchain technology.

4.1. Proposed Framework. The proposed solution aims to establish secure communication between IoT devices by leveraging Blockchain technology. Figure 4.1 illustrates the framework, demonstrating how IoT devices, specifically ESP32, interact with the Blockchain network through Zerynth Studio. The integration with

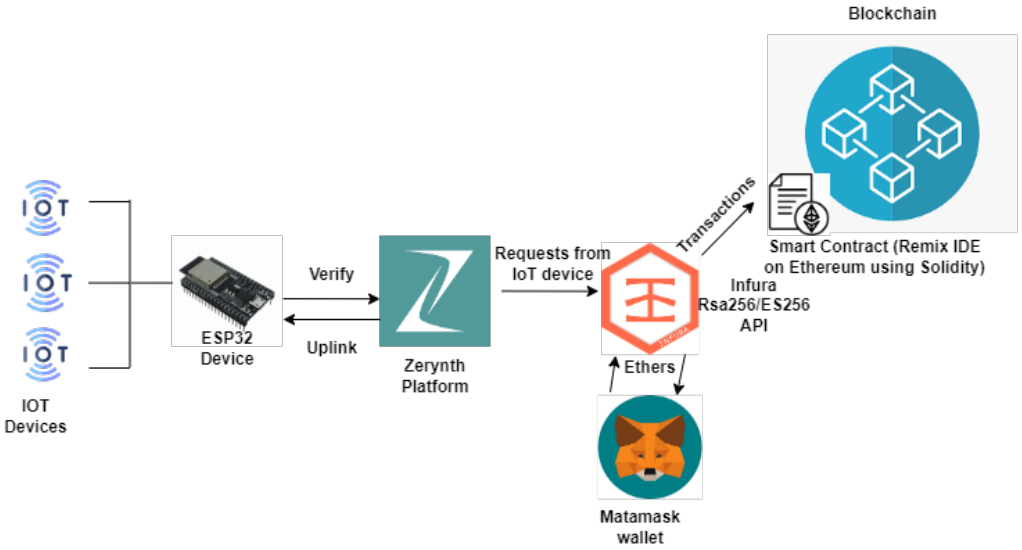

Fig. 4.1: Proposed framework

Infura API provides access to the Ethereum Blockchain network, while smart contracts facilitate a specific use case with owner restrictions governing payments and item deliveries. Transactions are recorded on the Ethereum Blockchain, and ES256 encryption is utilized for security. The smart contract has owner restrictions, which govern the receipt of payments and delivery of items. The smart contract is written in the Remix IDE and uses ethers provided by the Metamask wallet. All transactions are recorded on the Ethereum Blockchain, and their status can be visualized on Infura, which employs ES 256 for security. ES256 (Elliptic Curve Digital Signature Algorithm using the P-256 curve) is a digital signature algorithm Infura uses to secure client communication and API communication. It is a public-key cryptography algorithm that generates a pair of keys, one private and one public, to sign and verify digital transactions. This section covers all the components of the proposed scheme in detail.

4.1.1. Smart contract Deployment. We deployed a smart contract on Remix-IDE using the solidity programming language with the following assumptions.

Assumptions:

1. The smart contract is deployed on a Blockchain network accessible by IoT devices.
2. The IoT device is equipped with a secure digital wallet and can communicate with the Blockchain network.

The Item Manager end:

- The smart contract has a designated manager who has specific permissions and access rights.
- The manager is responsible for managing certain functions of the smart contract, such as creating and updating records.
- The manager is the only account that can access certain functions of the smart contract, as specified by the access control mechanisms implemented in the contract.
- The manager's account is secured by a private key, which is required to authenticate their identity when accessing the smart contract.
- The manager is responsible for ensuring that the smart contract is used in a secure and responsible manner, and for resolving any issues or disputes that may arise in the use of the contract.
- The manager is accountable for any actions taken on behalf of the smart contract and is required to act in the best interests of the contract and its users.The use-case application for buying and creating an item on Blockchain through an IoT device is depicted in figure 4.2.

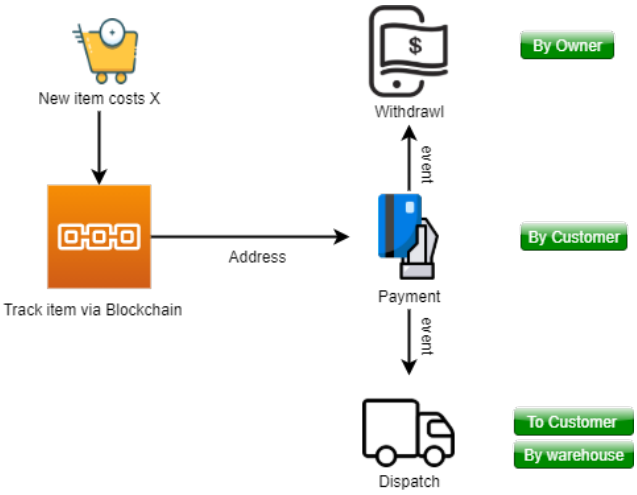

Fig. 4.2: Use-case application for buying and creating an item on Blockchain through an IoT device

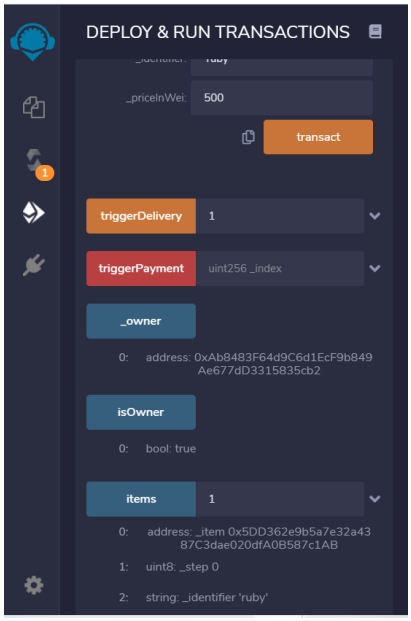

Fig. 4.3: User interface for use-case application on Remix IDE

The IoT device end:

- At the User-end, the user interacts with the IoT device to create an item purchase request. The User-end depicting the entire use-case is shown in figure 4.3.
- The IoT device sends the item purchase request to the smart contract deployed on the Blockchain network.
- The smart contract verifies that the request is valid and that the sender is the owner of the smart contract. If the verification fails, the smart contract sends an error message to the IoT device and terminates the transaction.
- If the verification is successful, the smart contract creates an item and generates a payment request to the user's digital wallet.
- The IoT device receives the payment request and sends the required amount of cryptocurrency from the user's digital wallet to the smart contract.
- The smart contract verifies the payment and dispatches the item to the user through the IoT device.
- If any other account tries to receive payment, the smart contract triggers an error message and terminates the transaction.

The complete working of the proposed framework is presented in Algorithm 2, Algorithm 3 and Algorithm 4.

4.1.2. Connecting Blockchain and IoT device. The Zerynth Ethereum library uses the JSON-RPC interface to communicate with an Ethereum node and send transactions. The primary class provided is RPC. We can perform transactions and retrieve network status information from an RPC object. There are also two companion classes, Transaction, and Contract, which provide a higher-level interface. The former can be used to register a smart contract and its methods for later calling, while the later aids in creating a correct signed transaction ready to be dispatched.

An RPC node providing API is required to communicate with the Ethereum Blockchain. We will use infura, which provides this service without charge. The user can note their API key and register on their website. We created an account in Infura and connected it with our metamask wallet on the Ropsten Test Network to provide us with ethers to make transactions. Infura supports the algorithms RS256 and ES256. The infura

Algorithm 2 Item Manager

Input: Customer requests to buy an item
Output: Item dispatched to customer via supply chain

1. Assign Item Manager as owner
   (a) owner (Item, SupplyChainStep of Item, Identifier of Item)
   (b) SupplyChainStep (Created, Paid, Delivered)
2. Procedure to Create an item
   (a) Assign name to Item
   (b) Assign supply chain step (whether created, paid or delivered)
   (c) Assign an identifier to the Item
3. Procedure to Trigger payment of an Item
   (a) Choose address where Item is to be delivered (only item can update address).
   (b) Allow above address to pay full amount in ethers.
   (c) Check status of Payment in supply chain step.
4. Procedure to Trigger delivery of an Item
   (a) Check if payment is full.
   (b) Change status of supply chain to 'Delivered'.
   (c) Deliver to the address assigned.

Algorithm 3 Authentication

Input: To authenticate if the caller is owner
Output: Returns true if the caller is owner

1. Procedure to check whether caller is owner
   (a) Returns true if the caller is current owner.
   (b) Throws a message if called by any account other than owner.

Algorithm 4 Contract for taking Payment of Item

Input: To receive payment in ethers
Output: Validating the full payment and transferring the amount to Item Manager for delivery of item

1. Create a contract for Item containing (PriceinWei, PaidAmountinWei, IndexOfItem)
   (a) Create a constructor for Item to set (ItemManagerAddress, PriceinWei, IndexOfItem)
2. Procedure to receive payment
   (a) If amount paid is less than PriceinWei, alert with a message "We don't support partial payments".
   (b) If amount paid is already full for an item and customer tries to pay again for same item index, alert with a message "Item already paid".
   (c) Using ItemManagerAddress and PaidAmountinWei, call Procedure Trigger payment using function signature abi.encodeWithSignature(TriggerPayment(Uint256, IndexOfItem)) to transfer money to ItemManager.
   (d) return Success otherwise unsuccessful and trigger the message "Delivery did not work"

Algorithm 5 Connecting Blockchain and IoT device

Require:
To connect IoT device to Ethereum Blockchain for secure communication
Ensure:
Secure Transactions of IoT device via Blockchain Technology
procedure ConnectIoTToBlockchain
Procedure to check WiFi connectivity
if successful connectivity
Print("Successful")
else
Print("Unsuccessful", error())
SSL context is needed to validate HTTPS certificates.
Assign HTTP Provider's API-Key from your Infura registered project account to a variable.
Procedure to interact with Smart Contract on Ethereum Blockchain using Web3.js library.
Assign a variable to object `w3.eth.contract(contract Address, Contract Abi)`.
Procedure `SendEthersToContract(amount)`
begin
nonce = Get the number of transactions sent from wallet address
transaction = {to: contract address,
value: amount in wei,
gas: inWei,
gasPrice: inWei,
nonce: nonce}
Sign the transaction with the wallet private key.
Calculate transaction hash.
Get transaction receipt.
end
Call Procedure `isOwner(address)` from Contract using address of Owner.
Call Procedure `TriggerPayment` from Contract
begin
nonce = Get the number of transactions sent from wallet address
transaction = {to: contract address,
value: amount in wei,
gas: inWei,
gasPrice: inWei,
nonce: nonce}
Sign the transaction with the wallet private key.
Calculate transaction hash.
Get transaction receipt.
end
Call Procedure `TriggerDelivery` from Contract
begin
Deliver the item to the address that paid for the item.
end
Go to infura.io and check the transaction status.
Retrieve the block ID of the last transaction.
end procedure

provides us with an API, a secret project key, and various other security features, including JWT (JSON Web Token), Allowing lists, limiting the number of daily requests, and so on. After Zerynth establishes a connection with infura, infura records the transactions done per second on the Ethereum Blockchain. The complete work of the proposed script is presented in Algorithm 5.

To connect to the ESP32 DevKitC, the configuration file written in python is created as per the requirements like wifi specifications, contract addresses, certificates, keys etc. To communicate with your smart contract on

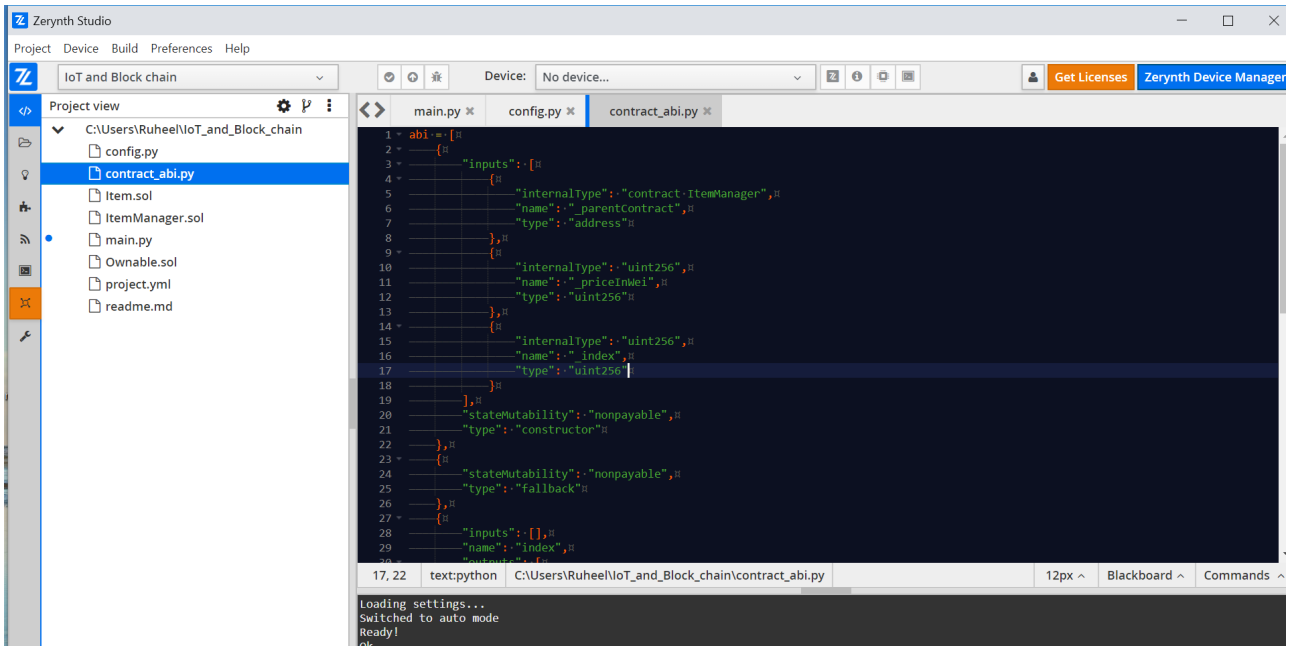

Fig. 4.4: Config ABI

Remix IDE, we need to add the contract's API from remix IDE into the config ABI file, as shown in figure 4.4. Finally the script is uploaded on to the ESP32 DevKitC microcontroller using Zerynth studio.

We designed a framework for secure communication of IoT devices using Blockchain technology. The platform used to achieve our goal is Zerynth Studio, infura and Remix IDE. All the transactions are stored on ledger and we can retrieve the block id of each transaction.

4.2. Security Analysis of proposed scheme. In this subsection, we leverage ProVerif, a widely used automated tool for cryptographic protocol verification, to analyze the access control mechanisms in our smart contract. We aim to ensure that only authorized users can perform specific actions within the contract. It uses a dialect of the pi-calculus to model the protocols and can automatically prove properties like secrecy, authentication, and access control. We model the contract's functions and events in ProVerif to verify the access control properties.

```
(* Declarations *)
(* Types *)
type user.
type item.
type identifier.

(* Constants *)
free alice : user.
free bob : user.
free secret_item : item [private].
free item567 : identifier.
free access_denied : string.

(* Functions *)
fun has_access(user, item): bool.

(* Events *)
```

```
event request_create_item(user, identifier, item).
event grant_create_item(user, identifier, item).
event request_trigger_payment(user, item).
event grant_trigger_payment(user, item).
event request_trigger_delivery(user, item).
event grant_trigger_delivery(user, item).

(* Processes *)

(* Access control process for an owner *)
let owner_process(user: user, item: item, identifier: identifier) =
  out(c, request_create_item(user, identifier, item));
  if has_access(user, item) then
    out(c, grant_create_item(user, identifier, item))
  else
    out(c, access_denied).

(* Example of creating an item by Alice *)
let alice_create_item =
  owner_process(alice, secret_item, item567).

(* Payment process *)
let payment_process(user: user, item: item) =
  out(c, request_trigger_payment(user, item));
  if has_access(user, item) then
    out(c, grant_trigger_payment(user, item))
  else
    out(c, access_denied).

(* Delivery process *)
let delivery_process(user: user, item: item) =
  out(c, request_trigger_delivery(user, item));
  if has_access(user, item) then
    out(c, grant_trigger_delivery(user, item))
  else
    out(c, access_denied).

(* Main process *)
process
  alice_create_item |
  payment_process(bob, secret_item) |
  delivery_process(alice, secret_item)

(* Secrecy: Secret item should not be accessible *)
query attacker(secret_item).

(* Authentication: If access is granted, there must have been a request *)
query grant_create_item(user,identifier,item)==>request_create_item(user,identifier,item)
    .
query grant_trigger_payment(user,item)==>request_trigger_payment(user,item).
query grant_trigger_delivery(user,item)==>request_trigger_delivery(user,item).
```

4.2.1. Result Analysis. By running the ProVerif model, we verify that the access control mechanisms are correctly enforced, ensuring that unauthorized users cannot create, pay for, or deliver items.

Figure 4.5 shows that our smart contract's access control policies are robust against common attacks. The result proves the following:

```
-- Query not attacker(secret_item) in process 0
Translating the process into Horn clauses...
Completing...
Starting query not attacker(secret_item)
RESULT not attacker(secret_item) is true.

------------------------------------------------------------
Verification summary:

Query not attacker(secret_item) is true.

------------------------------------------------------------
```

Fig. 4.5: ProVerif Output

- *Secrecy:* RESULT not attacker *(secret_item)* is true, means that the secrecy of secret_item is preserved by the protocol. ProVerif confirms that *secret_item* is not accessible to the attacker, provided no other vulnerabilities exist.
- *Authentication:* ProVerif verifies that the grant events *(grant_create_item, grant_trigger_payment, grant_trigger_delivery)* are indeed preceded by the corresponding request events. These queries pass, indicating that the system correctly enforces authentication. The system correctly enforces that all access grants are based on prior requests, ensuring proper authentication and access control.

4.3. Benefits of proposed scheme. The proposed scheme offers the following benefits for IoT device communication for a supply chain use case, including:

- Transparency and traceability: Blockchain technology can provide transparency and traceability throughout the supply chain by recording all transactions and data exchanges on an immutable ledger. This can help businesses and individuals track products and components, identify any issues or delays, and improve accountability.
- Data integrity and security: Blockchain technology can ensure the integrity and security of data exchanges in the supply chain by providing a tamper-proof and encrypted ledger. This can help prevent data breaches, reduce the risk of fraud, and improve the trustworthiness of the data.
- Improved efficiency and cost-effectiveness: Blockchain technology can help improve the efficiency and cost-effectiveness of supply chain processes by reducing the need for intermediaries and automating transactions. This can help streamline the supply chain, reduce operational costs, and increase productivity.
- Faster and more reliable transactions: Blockchain technology can provide faster and more reliable transactions in the supply chain by reducing the time and resources required to manage and validate transactions. This can help improve the speed and accuracy of supply chain operations, reducing the risk of errors and delays.

5. Discussion and Evaluation of the proposed scheme. Integrating Blockchain technology to secure communication between IoT devices effectively mitigates single point of failure risks and unauthorized access in resource-constrained devices. We present some evaluation metrics for analyzing the effectiveness of our proposed framework. We have achieved the following objectives using Blockchain for access control in an IoT environment.

- Enhanced Security: Our system leverages the key characteristics of Blockchain, such as smart contracts and peer-to-peer communication, to establish a highly secure access control mechanism. By employing Blockchain's immutability and decentralized consensus, we mitigate the risk of single points of failure and unauthorized access, a significant improvement over traditional centralized access control systems.
- Scalability and Speed: Our system achieves efficient access control without compromising on speed through careful design and optimization of smart contracts. On Ethereum, optimized smart contracts can reduce gas costs by up to 70%, translating to faster execution and lower costs for users. Ethereum 2.0 is expected to handle up to 100,000 transactions per second (TPS) with sharding and Layer 2 solutions, a significant increase from Ethereum 1.0's 15 TPS [33][39]. Blockchain's peer-to-peer network

facilitates faster verification and approval of access requests, enabling real-time communication between IoT devices while ensuring scalability for many devices.

- Decentralization and Trust: Unlike centralized access control systems, our system operates decentralized, removing the need for a trusted intermediary. This enhances trust and transparency, making it challenging for malicious entities to manipulate access control rules or forge identities, thereby strengthening the security posture of IoT networks.
- Flexibility and Customizability: The programmable nature of smart contracts enables our system to accommodate various access control policies and adapt to diverse IoT environments. Administrators can define and modify access rules based on specific use cases, enhancing the system's versatility compared to rigid, pre-defined access control mechanisms.
- Integration with Existing Solutions: Our system is designed with compatibility in mind, allowing easy integration with existing IoT infrastructures and cloud platforms. This reduces the implementation complexity and adoption barriers, making it feasible for organizations to upgrade their IoT security without overhauling their entire architecture.

6. Limitations and challenges of the proposed solution. Although Blockchain technology-based access control protocol has significant applications to mitigate security and privacy issues in resource-constrained IoT devices, some challenges need to be considered to alleviate the limitations of the proposed solution. This section presents an analysis of these challenges, focusing on scalability, interoperability, and regulatory compliance. Below, we provide a detailed discussion of each aspect:

- Scalability: Scalability is critical when implementing secure communication solutions for IoT devices using Blockchain technology. Although our proposed solution can enable real-time communication between IoT devices while ensuring scalability for a large number of devices, as the number of IoT devices grows, the Blockchain network's capacity to handle an increasing number of transactions becomes crucial. The main challenges we anticipate in terms of scalability are:
  a. Transaction Throughput: As the number of IoT devices participating in the Blockchain network increases, the transaction throughput may be affected. Blockchain networks like Ethereum have inherent limitations on the number of transactions they can process per second. To address this challenge, We must explore scaling solutions such as sharding, sidechains, or layer-2 solutions.
  b. Gas Costs: The cost of executing transactions on the Blockchain, measured in gas, could become prohibitive for resource-constrained IoT devices, limiting their participation. To minimize costs, we plan to investigate optimization techniques, smart contract design improvements, and gas-efficient operations.
- Interoperability: Interoperability ensures seamless communication between IoT devices and Blockchain networks. While our proposed solution focuses on the Ethereum Blockchain, there is a need to consider multi-chain scenarios and interactions with other Blockchain protocols. The challenges we acknowledge in achieving interoperability are:
  a. Cross-Blockchain Communication: Enabling communication between IoT devices on different Blockchain networks requires standardized protocols and bridges between chains. We will investigate interoperability solutions like Polkadot, Cosmos, or interoperability-focused smart contract standards.
  b. IoT Protocol Integration: Interoperability with existing IoT communication protocols (e.g., MQTT, CoAP) is essential for smooth integration. We intend to explore middleware solutions and bridge technologies to connect these protocols with Blockchain networks.
- Regulatory Compliance: Adhering to regulatory requirements is crucial, especially concerning data privacy, security, and financial transactions. The challenges we anticipate in terms of regulatory compliance are:
  a. Data Privacy and GDPR Compliance: IoT devices collect and transmit sensitive data, raising concerns about data privacy and compliance with regulations like the General Data Protection Regulation (GDPR). To address these concerns, we will explore encryption techniques, data anonymization, and privacy-preserving solutions.
  b. Financial Compliance: In scenarios involving financial transactions, our solution needs to adhere to financial regulations, such as Anti-Money Laundering (AML) and Know Your Customer (KYC) re-

quirements. We plan to investigate techniques for integrating compliance checks within smart contracts while maintaining data confidentiality.

7. Conclusion. The paper explores the potential of Blockchain technology to provide security for IoT devices and presents a smart contract-based solution using Ethereum and Zerynth. Infura and Remix IDE make the development process simple and efficient. The scheme offers numerous benefits, such as enhanced security, improved efficiency, cost-effectiveness, and reliable transactions. Using ECC in Blockchain ensures robust security without a single point of failure. The use of ProVerif in our analysis provides a formal guarantee of the correctness of our access control mechanisms. The result shows that our smart contract's access control policies are robust against common attacks. This strengthens the security of our smart contract and provides confidence in its deployment in real-world scenarios. The paper provides important contributions to integrating Blockchain technology with IoT devices, offering security, transparency, traceability, scalability, speed, and data integrity.

REFERENCES

[1] *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://git.dhimmel.com/bitcoin-whitepaper/. Accessed: 2023-10-20.
[2] *Block chain developer course*. https://vomtom.at /. Accessed: 2023-10-20.
[3] *Blockchain adoption could help in COVID-19 fight | 2020-05-11 | BioWorld*. https://www.bioworld.com/articles/435042-blockchain-adoption-could-help-in-covid-19-fight. Accessed: 2023-10-20.
[4] *Blockchain and Corona virus: could it prevent future pandemics?* https://www.finextra.com/blogposting/18570/blockchainand-corona-virus-could-it-prevent-future-pandemics. Accessed: 2023-10-20.
[5] *Cardano | Home*. https://cardano.org/. Accessed: 2023-10-20.
[6] *Ganache | Overview | Documentation | Truffle Suite*. https://www.trufflesuite.com/docs/ganache/overview. Accessed: 2023-10-20.
[7] *Home | ethereum.org*. https://ethereum.org/en/. Accessed: 2023-10-20.
[8] *How Blockchain and Smart Contracts Can Impact IoT | by Smartz | Smartz Platform Blog | Medium*. https://medium.com/smartz-blog/how-blockchain-and-smart-contracts-can-impact-iot-f9e77ebe02ab. Accessed: 2023-10-20.
[9] *IPFS Docs*. https://ipfs.io/docs/. Accessed: 2023-10-20.
[10] *Keccak Team*. https://keccak.team/index.html. Accessed: 2023-10-20.
[11] *Opinion | Five ways in which blockchain technology can aid a recovery*. https://www.livemint.com/opinion/columns/five-ways-in-which-blockchain-technology-can-aid-a-recovery-11589479234967.html. Accessed: 2023-10-20.
[12] *Serguei Popov ,The tangle 2017* . http://iotatoken.com/ IOTA_Whitepaper.pdf. Accessed: 2023-10-20.
[13] *slock.it Blog*. https://blog.slock.it/. Accessed: 2023-10-20.
[14] *Understanding How Blockchain Works*. https://blog.ndcconferences.com/understanding-blockchain/. Accessed: 2023-10-20.
[15] *World of empowered IoT users*, ieeexplore.ieee.org.
[16] *Zerynth*. https://www.zerynth.com/. Accessed: 2023-10-20.
[17] *Improving supply chain resilience with employment of iot*, Springer, Berlin, Heidelberg, 2015, pp. 404–414.
[18] *A review and development of research framework on technological adoption of blockchain and iot in supply chain network optimization*, (2020).
[19] *Iiot and cyber-resilience*, Ai & Society, 36 (2021), pp. 725–735.
[20] *Design and deployment of iot enabled blockchain based resilient supply-chain management system using ethereum*, International Journal of Computing and Digital Systems, 12 (2022), pp. 1029–1050.
[21] *Internet of things (iot)—blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era*, Frontiers of Engineering Management, 10 (2022), pp. 82–95.
[22] *Blockchain-based authentication and secure communication in iot networks*, Security and privacy, (2023).
[23] *Scalable lightweight protocol for interoperable public blockchain-based supply chain ownership management*, Sensors, 23 (2023), pp. 3433–3433.
[24] K. B. Adeusi, A. E. Adegbola, P. Amajuoyi, M. D. Adegbola, and L. B. Benjamin, *The potential of iot to transform supply chain management through enhanced connectivity and real-time data*, World Journal of Advanced Engineering Technology and Sciences, (2024).
[25] R. AlGhamdi, M. O. Alassafi, A. A. Alshdadi, M. M. Dessouky, R. A. Ramadan, and B. W. Aboshosha, *Developing trusted iot healthcare information-based ai and blockchain*, Processes, (2022).
[26] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, *MedRec: Using Blockchain for Medical Data Access and Permission Management*, ieeexplore.ieee.org, (2016).
[27] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, *Enabling Blockchain Innovations with Pegged Sidechains*, tech. rep., 2014.
[28] A. Bahga, , V. M. J. o. S. E. Applications, and undefined 2016, *Blockchain platform for industrial internet of things*, scirp.org.

[29] M. A. Baig, M. A. Baig, D. A. Sunny, D. A. Sunny, A. Alqahtani, A. A. Alqahtani, S. Alsubai, S. Alsubai, A. Binbusayyis, A. Binbusayyis, M. Muzamal, S. A. Khan, and M. Muzammal, *A study on the adoption of blockchain for iot devices in supply chain*, Computational Intelligence and Neuroscience, (2022).
[30] L. Baird, M. Harmon, and P. Madsen, *Hedera: A Governing Council & Public Hashgraph Network The Trust Layer of the Internet*, tech. rep.
[31] B. Blanchet, *Modeling and verifying security protocols with the applied pi calculus and proverif*, Foundations and Trends® in Privacy and Security, 1 (2016), pp. 1–135.
[32] B. Blanchet, *ProVerif Manual*, 2024. Accessed: 2024-07-25.
[33] V. Buterin, *Ethereum 2.0 will reach 100,000 transactions per second*, 2020. Accessed: 2024-07-26.
[34] K. Christidis, M. D. I. Access, and undefined 2016, *Blockchains and smart contracts for the internet of things*, ieeexplore.ieee.org.
[35] M. De Vos, J. A. Pouwelse, P. Otte, and J. Pouwelse, *Article in Future Generation Computer Systems ·*, Elsevier, (2017).
[36] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, *Securing iot devices: A novel approach using blockchain and quantum cryptography*, Internet of Things, 25 (2024), p. 101019.
[37] O. N. Ericsson and O. Novo, *Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT*, Article in IEEE Internet of Things Journal, (2018).
[38] A. Escobar-Molero, K. Bierzynski, A. Escobar, and M. Eberl, *Cloud, fog and edge: Cooperation for the future?*, ieeexplore.ieee.org, (2017).
[39] E. Foundation, *Sharding 101*, 2020. Accessed: 2024-07-26.
[40] I. Friese, J. Heuer, N. K. . I. W. F. on Internet, and undefined 2014, *Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative*, ieeexplore.ieee.org.
[41] Y. Ge and Q. Zhu, *Accountability and insurance in iot supply chain*, arXiv.org, (2022).
[42] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, *Algorand: Scaling Byzantine Agreements for Cryptocurrencies*, dl.acm.org, (2017), pp. 51–68.
[43] S. Huh, S. Cho, and S. Kim, *Managing IoT Devices using Blockchain Platform*.
[44] M. M. . I. t. international conference on E-health and undefined 2016, *Blockchain technology in healthcare: The revolution starts here*, ieeexplore.ieee.org.
[45] M. D. Kale and P. S. Rathod, *Agriculture food supply chain management system based on blockchain and iot*, International Journal of Advanced Research in Science, Communication and Technology, (2023).
[46] M. A. Khan, K. Salah B A Bahauddin, Z. U. Multan, and P. B. Khalifa, *IoT security: Review, blockchain solutions, and open challenges*, Future Generation Computer Systems, 82 (2018), pp. 395–411.
[47] N. S. Khan and M. A. Chishti, *Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review*, Scalable Computing: Practice and Experience, 21 (2020), pp. 515–542.
[48] A. Kiayias, A. Russell, B. David, and R. Oliynykov, *Ouroboros: A provably secure proof-of-stake blockchain protocol*, in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10401 LNCS, Springer Verlag, 2017, pp. 357–388.
[49] N. M. Kumar, N. K. Singh, S. Vallabhbhai, N. Manoj Kumar, A. Dash, and N. K. Singh^, *Internet of Things (IoT): An Opportunity for Energy-Food-Water Nexus Water based photovoltaic systems (WPVS): Floating and Submerged PV View project Blockchain applications for sustainability and resilience View project Internet of Things (IoT): An Opportunity for Energy-Food-Water Nexus*, ieeexplore.ieee.org, (2018).
[50] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, *A Survey on the Security of Blockchain Systems*, tech. rep.
[51] A. N, N. Anita., V. M, and M. Vijayalakshmi, *Iot security in supply chain using blockchain*, 2021 2nd International Conference on Communication, Computing and Industry 4.0 (C2I4), (2021).
[52] M. R. Nair, N. Bindu, R. Jose, et al., *From assistive technology to the backbone: the impact of blockchain in manufacturing*, Evolutionary Intelligence, 17 (2024), pp. 1257–1278.
[53] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, *Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT*, Springer, 520 (2017), pp. 523–533.
[54] K. Pal and K. Pal, *Security issues of blockchain-based information system to manage supply chain in a global crisis*, (2021).
[55] J. Poon and T. Dryja, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, tech. rep., 2016.
[56] V. Pureswaran and P. Brody, *Device democracy: saving the future of the internet of things. IBM (2014)*. https://public. dhe. ibm. com/common/ssi/ecm/gb/en/gbe03620usen/global-business-services-globalbusiness-services-gb-executive-brief-gbe03620usen-20171002. pdf (2019). Accessed: 2023-10-20.
[57] A. N. Putri, A. N. Putri, A. N. Putri, A. N. Putri, M. Hariadi, M. Hariadi, M. Hariadi, M. Hariadi, A. D. Wibawa, A. D. Wibawa, A. D. Wibawa, and A. D. Wibawa, *Smart agriculture using supply chain management based on hyperledger blockchain*, IOP Conference Series: Earth and Environment, (2020).
[58] L. F. Rahman, L. Alam, M. Marufuzzaman, and U. R. Sumaila, *Traceability of sustainability and safety in fishery supply chain management systems using radio frequency identifica- tion technologylabonnah*, (2021).
[59] N. Rifi, E. Rachkidi, N. A. . I. t. …, and undefined 2017, *Towards using blockchain technology for IoT data access protection*, ieeexplore.ieee.org.
[60] M. Samaniego, U. Jamsrandorj, and R. Deters, *Blockchain as a Service for IoT Cloud versus Fog*, ieeexplore.ieee.org, (2016).
[61] J. Sengupta, S. Ruj, and S. Das Bit, *A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT*, Article in Journal of Network and Computer Applications, 149 (2019), p. 102481.
[62] H. Sharma, R. Garg, H. Sewani, and R. Kashef, *Towards a sustainable and ethical supply chain management: The*

potential of iot solutions, arXiv.org, (2023).
[63] T. O. Shawn Hernan, Scott Lambert and A. Shostack, *Uncover Security Design Flaws Using The STRIDE Approach*. https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach. Accessed: 2022-09-15.
[64] H. K. Skrodelis, H. K. Skrodelis, A. Romanovs, and A. Romānovs, *Synthetic network traffic generation in iot supply chain environment*, International Scientific Conference Information Technology and Management Science Riga Technical University, (2022).
[65] I. Stojmenovic and S. Wen, *The Fog Computing Paradigm: Scenarios and Security Issues*, ieeexplore.ieee.org.
[66] U. Surya and M. Shamaiah, *An interpretation of the challenges and solutions for agriculture-based supply chain management using blockchain and iot*, International Conference Computing Methodologies and Communication, (2023).
[67] S. Taj, A. S. Imran, Z. Kastrati, S. M. Daudpota, R. A. Memon, and J. Ahmed, *Iot-based supply chain management: A systematic literature review*, Internet of Things, 24 (2023), p. 100982.
[68] B. Venkata, R. Reddy, and B. V. R. Reddy, *Block chain: A Game Changer for Securing IoT Data*, tech. rep., 2019.
[69] S. M. Zanjani, H. Shahinzadeh, J. Moradi, Z. Rezaei, B. Kaviani-Baghbaderani, and S. Tanwar, *Securing the internet of things via blockchain-aided smart contracts*, in 2022 13th International Conference on Information and Knowledge Technology (IKT), 2022, pp. 1–8.
[70] J. Zhang, N. Xue, X. H. I. Access, and undefined 2016, *A secure system for pervasive social network-based healthcare*, ieeexplore.ieee.org.
[71] J. Zhou, Z. Cao, X. D. I. C. …, and undefined 2017, *Security and privacy for cloud-based IoT: Challenges*, ieeexplore.ieee.org.
[72] G. Zyskind, O. Nathan, and A. . Sandy' Pentland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, ieeexplore.ieee.org, (2015).

Edited by: Kumar Abhishek
Special issue on: Machine Learning and Blockchain based solution for privacy and access control in IoT
Received: Nov 29, 2023
Accepted: Aug 25, 2024