Secure Communication And File Transfer System Using Blockchain Technology

Mr. Prasad Uttam Harer[1], Mr. Kshitij Kantilal Bhosale[2], Miss. Mayuri Hemraj Godse[3] Mrs. Neha Bhagwat[4],
Department of Computer Engineering [1,2,3,4]
Nutan Maharashtra Institute of Engineering and Technology, Pune,
Maharashtra.[1,2,3,4]
.

Abstract: In the digital age, the security and integrity of communi cation and data transfer has become important. Centralized syste ms face challenges in managing data confidentiality, preventing ta mpering, and ensuring authenticity. To solve these problems, this article proposes a new way to create secure communication and data transfer using blockchain technology. Known for its distribution and immutability, blockchain has a unique advantage in increa sing security and trust. By leveraging decentralized blockchain da ta, encryption mechanisms and smart contracts, we can create a strong infrastructure for secure communication and data transmission. Key elements of the process include self-governance using blo ckchainbased digital signatures, data encryption using strong encr yption algorithms, smart contracts automati on, decentralized management for redundancy and fault tolerance,and an immutable audit method for transparency and accountability. . Thanks to the integration of blockchain technology, users can enjoy enhanced security, privacy and accuracy in communicationand data transfer activities. The system reduces the risks with unauthorized access, interception and leakage of information on by ensuring that only authorized individuals access and interact with data. This article provides concept and design considerations for using secure communication and data transfer using blockchain technology. It highlights the benefits and challenges associated with these systems and provides insight into future research directions to improve their effectiveness and application potential.

Keywords: blockchain, secure communication, decentralization cryptography, access control, smart contracts, data encryption, authentication, data integrity, trust, privacy protection

I. INTRODUCTION

In recent years, blockchain is an innovative technology. It first appeared in 2008 and is popularly known as Bitcoin. Blockchain brings a new perspective to business trust between two organizations without the third party. The main advantage of blockchain is the reduction of interference due to its immutability. It also has some advantages. Centralization means that single organization controlling the system.The rapid expansion of the Internet and the rapid growth of digitalinformation have highlighted the urgent need for secure and reliable communication and data transfer. Traditional systems suchas email and cloud storage often do not protect confidentiality and integrity. For example, emails can be easily intercepted and altered; Since cloud storage solutions depend on central servers, they are easily interrupted.Blockchain technology offers the promise of missing from traditional communication and data transfer processes. Its decentralized, immutable and transparent structure is essential. Using blockchain's decentralized information system, information is distributed across multiple nodes, thus reducing the possibility of unauthorized access. The growth of online communication and data transfer in today's digital environment highlights the importance of security and trust. Traditional systemssuch as email and cloud storage often fail to meet stringent requirements for protecting sensitive data. Emails can be intercepted, and cloud storage systems that rely on centralized servers are prone to vulnerabilities and breaches. Blockchain technology, which provides distributed, immutable, transparent and secure communication and data transmission, has emerged as an effective solution to solve these problems.

By leveraging the decentralized information technology of Blockchain, data integrity and confidentiality can be ensured collaboratively, thus reducing the risks associated with the process. This article explores the potential to revolutionize secure communication and data transfer. It examines the principles and methods of blockchain technology and shows how they improve security, privacy and trust in digital communication andinformation exchange. Additionally, the impact of blockchain integration into existing systems is discussed and challenges and future directions in this development are explored. Through this research, we aim to deeply understand the changes that the evolution of blockchain technology will create on communication and information security in the digital age. In an age where digital interaction and data exchange are important, the need for secure communication and data transfer is more important than ever. As organizations and individuals continue to use technology to communicate and share important information, the shortcomings of traditional methods are becoming more apparent and serious. Addressing these security issues requires new solutions that adapt to the state of the digital environment. Originally created to support cryptocurrencies, blockchain technology has become a valuable candidate for improving the security and integrity of communications and data transfer. In today's digital age, the need for secure communication and data transfer has become indispensable. As organizations and individuals rely on digital channels to exchange sensitive information, ensuring the confidentiality, integrity and accuracy of information has become a priority and important. Communication and data transmission arealways subject to various threats such as data inaccessibility, interception and interference.In today's digital landscape, safeguarding the confidentiality and integrity of communication and data exchange has become paramount. Traditional centralized systems encounter difficulties in maintaining data security, preventing tampering, and guaranteeing authenticity. This article proposes a novel approach to address these issues by harnessing blockchain technology, renowned for its decentralized nature and immutability, to bolster security and trust. By capitalizing on decentralized blockchain data, robust encryption methods, and smart contracts, we can establish a robust framework for secure communication and data transmission. The process entails several key components: Self-governance: Utilizing blockchain-based digital signatures to ensure authenticity and integrity.Data encryption: Employing powerful encryption algorithms to safeguard information. [3]

Smart contracts: Facilitating access control and automation for enhanced security. Decentralized management: Providing redundancy and fault tolerance. Immutable audit trail: Ensuring transparency andaccountability. Through the users can benefit from heightened security, privacy, and accuracy in their communication and data exchange endeavors. This system mitigates the risks associated with unauthorized access, interception, and leakage of information by restricting data interaction to authorized individuals only. The article offers an overview of this concept and explores design considerations for implementing using blockchain technology. It outlines the advantages and challenges of suchsystems and suggests future research avenues to enhance their effectiveness and broaden their application scope

II. LITERATURE SURVEY

With the increasing demand for secure and decentralized filesharing systems, this paper proposes a novel approach combining blockchain technology. The proposed system leverages the decentralized storage capabilities offs for file storage and distribution, while blockchain ensures data integrity and access control. In this system, files are divided into chunks and stored across multiple IPFS nodes, ensuring redundancy and fault tolerance. Smart contracts deployed on the blockchain manage access control and file permissions, providing a secure and transparent mechanism for users to share files.
Additionally, cryptographic techniques are utilized to encrypt files and ensure confidentiality during storage and transmission. [1]

This paper presents an in-depth exploration of the design and implementation of a secure storage solution leveraging blockchain technology deployed on cloud infrastructure. By harnessing the immutable and decentralized nature of blockchain, the proposed solution ensures data integrity, confidentiality, and availability in cloud storage environments. The integration of provides tamper-proof audit trails, cryptographic verification, and distributed consensus mechanisms, thereby enhancing the security and reliability of data storage and retrieval operations. This paper discusses the architecture, components, and functionalities of the proposed secure storage system, along with practical considerations for deployment and management in cloud environments. Through a comprehensive evaluation, this study demonstrates the effectiveness and feasibility of utilizing blockchain technology for achieving secure storage in the cloud [2]

Sure, imagine a network where authority like a government or a corporation to facilitate communication, everyone involved shares the responsibility equally. Each participant in this network maintains a record of all communications, which are secured through cryptographic techniques. This ensures that messages cannot be tampered with or accessed by unauthorized parties. It's like a digital version of passing notes in class, but with advanced security measures and no single person in charge. In contrast, our proposed system utilizes blockchain technology to establish a decentralized network where communication is secured through cryptographic techniques and consensus mechanisms. The security and reliability of data storage and retrieval operations. This the architecture, components, and functionalities of the proposed securestorage system, along with practical considerations for deployment and management in cloud environments. Through a comprehensive evaluation, this study demonstrates the intermediaries, our system enhances security, privacy, and resilience against malicious attacks. We outline the architecture and functionality of the proposed system, including the role of blockchain nodes, cryptographic protocols, and consensus algorithms. Furthermore, we discuss the potential applications and benefits of deploying such a decentralized communication system in various domains, including messaging, file sharing, and data transmission.[5]

This paper introduces a groundbreaking communication system that harnesses the power of blockchain technology for security. Unlike traditional systems that depend on centralized authorities, our approach ensures decentralization, meaning no single entity controls the network. we establish a distributed network where participants collectively maintain the system's integrity. Communication within this network is fortified by cryptographic methods, guaranteeing thatmessages remain confidential and unaltered. Additionally, consensusmechanisms ensure agreement among participants on the validity of transactions, enhancing the system's reliability and resilience against attacks. mechanisms. We outline the architecture and functionality of the proposed system, including the role of blockchain nodes, cryptographic protocols, and consensus algorithms. This paper presents an in-depth exploration of the designand implementation of a secure storage solution leveraging blockchain technology deployed on cloud infrastructure. considerations for deployment and management in cloud environments. Through a comprehensive evaluation, this study demonstrates the intermediaries, our system enhances security, privacy, and resilience against malicious attacks. We outline the architecture and functionality of the proposed system, including the role of blockchain nodes, cryptographic protocols, and consensus algorithms. Furthermore, we discuss the potential applications and benefits of deploying such a decentralized communication system in various domains, including messaging, filesharing, and data transmission.[4]

This paper presents an in-depth exploration of the a secure storage solution leveraging blockchain technology deployed on cloud infrastructure. By harnessing the immutable and decentralized nature of blockchain, the proposed solution ensures data integrity, confidentiality, and availability in cloud storage environments. The integration of blockchain technology provides tamper-proof audit trails, cryptographic verification, and distributed consensus mechanisms, thereby enhancing the security and reliability of data storage and retrieval operations. This paper discusses the architecture, components, andfunctionalities of the proposed secure storage system, along with practical considerations for deployment and management in cloud environments. Through a comprehensive evaluation, this study demonstrates the effectiveness and feasibility of utilizing blockchain technology for achieving secure storage in the cloud.[6]

This paper introduces a novel communication system that is built on blockchain technology. This system is entirely decentralized, implying This paper presents a novel approach to secure communication systems leveraging fully decentralized blockchain technology. Traditional communication systems often rely on centralized authorities or intermediaries to facilitate secureexchanges, which can introduce vulnerabilities and single points of failure. In contrast, our proposed system utilizes blockchain technology to establish a decentralized network where communication is secured through cryptographic techniques and consensus mechanisms. The security and reliability of data storage and retrieval operations. This paper discusses the architecture, components, and functionalities of the proposed secure storage system, along with practical considerations for deployment and management in cloud environments. Through a comprehensive evaluation, this study demonstrates the intermediaries, our system enhances security, privacy, and resilience against malicious attacks. We outline the architecture Furthermore, we discuss the potential applications and benefits of deploying such a decentralized communication system in various domains, including messaging, file sharing, and data transmission. [8]

This paper proposes a novel framework for secure file sharing and data provenance leveraging the integration of Blockchain technology and the Interplanetary File System (IPFS). In traditional file sharing systems, maintaining data integrity, authenticity, and provenance can be challenging due to centralizedstorage and reliance on trust-based mechanisms. By combining thedecentralized and immutable nature of Blockchain with the distributed storage capabilities of IPFS, our framework offers enhanced security, transparency, and accountability in file sharing. Files are hashed and stored on IPFS, with their corresponding metadata and transaction records stored on the Blockchain. This ensures tamper-proof data storage and enables transparent tracking of file provenance throughout its lifecycle. Additionally, smart contracts are utilized to automate file sharing agreements and enforce access control policies, further enhancing security and efficiency. We present a detailed architecture of our framework and discuss its advantages in ensuring secure file sharing and preserving data provenance in various applications.[18]

Cloud storage is one of the leading options where you can keep big data, however, a way to keep a single cloud space using a computer is not secure. By contrast, Blockchain is a cloud-based storage system that guarantees security of data. A peer network can be joined and developed by any computer node connected to the Internet, which willincrease resource use Blockchain is a distributed peer-to-peer system that is kept immutable by each node in the network maintaining a copy of the blockchain. The IPFS (Inter Planetary File System) protocol is used in the suggested system to encrypt user files, which are then stored across several network peers. Hashes are generated by IPFS. The file path is indicated by the hash value, which is kept on the blockchain. [10]

III. METHODOLOGY

Proposed System:

The system intends to create data transport, communication, and security using blockchain technology. Three primary parts make up the system: blockchain system The blockchain stores all conversations and transaction data, serving as an in-terrify map. To ensure the data's authenticity and immutability, each block in the chain includes the timestamps, transaction record numbers, and cryptographic details from the block before it.

Benefits:

1. Enhanced security: To guarantee the security and integrity of conversations and data transfers, Blockchain makes use of encryption technologies. Documents and messages are encrypted to guard against illegal access, eavesdropping, and interception. Because blockchain networks are decentralized, there is a lower chance of errors and cyberattacks, which raises overall security.[16]

2. Distribution and peer-to-peer communication: Blockchain makes it unnecessary to transmit data or use middlemen or central administrators for communication. Rather than relying on centralized servers and outside services, members converse directly with one another peer-to-peer. Due to the lack of a centralized authority or backup, independent administration promotes privacy, independence, and flexibility.[17]

3. Transparency and trust: The authenticity and transparency of blockchain technology foster more communication between parties. any transaction is documented on the blockchain and accessible to any member of the network. Because users can trace the beginning and end of conversations and data transfers, transparency raises accountability and lowers the possibility of fraud or poor management.

4. Efficiency and cost savings: By removing pointless middlemen and optimizing data flow, blockchain streamlines communication and data exchange. By automating and processing business agreements, smart contracts lessen the need for manual intervention and the load on managers.

1. System Architecture:

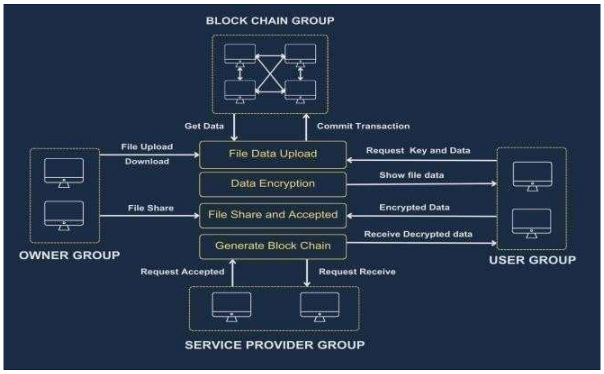


Figure 1- System Architecture

1. Blockchain team: Data encryption and decryption are handled by the blockchain team. In the blockchain ledger, it further saves metadata and access control permissions.
2. Owner group: Users who possess the file make up the owner group. Users are able to share, download, and upload files.
3. User Group: Users with data access make up the user group. They are unable to post or share files, but they can download and view files.
4. Service provider group: Nodes that offer data transfer services make up a service provider group. They are in charge of relaying messages exchanged between group users and owners.
5. Group owners: make the first move to ask group suppliers for data transfers. The user receives a metadata information-containing application.
6. Decentralized: Since the system is decentralized, errors cannot occur. It becomes more impervious to censorship and assaults as a result.
7. Encryption: Before any data is sent or kept on the blockchain ledger, it is encrypted. This information's confidentiality is safeguarded.
8. Access control: Authorization governs access to information. Files can only be downloaded, downloaded, and distributed by authorized users.
9. Auditability: A blockchain ledger has a record of every transaction. This is a thorough summary of all the research data.

1. Algorithm:

Peer Verification Protocol: -

Peer Verification Protocol (PVP) is a system and process designedto verify the identity, credentials, or other relevant information of individuals in a community, network, or platform. It aims to build trust and confidence among peers by ensuring that members represent themselves and their qualifications.[20]

Creating a hash: -

Hashing is an technique that creates a stable string (hash value or checksum) from input data of any size. A hash function is a mathematical algorithm that takes input data and produces a unique hash value that represents the original data. Even small changes in input data can cause a difference in the hash. In secure data communication, a hashing protocol is used to create a hash value for each data sent. This hash value is used as a digital fingerprint or checksum for the data. It allows the receiver to verifythe authenticity and accuracy of the received data by comparing thehash value with the hash value provided by the sender.[14]

Mining Algorithms for Generating Valid Hashes: -

In secure data communication, mining algorithms are generally not used to generate hashes. Instead, cryptographic hash functions are often used to ensure data integrity and authenticity during archive transmission. A hash function is a mathematical algorithm that accepts input (or words) and produces a constant string, usually a hexadecimal number. The output (called the hash value or hash digest) is specific to the input data. Even smallchanges in input data can cause a difference in the hash.[13]

1. USE CASE DIAGRAM :

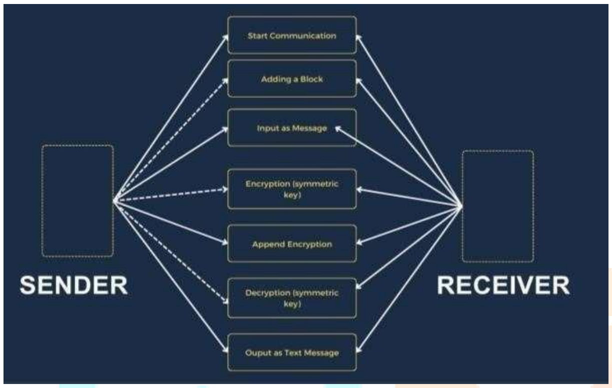


Figure 2- Use case Diagram

Use case diagrams assist developers in understanding user requirements by modeling system behavior. A use case diagram can be helpful in providing an overview of the system and in defining the roles and responsibilities of each person. Use case diagrams illustrate the relationship between use cases and actors by combining them with use cases.

The user and the system are the two actors in the diagram. The user has the ability to choose an entity and enter information, among other tasks. The system loads the data set, classifies the data, and then predicts the disease. Selecting the entity entails choosing the disease and entering the patient's information[12]

In contrast, our proposed system utilizes blockchain technology to establish a decentralized network where communication issecured through cryptographic techniques and consensus mechanisms. The security and reliability of data storage and retrieval operations. The architecture, parts, and features of the suggested secure storage system are covered in this article, along with useful advice for setup and administration in cloud contexts. This paper illustrates the intermediates, our system improves security, privacy, and resistance against malicious attacks via an extensive examination [11]

As previously stated, a blockchain is a distributed ledger, and the entries on the chain include new transactions as well as data needed to maintain track of past transactions. Nevertheless, storing huge data or documents on the blockchain comes with some restrictions. Since the quantity of data that can be stored in a block is restricted, it functions effectively as an expensive database for huge data storage.

Mathematical model:

Algorithm 1: Peer Verification Protocol

```
User Transaction TID (Terminal Identification Number) and IP
address are provided for input.
Step 1: Users create any kind of DDL, DML, or DCL transaction
query.
Step 2: Obtain your IP address right now Else Flag false If
(connection (IP) equals (true))
 Step 3 ends if (Flag == true). Valid Peer-to-Peer Verification
 Other Inter-Peer Validation
 Not Valid Finish if End of Output:
Enable the IP address or, if there is a valid connection, the current
query.
```

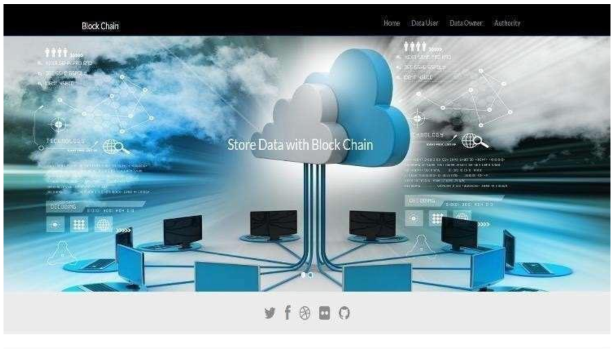
Algorithm 2: Hash Generation

```
Input: Data D, the previous hash, and the Genesis block First,
enter the data as d
Step 2: Utilize SHA 256 from the SHA group
Step 3: SHA256(d) is the current hash.
Step 4: Return Current Hash Output: Based on the provided data, a
hash H was generated.
```

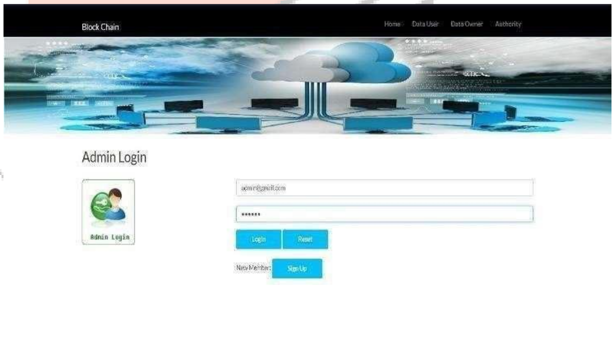
Algorithm 3: Mining Algorithm for valid hash creation

```
Entry: Policy P for Hash Validation [], Current Hash Values hash
Val
Step 1: - The system uses Algorithm 1 to produce the hash value
for Transaction 1.
Step 2: - if (validity of hash value with P []) 1 for the flag Else
Flag: 0
Step 3: - If flag=1, return a valid hash Valid hash is the output.
```

VI. RESULTS



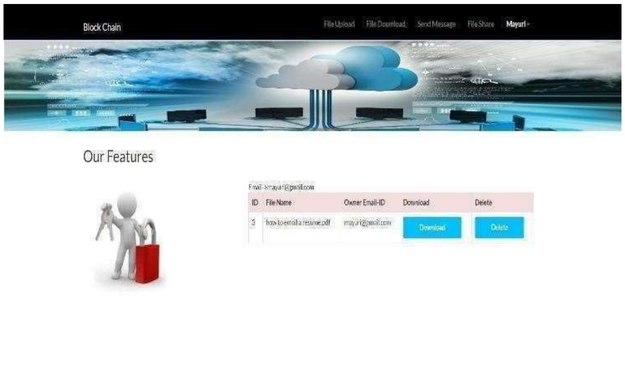
Frontend



admin@gmail.com

******

Admin Login page



Email- mayuri@gmail.com

ID	File Name	Owner Email-ID	Download	Delete
3	how to email a resume.pdf	mayuri@gmail.com	Download	Delete

Profile of the User

IV. CONCLUSION

In conclusion, blockchain technology is a more private, efficient, transparent, safe, and effective method to engage with others and manage our data, which has the potential to revolutionize the way we exchange information and communicate. We may anticipate further uses in this field of interest as blockchain technology develops further. Technology, encryption, and data exchange are fascinating concepts. This system presents the several encryption techniques utilized in the blockchain as well as the evolution of encryption techniques. Also covered are some security flaws with blockchain technology. A quick discussion of blockchain concerns and the various security services offered for privacy and authentication follows. The program may be used to guarantee the accessibility, confidentiality, and privacy of private data exchanged with users inside an organization.

Network security will be the primary focus of blockchain technology's future uses. Information on the blockchain is secure and verifiable while being open and decentralized. To achieve this, risks like illegal data manipulation are removed by encryption.

V. REFERENCES

[1] Yuan J, Yang H, Dong S, Yao Q, Jiao L, Zhang J. Demonstration of Blockchain-based IoT Devices Anonymous Access Network Using Zero-knowledge Proof. In2020 International Wireless Communications and Mobile Computing (IWCMC) 2020 Jun 15 (pp. 1607 1609).IEEE.

[2] Yazdinejad A, Srivastava G, Parizi RM,Dehghantanha A, Karimi pour H, Karizno SR. SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks. In2020 IEEE 91st Vehicular Technology Conference (VTC2020- Spring) 2020 May 25 (pp. 1-5). IEEE.

[3] Al-madaniAM, Gaikwad AT. IoT Data Security Via Blockchain Technology and Service Centric Networking. In2020 International Conference on Inventive Computation Technologies (ICICT) 2020Feb 26(pp. 17-21). IEEE.

[4] Qiu C, Wang X, Yao H, Du J, Yu FR, Guo S. Networking Integrated Cloud-Edge-End in IoT: A Blockchain Assisted Collective Q-Learning Approach. IEEE Internet of Things Journal.2020 Jul 7.

[5] Lao L, Dai X, Xiao B, Guo S. G-PBFT: a location- based and scalable consensus protocol for IOT Blockchainapplications. In2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS) 2020 May 18(pp. 664-673). IEEE.

[6] U. Bodkhe, Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab ''Blockchain for industry 4.0 79764– 79800, 2020.

[7] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, ''Blockchain-enabled distributedsecurity framework for nextgeneration IoT: An edge cloud and software-defined network-integrated approach,'' IEEE Internet Things J., vol. 7, no. 7, pp. 6143–6149, Jul. 2020.

[8] F. Kandah, B. Huber, A. Altarawneh, S. Medury, and A. Skjellum, ''BLAST: Blockchain-based trust management in smart citiesand connected vehicles setup,'' in Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC), Sep. 2019, pp. 1–7.

[9] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, ''A privacy-preserving trust model based on blockchain for VANETs,'' IEEE Access, vol. 6, pp. 45655–45664, 2018.

[10] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo, ''Blockchain- enabled cyber-physical systems: A review,'' IEEE Internet Things J., early access, Aug. 6, 2020, doi: 10.1109/JIOT.2020.3014864.

[11] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. H. Park, ''Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems,'' IEEE Sensors J., early access, Jul. 15, 2020, doi: 10.1109/JSEN.2020.3009382.

[12] M. D. Borah, V. B. Naik, R. Patgiri, A. Bhargav, B. Phukan, and

[13] S. G. Basani, ''Supply chain management in agriculture using blockchain and IoT,'' in Advanced Applications of Blockchain Technology. Singapore:Springer, 2020, pp. 227–242. [14]

M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, ''A lightweight blockchain based framework for underwater IoT,'' Electronics, vol. 8, no. 12, p. 1552, Dec. 2019. [15]

M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, ''Formal security analysis of LoRaWAN,'' Comput. Netw., vol. 148, pp. 328–339, Jan. 2019.

[16] J. de Carvalho Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic,and A. L. L. Aquino, ''LoRaWAN—A low power wan protocol for Internetof Things: A review and opportunities,'' in Proc. 2nd Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech), 2017, pp. 1–6.

[17] J. Wu, Y. Feng, and P. Sun, ''Sensor fusion for recognition of activities of daily living,'' Sensors, vol. 18, no. 11, p. 4029, Nov. 2018.

[18] D. Puri. IoT and LoRaWAN Modernize Livestock Monitoring. Accessed: Feb. 10, 2020. [Online]. Available: http://www.braemacca. com/en/news/item/iot-and-lorawan-modernize-livestock-monitoring

[19] I. Butun and R. Sankar, ''A brief survey of access control in wireless sensor networks,'' in Proc. IEEE Consum. Commun. Netw. Conf. (CCNC), Jan. 2011, pp. 1118–1119.

[20] V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, and S. Kanhere, ''Blockchain technologies for IoT,'' in Advanced Applications of Blockchain Technology. Singapore: Springer, 2020, pp. 55–89.