PRIVACY PRESERVING ACCESS CONTROL FRAMEWORK FOR CLOUD DATA USING BLOCKCHAIN

Manjunath H[1], Bhumika R[2], Harsha G[3], Varshitha D[4], Yamuna[5]

[1]Dept of CS&E, Bangalore Institute of Technology, Bangalore, India.
E-mail: manjunathh@bit-bangalore.edu.in
[2]Dept of CS&E, Bangalore Institute of Technology, Bangalore, India.
E-mail: 1bi20cs403@bit-bangalore.edu.in
[3]Dept of CS&E, Bangalore Institute of Technology, Bangalore, India.
E-mail: 1bi20cs407@bit-bangalore.edu.in
[4]Dept of CS&E, Bangalore Institute of Technology, Bangalore, India.
E-mail: 1bi20cs418@bit-bangalore.edu.in
[5]Dept of CS&E, Bangalore Institute of Technology, Bangalore, India.
E-mail: 1bi19cs190@bit-bangalore.edu.in

ABSTRACT

The cloud is a computer platform that enables sharing and universal on-demand access, bringing new data processing and services to a wide range of sectors, drastically lowering user computing and storage costs, and enhancing usability. Cloud security has grown in importance as a result of the scalability and intensity of clouds in the world of cloud computing. One of the essential security methods for safeguarding sensitive data that businesses and individuals store in the cloud is access control. The centralised access control system used in the cloud makes it simple for hackers or inside cloud managers to alter or leak critical data. We provide Privacy Preserving Access Control Framework Using Blockchain to solve this problem. First, we use the blockchain node's account address as its identity. At the same time, we reconfigure the data's access control permissions for the cloud, where the data is encrypted and kept. Then, using a framework for privacy-preserving access control, we build processes for access control, authorisation, and authorization revocation. Last but not least, we put the Privacy Preserving Access Control Framework based on enterprise operation system (EOS) into practise. The findings demonstrate that the framework can both safeguard authorised privacy and stop hackers and administrators from improperly accessing resources.

Keyword: - *Authorization, Access, Revocation, Indirect Access*

1. INTRODUCTION

Cloud computing, as a new computing model, can provide users with services of omnipresence, and reduce the cost of user storage and computing, and improve the convenience of use, so more and more businesses and individuals choose to store data in cloud. However, with the development of cloud computing scale and intensification, research on fog computing and edge computing has also gradually risen, cloud security issues have become an important factor restricting cloud computing development. In July 2017, the cloud security alliance (CSA) published a "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0", which identified 14 cloud computing security focus areas, among which access control is one of the core technologies of cloud security. The goal of using access control to stop resources saved in cloud storage from being accessed or stolen by unauthorised users is another ongoing research area. The main three service systems of cloud computing, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), all need to protect relevant resources through access control, so access control plays an important role in cloud.

Compared with the traditional computing model, the computing and storage mode of cloud computing have undergone many changes, which are mainly reflected in the following five aspects:

- Users cannot control the resources in cloud;
- Lack of trust between users and cloud;

- Migration technology may cause data to change the security domain;
- Multitenant technology makes the access subject to be redefined;
- Virtualization technology may lead resources to be stolen on the same physical device.

2. LITERATURE WORK

In this section, we describe about the existing work. Our Paper deals with the problem associated with the existing system and also gives user a clear knowledge on how to deal with the existing problems and how to provide solution to the existing problems.

Distributed systems with wireless networks, massive amounts of data, analytical tools, and industrial and physical equipment are combined and connected to create the Industrial Internet. Since the industrial data are shared, access control techniques must be used to limit who or what can access the data. Currently, the majority of Industrial Internet access control systems are built for cloud computing platforms, presuming that all industrial data is exchanged over the cloud. In [1], we take into account a different situation in which the business instead stores the industrial data locally on-site. We suggest a distributed access control mechanism based on blockchain and smart contract technology for this scenario. We assess its performance in various system setups as well.

Social data, which is frequently saved in the social data server (SdS), local real-time data, which is typically stored in the fog-edge server (FeS), and historical data from all over the world, which is typically stored in the cloud, are all included in the Cyber-Physical-Social System (CPSS) concept of big data. Additionally, CPSS big data has a central access control system that can quickly block customer access to it. For CPSS huge data, it is therefore recommended to adopt the BacCPSS access control mechanism [2]. Before deciding to use a lightweight symmetric encryption technology to preserve privacy, BacCPSS developed mechanisms for permission, authorization revocation, access control, and audit. The processes of permission, revocation, access control, and audit are implemented by BacCPSS. Redefining and recording access control permission for the massive CPSS data set in blockchain. The account address of the node on the blockchain is used as the identity to access CPSS big data. The result is the creation of an exact experimental model based on the EOS and Aliyun clouds. Results demonstrate that BacCPSS is a practical and effective method for granting secure access in CPSS while preserving privacy.

The cloud storage system has developed a powerful technique called Blockchain-based access control and data sharing strategy to improve data security. Single-point failure in the cloud system is successfully resolved by the suggested Blockchain-based access control and data sharing strategy [3]. By boosting throughput and decreasing cost, it offers greater advantages. Using their ID and password, the Data User (DU) submits a registration request to the Data Owner (DO), who handles it and verifies the Data User's identity. Using the encrypted master key, the data owner's information is encoded and added to the transactional blockchain. The Interplanetary File System (IPFS) receives encrypted files after the Data Owner completes the data encryption procedure. Based on the encrypted file location and encrypted key, the Data owner generates the ciphertext metadata and is embedded in the transactional blockchain. The proposed Blockchain-based access control and data sharing approach achieved better performance using the metrics, like a better genuine user detection rate of 95% and lower responsiveness of 25sec with the blockchain of 100 sizes.

A taxonomy and an evaluation of blockchain-based trust management strategies in cloud computing systems are introduced in [4]. Three phases—blockchain-based fundamental trust framework, blockchain improved trust interaction framework and mechanisms, and data management—are used to categorise these techniques into several taxonomies. Then, a thorough examination and comparison of the current blockchain-based trust techniques is presented. A novel cloud-edge hybrid trust management framework and a cloud transaction model based on double blockchains are suggested in order to increase the effectiveness and adaptability of trust-enabled cloud computing. Finally, we outline the current issues facing blockchain-based trust management systems and make some suggestions for the future. The uniqueness of [4] is that it studies the application of blockchain from the perspective of trust. Our analysis shows that using blockchain technology to construct a decentralized trust management framework has the following benefits:

- It eliminates the single point of failure and avoids data leakage,
- Identity and trust behavior evidence is traceable and interpretable, trust evaluation results are convincing, the malicious use of data is prevented,
- It is especially suitable for constructing IoT trust relationships.

The Internet of Things (IoT)'s dispersed architecture and rapid, widespread adoption pose a number of security and privacy issues. One of the main issues being addressed at the moment is access control. The dependence of centralised systems on a third party as well as their scalability and availability restrictions may cause a performance bottleneck. [5] suggests a novel method for managing the lightweight, decentralised safe access to an IoT system. It is built on a multi-agent system and a blockchain. Building Blockchain Managers (BCMs) for safeguarding IoT access control and enabling secure communication between local IoT devices is the major goal of the suggested technique. The method also makes it possible for secure connections to be made between Internet of Things devices.

Most of the existing works only focus on knowledge generation rather than trading in IoT. To address this issue, [6] proposes a peer-to-peer (P2P) knowledge market to make knowledge tradable in edge-AI enabled IoT. [6] propose an implementation architecture of the knowledge market. Moreover, we develop a knowledge consortium blockchain for secure and efficient knowledge management and trading for the market, which includes a new cryptographic currency knowledge coin, smart contracts and a new consensus mechanism Proof-of-Trading (PoT).

When outsourcing data-mining tasks to the cloud, the data owner chooses n ($n > 2$) servers be longing to the different clouds. It splits its private key into n pieces and distributes them to the n servers, respectively. The private key is secure as long as not all the n servers collude. [8] assume that at least one out of n servers is honest. In addition, the data owner sends an encryption of the minimum support threshold to the servers.
[8] assume that each server is semi honest; that is, it honestly follows the data mining algorithm but might be curious about the privacy of the data (for example, the frequencies of items or association rules).
In this setting, [8] propose three solutions at different security levels for the servers from different clouds to cooperate to mine association rules from the encrypted data and return to the data owner encrypted association rules with encrypted support and confidence. Compared to the work on outsourcing of association rule mining, the main advantage of their work is that it relaxes the data owner’s requirements for data storage, computation resources, and expertise.

Cloud computing is a paradigm that is changing. The NIST definition provides a foundation for discussion on everything from what cloud computing is to the best ways to use it. It characterises key elements of cloud computing and is meant to be used as a tool for broad comparisons of cloud services and deployment approaches. The service and deployment models described create a straightforward taxonomy that does not aim to impose or restrict any specific deployment, service delivery, or business operating technique.
Cloud computing is very emerging area in IT industries. In a cloud environment, many distributed systems are interconnected to provide software, hardware and resources over the internet. Since this new paradigm requires users to ensure the security of their personal data, there are gradually increasing security and privacy issues on outsourced data. A natural way to keep the data in a confidential manner is to encrypt it before storing on cloud server. The main problems of this process include building scalable access control for storing data and revoking access rights from users if they are revoked from the system. Many access control schemes have been already developed. In [11], a taxonomy and brief survey of secure data access control schemes in cloud environment have been presented. The current research issues and future work directions are also presented in [11] in the area of security of cloud computing.

Multi-Authority Based on Attributes In order to implement fine-grained access control on the encrypted data in cloud computing, encryption is a potential cryptographic technology. However, the attribute with weight is typically ignored by the multi-authority based attribute encryption techniques used in cloud computing. In this research, a multi-authority based attribute encryption method is given the concept of weight. In cloud computing, a suggested multi-authority based weighted attribute encryption system. According to their significance, the attribute authorities give characteristics varying weights. According to the analysis, the [12] is secure. Compared to the existing schemes, the scheme is better suited for the cloud computing environment since it may indicate the importance of qualities.

In industrial automation, numerous devices are interconnected in smart factories for further monitor and control. Various infrastructure devices in industrial automation are usually used for control instruction distribution, data collection, and collaboration of the industrial applications. Recent security threats on industrial automation are more frequent and the industrial control systems lack trust mechanism. Blockchain has been introduced due to its decentralization and security promise, but the election results in the original designs could be biased without collaboration trust, which leads the blockchain-based industry applications invalid. In addition, in existing solutions, neither super nodes nor normal nodes in blockchain can transfer their control authorities for disaster backup. To address the aforementioned challenges, [13] proposes a collaborative trust based unbiased control transfer mechanism (CTM), which realizes a dynamic assignment of industrial control. First, a collaborative trust based delegated proof of stake consensus is proposed for determining the authorities of control dynamically and unbiasedly, by designing a lightweight trust propagation protocol. Second, a CTM

for checking, alarming, and restarting CTM is devised for the disaster backup. The simulation results demonstrate the CTM, which is feasible and effective for industrial automation security.

3. SYSTEM ARCHITECTURE

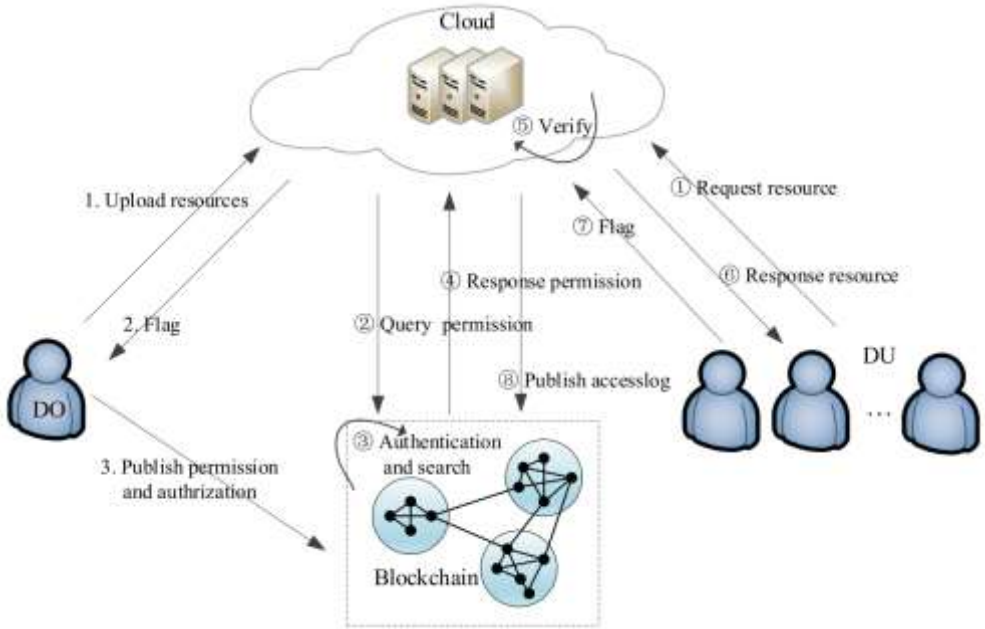

Fig-1: Architecture of Access Control Framework

The system architecture defines the overall structure of the system, including its components, their interactions, and the data flow between them. In this system, we have identified the following components:

- **Cloud:** It provides authentication and data storage for users. Cloud determines access rights of DU or DO by Blockchain. Cloud will issue request for registration to Blockchain.
- **Blockchain:** It is open, transparent, tamper-proof, and irreversible, and the same as the distributed database, we use it as an authorization policy database for access control.
- **DO:** DO uploads the resources to Cloud and publishes the resource's access rights to Blockchain. Data owner need to register to our application if they registered then they can login to our application using the user name and password. DO will authorize data users to Blockchain, can upload/publish files and can perform revoke. DO login then uploads the resources to Cloud and publishes the resource's access rights to Blockchain.
- **DU:** DU can access the resources if he has permission from Cloud. Data User can access the resources if he has permission from Cloud. All users will sign up with application and this details will be stored in Blockchain by using ISAVE Smart Contract function. After registration Blockchain can be used to store access permission or control. To identify each user Blockchain generate identify keys.

4. RESULTS AND PERFORMANCE ANALYSIS

Different performance indicators were established and analysed in terms of performance analysis to assess the effectiveness of the system. Different facets of the system's behaviour were evaluated using metrics such response time, throughput, resource utilisation, and scalability. The system's overall performance was revealed by the performance study, which also pointed up potential bottlenecks and constraints. It was noted that the system's response time occasionally surpassed the predetermined performance goal, which negatively impacted the user experience.Based on the performance analysis, performance optimization efforts were undertaken to address the identified issues. Code optimizations, caching strategies, and algorithmic enhancements were implemented to improve the system's performance. These optimization measures yielded positive results,

reducing the response time and enhancing overall system efficiency. However, Also observed was that some optimizations required trade-offs in terms of increased resource utilization or complexity.

The findings from the results analysis and performance evaluation provide valuable insights into the system's functionality and performance. The identified defects and inconsistencies were resolved, ensuring the system's reliability and stability. The performance analysis shed light on areas for improvement and optimization, allowing for a more efficient and responsive system.

The experimental results show that the authorization publish performance is related to the selected blockchain and the nodes connecting blockchain. Selecting the appropriate blockchain and configuring the nodes will greatly improve the performance. As shown in Figure 3(c), the optimal performance of the Jungle is about 4.4s, the optimal performance of Kylin is about 0.4s, and the optimal performance of the localhost less than 0.02s.

According to Figure 2, the overall performance of AuthPrivacyChain and traditional access control is very similar. Traditional access control is done in cloud, and AuthPrivacyChain's access control needs to interact with blockchain. In conclusion, both the authorization and access control performance are related to the configuration of blockchain. The choice of blockchain has an impact on performance. For the same blockchain, you can configure nodes to achieve better performance.

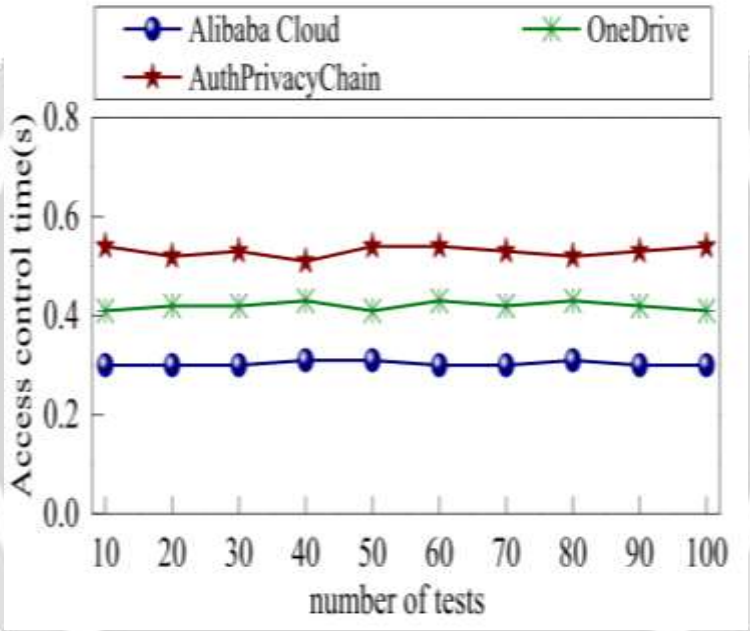

Fig-2:Traditional and AuthPrivacyChain access control performance comparision

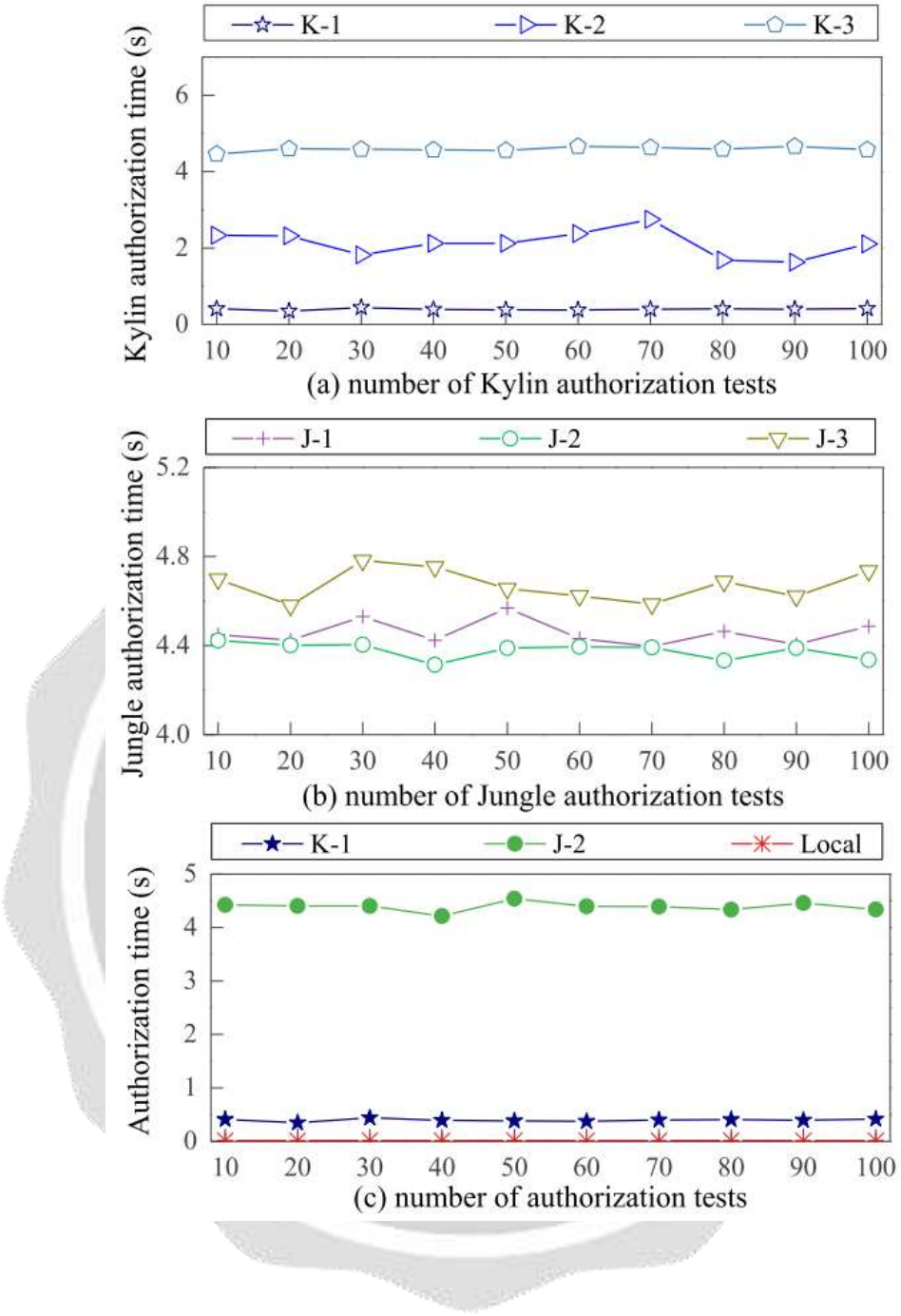

Fig -3: Comparison of authorization time, including Kylin, Jungle, and Local. (a) Kylin: K-1 is api-kylin.eoslaomao.com, K-2 is api-kylin.eosasia.one and K-3 is api.kylin.alohaeos.com. (b) Jungle: J-1 is jungle2.cryptolions.io, J-2 is jungle.eosam.sterdam.net, J-3 is api.jungle.alohaeos.com. (c) Jungle, Kylin and Local's authorized publish performance comparison.

5. CONCLUSION AND FUTURE ENHANCEMENTS

This paper designs an access control framework with privacy protection in cloud environment. All authorization-related transactions are posted by the user to blockchain. We implement the framework model based on the EOS blockchain and regards access permission and other information as an additional description of blockchain transactions. The experimental results show that only users with access rights can access

resources. So our solution can satisfy with confidentiality, integrity, availability, authenticity, and accountability, and can not only prevent attacks from external users but also prevent internal management attacks.

In this project we have implemented file access control for the specific users only in future we can extend for all domains and all kind of files with real cloud implementation.

6. REFERENCES

[1] Wei Zhou, Jiahui Ji, ‘‘A Blockchain-Based Access Control Framework for Secured Data Sharing in Industrial Internet,’’ IEEE Eighth International Conference on Advanced Cloud and Big Data, 978-1-6654-2313-7/20/$31.00 ,2019.

[2] LIANG TAN 1,2, NA SHI 1 , CAIXIA YANG 1 , AND KEPING YU 3,4, ‘‘A Blockchain-Based Access Control Framework for Cyber-Physical-Social System Big Data,’’ Global Information and Telecommunication Institute, Waseda University, Tokyo 169-8050, Japan, 2020.

[3] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, ‘‘Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach,’’ IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[4] Wenjuan Li, Jiyi Wu, Jian Cao, Nan Chen1, Qifei Zhang and Rajkumar Buyya, ‘‘Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions,’’ 1 Qianjiang College, Hangzhou Normal University, Hangzhou 310018, China, 2021.

[5] Sultan Algarni, Fathy Eassa, Khalid Almarhabi, Abduallah Almalaise, Emad Albassam, ‘‘Blockchain-Based Secured Access Control in an IoT System2. https://doi.org/10.3390/app11041772, 1772, 2021.

[6] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, ‘‘Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach,’’ IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[7] Y. Q. Zhang, X. F. Wang, X. F. Liu, and L. Liu, ‘‘Survey on cloud computing security,’’ J. Softw., vol. 27, no. 6, pp. 1328–1348, 2016.

[8] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, ‘‘Security and privacy in cloud computing: Vision, trends, and challenges,’’ IEEE Cloud Comput., vol. 2, no. 2, pp. 30–38, Mar. 2015, doi: 10.1109/MCC.2015.45.

[9] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, ‘‘NIST cloud computing reference architecture,’’ NIST Special Publication, vol. 500, no. 211, pp. 1–28, 2011.

[10] P. Mell and T. Grance, ‘‘The NIST definition of cloud computing,’’ Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. Special Publication 800-145, 2011.

[11] S. Namasudra and P. Roy, ‘‘Secure and efficient data access control in cloud computing environment: A survey,’’ Multiagent Grid Syst., vol. 12, no. 2, pp. 69–90, May 2016, doi: 10.3233/MGS-160244.

[12] Y. Wang, D. Zhang, and H. Zhong, ‘‘Multi-authority based weighted attribute encryption scheme in cloud computing,’’ in Proc. 10th Int. Conf. Natural Comput. (ICNC), Aug. 2014, pp. 1033–1038, doi: 10.1109/ICNC.2014.6975982.

[13] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, ‘‘Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation,’’ IEEE Trans. Ind. Appl., early access, Dec. 13, 2019, doi: 10.1109/TIA.2019.2959550.