OPTIMIZED GOVERNMENT DATA ACCESS THROUGH MULTI-ATTRIBUTE CENTERED IDENTITY AUTHENTICATION

Sadiya Fathima[1], Dr. Mohd Umar Farooq[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad,
sadiyeahfathima@gmail.com
[2]Professor, Department of CSE, Shadan Women's College of Engineering and Technology
umarfarooq.mohd@gmail.com

ABSTRACT

In the processing of massive data, Identity Authentication (IA) is a critical step in ensuring secure government data exchange. However, issues with key escrow, information leakage, and single points of failure are presented by the centralized IA approach that relies on a reliable third party. As a result, an efficient IA model built on multi-attribute centers is created here. The attribute authorization center first generates a private key for each attribute of a data requester. The data requester creates a personal private key after acquiring the attribute's private key. Second, a dynamic key generation method is proposed that regularly updates a data requester's key using blockchain technology and smart contracts. This reduces the possibility of privacy breaches, guarantees IA traceability, and prevents theft by external adversaries. Third, attribute field data of the data requester is saved using a combination of blockchain technology and interplanetary file systems to further reduce the cost of blockchain information storage and boost its effectiveness. Experimental results show that the proposed method ensures the privacy and security of identity information while outperforming similar authentication models in terms of communication and processing costs.

1. INTRODUCTION

In the digital era, government data has become an essential resource for improving coordination and building smart, service-oriented administrations, yet challenges such as scattered storage, weak security, and unreliable identity verification hinder effective sharing. Traditional authentication methods like centralized PKI and password systems rely on third-party trust, making them vulnerable to single points of failure, data breaches, and key escrow risks. To overcome these limitations, this study proposes a multi-attribute authorization center-based identity authentication system that distributes trust, enables dynamic key generation through blockchain and smart contracts, and integrates blockchain with the Interplanetary File System (IPFS) for secure storage. Additionally, Non-Interactive Zero-Knowledge Proofs (NIZKP) combined with elliptic curve cryptography ensure lightweight yet robust authentication, enhancing both security and efficiency in government data sharing.

OBJECTIVE OF THE STUDY

To address the issue of single points of failure in conventional centralized systems, this work introduces a multi-attribute authorization center architecture where each center generates private keys for specific attributes, allowing the data requester to create a personal key that remains hidden from third parties. To further enhance security, a dynamic key generation mechanism is integrated with blockchain and smart contracts, ensuring periodic updates, preventing key theft, and combining Ethereum with the Interplanetary File System (IPFS) for secure and efficient identity information storage. Additionally, identity verification of data requesters is achieved using a Non-Interactive Zero-Knowledge Proof (NIZKP) mechanism, supported by lightweight elliptic curve cryptography to provide efficient, privacy-preserving, and reliable authentication.

PROBLEM STATEMENT

The primary step in protecting departmental exchange of agency secrets is Id Assurance (IA). To prevent unauthorized access and use of important government data, security and consumer prevention measures are required. However, conventional authentication methods, such the well-known Public Key Infrastructure (PKI), cloud-driven trusted certificate authority, and current internet address allocation approach, are typically predicated on trust supplied by a third party. Three parties usually make up a traditional IA model, like the condensed form that is being presented: the data owner, the authorization center, and the data requester. The identity authorisation service receives a request for self-recognition from the data requester.

EXISTING SYSTEM

Current identity authentication systems rely heavily on centralized trusted parties, which makes them prone to security risks, inefficiencies, and misuse. Data stored in isolated departmental silos often becomes inconsistent and difficult to share. Most existing solutions use traditional encryption and access control techniques, but because they are centrally managed, they remain vulnerable to information leakage and key escrow problems.

Disadvantages of Existing System

- Centralized storage creates a single point of failure.
- Isolated departmental data reduces efficiency and consistency.
- Heavy reliance on trusted third parties increases risk of misuse.
- Information leakage and key escrow problems remain unresolved.

PROPOSED SYSTEMS

In the proposed system, the attribute authorization center first generates a private key for each attribute of the data requester. Using these attribute keys, the requester then creates a unique personal private key that is unknown to third parties, ensuring stronger confidentiality. To enhance security, a dynamic key generation algorithm is introduced, which integrates blockchain and smart contracts to periodically update requester keys. This not only prevents external theft but also ensures traceability of authentication activities and reduces risks of privacy leakage. Furthermore, blockchain is combined with the InterPlanetary File System (IPFS) to store attribute-related information. This hybrid design reduces blockchain storage costs, improves scalability, and provides efficient, tamper-resistant storage, thereby supporting more secure and reliable government data sharing.

Advantages of Proposed System

- Enhanced security for shared information.
- Distributed and reliable data storage.
- Improved efficiency of government data sharing.
- Reduced blockchain storage cost with IPFS integration.
- Stronger protection against key theft and misuse.

2. RELATED WORK

In this section, we review previous researches relevant to this article;

This paper proposes a correlation graph-based framework to support developers in selecting Web APIs for mobile application development. Since APIs vary widely in compatibility and functionality, developers often struggle to identify the most suitable combinations. The suggested method models API functions and compatibility relationships through a graph structure, enabling automated recommendations that match developer requirements. Evaluations on real-world datasets show that this approach improves the reliability and speed of API selection in app development. **[1]**

This study investigates intrusion detection in Internet of Things environments, where current systems suffer from a lack of balanced and sufficient attack data. The authors introduce a Hierarchical Adversarial Attack (HAA) technique that targets Graph Neural Network-based detection models. By using shadow networks, saliency maps, and Random Walk with Restart to identify vulnerable nodes, adversarial examples are created with minimal disturbance. Experimental results demonstrate that this attack can reduce the accuracy of advanced detection models such as GCN and JK-Net by over 30%, exposing serious vulnerabilities in IoT security. **[2]**

This article reviews authentication mechanisms in the Internet of Medical Things (IoMT), where healthcare services increasingly rely on connected devices. The survey organizes authentication solutions according to cloud, fog, and edge deployment models. It further maps out common security threats, compares existing techniques, and highlights gaps that need to be addressed. The work concludes with suggestions for advancing authentication practices in IoMT to ensure both privacy and system reliability. **[3]**

This conference paper examines security issues in Vehicle-to-Grid (V2G) technology, where electric vehicles interact with charging stations and grid controllers. Since communication occurs over open networks, ensuring confidentiality and stability is crucial. The proposed solution leverages blockchain for secure transaction management, selecting validators based on computational capacity and energy resources. A game theory-based mechanism is also used to balance peak and off-peak energy demand. Compared with earlier approaches, this design achieves stronger privacy protection and more efficient energy trading. **[4]**

This research focuses on privacy in smart grids and other critical infrastructures. Earlier methods that depended on centralized key management were limited by weak revocation capabilities and potential linkability issues. To resolve these limitations, the authors design a decentralized identity management system that relies on blind signatures and pseudonym revocation. This solution enhances unlinkability and eliminates reliance on central key authorities, making it suitable not only for smart grids but also for banking, healthcare, and e-voting environments. **[5]**

This paper considers the security of Wireless Body Area Networks (WBANs) in cloud-assisted healthcare systems. Since WBANs are resource-constrained and vulnerable to external attacks, the authors propose the Identity-Based Anonymous Authentication and Key Agreement (IBAAKA) protocol. The scheme provides user anonymity, mutual authentication, and low overhead, proving both efficient and secure for healthcare applications that depend on wearable technologies and remote monitoring. **[6]**

This study highlights the risks of centralized healthcare data storage, which can compromise security and long-term availability. To overcome these risks, the authors propose an architecture that combines blockchain with the Interplanetary File System (IPFS). This decentralized model allows patients and providers to securely share

and access medical data while ensuring resilience, privacy, and trust in healthcare information systems. **[7]**
This article presents a lightweight protocol known as Leakage-Resilient Identity-Based Mutual Authentication and Key Exchange (LR-IDMAKE), designed specifically for low-resource IoT devices. The protocol enables secure mutual authentication and session key generation while resisting continuous key leakage. Experiments on Raspberry Pi devices show extremely low computational cost (≈0.5 ms) and minimal communication overhead, making the protocol practical for constrained IoT environments. **[8]**
This research takes a theoretical perspective on secure communication. The authors investigate whether secure authentication capacity and forward secret key capacity can be computed for systems with privacy leakage and channel storage limitations. Using a computability framework, they demonstrate that these capacities are algorithmically incomputable for general discrete memoryless channels. This implies that neither exact values nor approximations can be determined, even under optimal coding strategies, setting fundamental limits on secure system design. **[9]**
This conference paper integrates blockchain technology into IoT systems to enhance authentication, access control, and data privacy. The architecture employs Ethereum smart contracts, consensus mechanisms, and immutable ledgers to improve system security. By decentralizing identity management and reducing dependence on central authorities, the model addresses weaknesses in conventional IoT frameworks. It also provides a more trustworthy basis for secure data exchange in applications such as smart cities and industrial IoT. **[10]**

3. METHODOLOGIES

Blockchain, with its decentralized and tamper-resistant structure, ensures secure and traceable data sharing by preventing large-scale breaches common in centralized systems. To optimize storage, the Interplanetary File System (IPFS) is integrated, where files are uniquely addressed through cryptographic hashes, enabling efficient retrieval and reducing storage costs. Alongside, bilinear pairing is employed to strengthen cryptographic operations such as identity-based encryption, while distributed key generation removes reliance on a single trusted party. In an (N,T) (N, T) (N,T) threshold scheme, attribute keys are collaboratively generated by multiple authorization centers, ensuring that no single entity can compromise the secret, thus enhancing security and fault tolerance.
The proposed system establishes a distributed identity authentication model for secure government data sharing. A data requester submits verified identity attributes such as name, ID, and department, which are confirmed by multiple authorization centers and then stored in IPFS. Partial attribute keys are issued, and the requester generates a personal key pair, with the public key recorded on the blockchain. Identity verification is then performed using Non-Interactive Zero-Knowledge Proofs, ensuring privacy while confirming legitimacy. Once validated, secure and efficient data exchange takes place between the requester and the data owner, enabling trusted interdepartmental collaboration.

MODULE DESCRIPTION:

Data Requester: the head of a government agency that makes a request to view data from other agencies. Through a smart contract, the data requester can identify the relevant data owner, verify their identity, and then request the necessary access.
Data Owner: The head of a government agency that supplies information to other agencies. Since the identification of the data requester is presumed to be reliable in this study, it is the data owner's responsibility to confirm its validity.
Attribute Set: To solve the problem of rigid single-factor authentication, the data requester creates an attribute set based on Mult attribute factors like name, employee number, and department number. These factors are then utilized to construct attribute keys.
Blockchain: Using the blockchain, the data owner confirms the identity of the person requesting the data. Large volumes of data cannot be stored on the blockchain since doing so results in transaction costs. As a result, we reduce costs by storing data hash values in the system.
Smart Contract: In order to control the time validity of the data requester's keys, this application is integrated with blockchain technology.
IPFS: It saves the data requester's attribute information and computes a distinct hash value for every attribute using the hash function. Blockchain and IPFS work together to save storage costs, guarantee data security, and store identification information.
Authorization Center: Several attribute authorization centers are used in the suggested architecture, and their job is to generate matching attribute keys for the data requester.
Government Data Sharing: The data requester uses the information to fulfill the department's requirements after receiving it from the data owner.

4. ALGORITHM

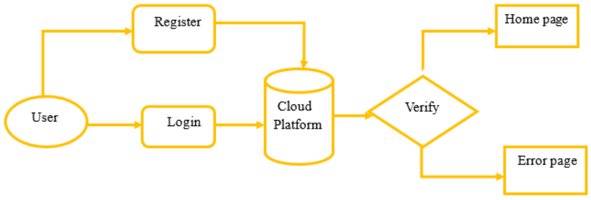
The algorithm presented here relies on a hybrid approach that combines attribute-based encryption with dynamic key management. In the initialization stage, multiple attribute authorization centers collaborate to generate the system master key. This is achieved through a polynomial-based threshold method, which is essentially derived from Shamir’s Secret Sharing. In this way, at least a threshold number of centers are required to jointly construct the master secret, ensuring that no single center can compromise the system's security. Pairing-based cryptography over cyclic groups is employed in this stage to set up the cryptographic environment needed for identity authentication.

Once the system parameters and master key are in place, the process moves to dynamic key generation. Each data requester generates a private key and then computes the corresponding public key using elliptic curve cryptography (ECC). The ECC-based key generation provides strong security while keeping the computation lightweight. Importantly, the scheme introduces the concept of a delay time, which defines the validity period of a public key. A smart contract on the blockchain is used to automatically enforce this delay time. When the set period expires, the smart contract invalidates the public key without requiring any manual intervention.

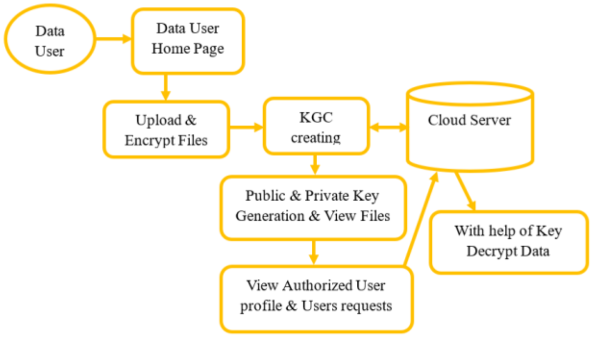
Through this design, the algorithm ensures that compromised or stolen keys become useless once they expire. The requester must generate new keys when needed, and any expired or revoked keys remain recorded in the blockchain history for transparency. This approach effectively combines pairing-based cryptography, Shamir's Secret Sharing, elliptic curve cryptography, and blockchain smart contracts into a dynamic identity authentication algorithm that enhances both security and resilience against key theft.

5. DATA FLOW DIAGRAM

Level 0



Level 1


Data User
Data User Home Page
Upload & Encrypt Files
KGC creating
Cloud Server
Public & Private Key Generation & View Files
With help of Key Decrypt Data
View Authorized User profile & Users requests

6. SYSTEM ARCHITECTURE

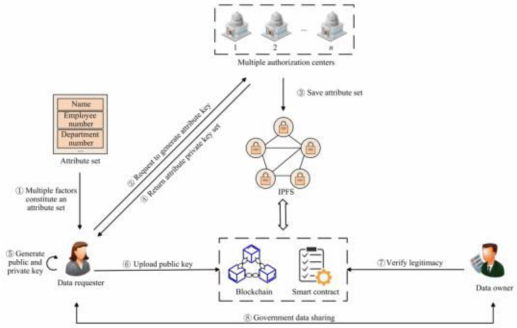

1
2
n
Multiple authorization centers
③ Save attribute set
Name
Employee number
Department number
Attribute set
② Request to generate attribute key
④ Return attribute private key set
IPFS
① Multiple factors constitute an attribute set
⑤ Generate public and private key
Data requester
⑥ Upload public key
Blockchain
Smart contract
⑦ Verify legitimacy
Data owner
⑧ Government data sharing

Fig. System Architecture Of The Project

This diagram shows a blockchain-based identity authentication system where user attributes are verified by multiple authorization centers, stored in IPFS, and linked to dynamically managed keys via smart contracts. The data requester uploads a public key to the blockchain, and the data owner verifies legitimacy before secure data sharing.

7. RESULTS

The proposed system was successfully implemented and evaluated for secure government data access using multi-attribute centered identity authentication. The application provides an organized interface where data owners can upload encrypted files and define access policies, while data users can submit access requests. Authentication is enforced through secret code verification and attribute key validation, with attribute keys securely delivered to users via email. Once verification is completed, authorized users gain secure access to the requested files. The results confirm that the system effectively prevents unauthorized access, enhances data confidentiality, and establishes a reliable authentication mechanism for government data sharing.

8. FUTURE ENHANCEMENT

In the future, the focus will be on incorporating a fair incentive and penalty mechanism for blockchain nodes to enhance consensus reliability and efficiency. Such an approach will help preserve the legal soundness of the system while protecting citizens' privacy during government data sharing. Furthermore, improvements in scalability, adaptability, and security will be prioritized so that the framework can effectively cope with the growing demands and complexities of modern digital governance. These enhancements will contribute to building a more secure, efficient, and citizen-friendly platform for inter-departmental data exchange.

9. CONCLUSION

This research introduced a secure framework for government data exchange by emphasizing the legitimacy of data requesters' identities. The proposed identity authentication model, based on multiple authorization centers, effectively mitigates the key escrow problem while ensuring data protection. Although data requesters need to generate their own private keys, the use of dynamic key generation with NIZKP strengthens security by allowing public keys to be updated automatically. Experimental evaluation confirmed that the system achieves lower communication and computational overhead compared to existing approaches. While the design demonstrates strong results, further investigation is needed to address issues such as secure data transmission in subsequent phases and potential risks caused by malicious nodes in the blockchain network.

10. REFERENCES

1. L. Qi, W. Lin, X. Zhang, W. Dou, X. Xu and J. Chen, "A correlation graph-based approach for personalized and compatible web APIs recommendation in mobile APP development", IEEE Trans. Knowl. Data Eng., vol. 35, no. 6, pp. 5444-5457, 2023.
2. X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. K. Wang, "Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system", IEEE Internet Things J., vol. 9, no. 12, pp. 9310-9319, 2022.
3. P. Zhang, M. Zhou, Q. Zhao, A. Abusorrah and O. O. Bamasag, "A performance-optimized consensus mechanism for consortium blockchains consisting of trust-varying nodes", IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2147-2159, 2021.
4. Z. Rahman, I. Khalil, X. Yi and M. Atiquzzaman, "Blockchain-based security framework for a critical industry 4. 0 cyber-physical system", IEEE Commun. Mag., vol. 59, no. 5, pp. 128-134, 2021.
5. W. Diffie and M. Hellman, "New directions in cryptography", IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644-654, 1976.
6. W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu and C. Su, "Block SLAP: Blockchain-based secure and lightweight authentication protocol for smart grid", Proc. IEEE 19 th Int. Conf. on Trust Security and Privacy in Computing and Communications (TrustCom) , pp. 1332-1338, 2020.
7. G. Li, X. Ren, J. Wu, W. Ji, H. Yu, J. Cao, et al., "Blockchain-based mobile edge computing system", Inf. Sci., vol. 561, pp. 70-80, 2021.
8. M. Di, G. Galatro, M. Longo, F. Postiglione and M. Tambasco, "HASFC: A MANO-compliant framework for availability management of service chains", IEEE Commun. Mag., vol. 59, no. 6, pp. 52-58, 2021.
9. Y. M. Tseng, J. L. Chen and S. S. Huang, "A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices", Comput. Networks, vol. 196, pp. 108246, 2021.
10. H. Boche, R. F. Schaefer, S. Baur and H. V. Poor, "On the algorithmic computability of the secret key and authentication capacity under channel storage and privacy leakage constraints", IEEE Trans. Signal Process., vol. 67, no. 17, pp. 4636-4648, 2019.
11. M. A. Khan, I. U. Din, T. Majali and B. S Kim, "A survey of authentication in internet of things-enabled healthcare systems", Sensors, vol. 22, no. 23, pp. 9089, 2022.
12. Y. Yu, Y. Li, J. Tian and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things", IEEE Wireless Commun., vol. 25, no. 6, pp. 12-18, 2018.
13. M. Asghar, R. R. M. Doss and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs", Proc. 28 th Int. Telecommunication Networks and Applications Conf. (ITNAC) , pp. 1-3, 2018.
14. F. Marino, C. Moiso and M. Petracca, "PKIoT: A public key infrastructure for the internet of things", Trans. Emerg. Telecommun. Technol., vol. 30, no. 10, pp. e3681, 2019.
15. H. Qiu, M. Qiu and R. Lu, "Secure V2X communication network based on intelligent PKI and edge computing", IEEE Network, vol. 34, no. 2, pp. 172-178, 2020.
16. J. Arm, P. Fiedler and O. Bastan, "Offline access to a vehicle via PKI-based authentication", Proc. Int. Conf. on Computer Safety Reliability and Security, pp. 76-88, 2021.
17. D. D. F. Maesa and P. Mori, "Blockchain 3. 0 applications survey", J. Parallel Distrib. Comput., vol. 138, pp. 99-114, 2020.
18. C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen, et al., "Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach", IEEE Network, vol. 35, no. 1, pp. 130-137, 2021.
19. S. Guo, X. Hu, S. Guo, X. Qiu and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system", IEEE Trans. Ind. Inf., vol. 16, no. 3, pp. 1972-1983, 2020.
20. A. Barnawi, S. Aggarwal, N. Kumar, D. M. Alghazzawi, B. Alzahrani and M. Boulares, "Path planning for energy management of smart maritime electric vehicles: A blockchain-based solution", IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 2282-2295, 2023.
21. S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid", IEEE Trans. Ind Inf., vol. 16, no. 5, pp. 3548-3557, 2020.
22. J. S. Shin, S. Lee, S. Choi, M. Jo and S. H. Lee, "A new distributed decentralized privacy-preserving ID registration system", IEEE Commun. Mag., vol. 59, no. 6, pp. 138-144, 2021.

23. J. Liu, Z. Zhang, X. Chen and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless Body area networks", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332-342, 2014.

24. M. Kumar and S. Chand, "A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network", IEEE Syst. J., vol. 15, no. 2, pp. 2779-2786, 2021.

25. S. Jegadeesan, M. Azees, N. R. Babu, U. Subramaniam and J. D. Almakhles, "EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)", IEEE Access, vol. 8, pp. 48576-48586, 2020.

26. X. Jia, D. He, N. Kumar and K. K. R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing", IEEE Syst. J., vol. 14, no. 1, pp. 560-571, 2020.

27. K. Zarour, O. A. Bounab, Y. Marir and I. Boumezbeur, "Blockchain-based architecture centred patient for decentralised storage and secure sharing health data", Int. J. Electron. Healthcare., vol. 12, no. 2, pp. 170-190, 2022.

28. H. Chai, S. Leng, J. He, K. Zhang and B. Cheng, "Cyber Chain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles", IEEE Trans. Veh. Technol., vol. 71, no. 5, pp. 4620-4631, 2022.

29. J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy", J. Parallel Distrib. Comput., vol. 164, pp. 152-167, 2022.

30. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, [online] Available: http://bitcoin.org/bitcoin.pdf.

31. Q. Feng, D. He, S. Zeadally, M. K. Khan and N. Kumar, "A survey on privacy protection in blockchain system", J. Network Comput. Appl., vol. 126, pp. 45-58, 2019.

32. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems", Proc. Int. Conf. on the Theory and Applications of Cryptographic Techniques, pp. 295-310, 1999.

33. R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM, vol. 21, no. 2, pp. 120-126, 1978.

34. Cygwin: Linux environment emulator for windows, 2022.

35. J. A. Fernandez-Carrasco, T. Egues-Arregui, F. Zola and R. Orduna-Urrutia, "ChronoEOS: Configuration control system based on EOSIO blockchain for on-running forensic analysis", Proc. Int. Congress on Blockchain and Applications, pp. 37-47, 2022.