WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Certificateless Public Cloud Data Integrity Auditing Scheme Enhanced by Blockchain Technology

Mr. S. Saravana Kumar[1], G. Gopika[2], R. Keerthana[3], M. Logasri[4]

[1] Assistant Professor, Department of Information Technology Dhanalakshmi Srinivasan engineering college (Autonomous), Perambalur, Tamil Nadu.
[2,3,4] UG-Department of Information Technology Dhanalakshmi Srinivasan engineering college (Autonomous), Perambalur, Tamil Nadu.
E. Mail: saravana.coolya@gmail.com [1], gopikagkn1@gmail.com[2], kkeeethi2002@gmail.com[3],logasrilogasri6@gmail.com[4],

ABSTRACT

Traditional certificate validation processes are susceptible to security risks and tampering. Certificates stored in centralized databases or physical copies are vulnerable to unauthorized access, alteration, or forgery. The proposed system for a blockchain-based certificate verification system incorporating a link method with OTP (One-Time Password) access format and verifier details checked using hash values outlines a robust and secure approach to certificate validation. In this innovative system, the certificates are intricately linked to the blockchain through a specialized link method, ensuring a direct and immutable connection between the certificate and the blockchain transaction. During the verification process, the OTP access format is employed to authenticate the user attempting to validate the certificate link. Simultaneously, the hash values of the certificate and verifier details are cross-referenced with the corresponding values stored on the blockchain. Any inconsistencies or tampering with the certificate information trigger a mismatch in the hash values, promptly signalling potential fraudulent activity. This blockchain-based certificate verification system, incorporating a link method with OTP access format and hash value verification, establishes a highly secure and transparent framework for authenticating certificates, ensuring the integrity of the certification process.

KEYWORDS: Blockchain Integration, Link Method, OTP Generation and Verification, Verifier Details check, Certificate submission, Certificate Retrieval, User Management.

I.INTRODUCTION

A Security certificate is a small data file used as an Internet security technique through which the identity, authenticity and reliability of a website or web application is established. A security certificate is used as a means to provide the security level of a website to general visitors Internet service providers (ISPs) and Web servers. A security certificate is also known as a digital certificate and as a Secure Socket Layer (SSL) certificate. Blockchain technology is a decentralized, distributed ledger system that securely records transactions across multiple computers in a way that is transparent, immutable, and resistant to tampering. At its core, a blockchain consists of blocks of data that are cryptographically linked and chronologically ordered. Each block contains a batch of transactions, and once added to the chain, it becomes permanent and cannot be altered retroactively without altering all subsequent blocks, making the data inherently resistant to modification. verify the integrity of the data without relying on a central authority. Blockchain technology eliminates the need for intermediaries in various fields, such as finance, supply chain management, healthcare, and more, by enabling peer-to-peer transactions and smart contracts. Smart contracts are self-executing contracts with the terms of the agreement directly written into code, automating and enforcing the terms of the agreement without the need for intermediaries. Overall, blockchain technology has the potential to revolutionize industries by providing secure, transparent, and efficient solutions to various challenges, fundamentally changing the way transactions and data are managed and verified.

II. PURPOSE

The Scope of this project is to provide a secure and transparent method for verifying the integrity of data stored in a public cloud environment. By leveraging blockchain technology, the scheme aims to eliminate the need for traditional certificate-based authentication, reducing overhead and potential management. Additionally, the use of blockchain ensures that audit trails are tamper- proof and immutable, enhancing data integrity and providing a cloud. This scheme addresses concerns related to data security, trustworthiness.

III. OBJECTIVE

To develop a robust and secure certificate verification system using blockchain technology. The proposed system incorporates a specialized link method that intricately connects certificates to the blockchain, ensuring immutability and direct association between certificates and blockchain transactions. Additionally, the system employs OTP access format to authenticate users during the verification process, adding an extra layer of security. Verifier details are also checked .

IV. EXISTING SYSTEM

Manual verification processes further exacerbate the inefficiencies and security risks associated with centralized systems. These processes typically involve time-consuming communication with issuing authorities to This immutability ensures trust and transparency in transactions, as all participants can verify the integrity of the data without relying on a central authority. Validate the authenticity of certificates. Such procedures lack real-time efficiency, leading to delays in verifying credentials and potentially hindering critical decision-making processes. Additionally, manual verification is labour-intensive and prone to human error, increasing the likelihood of overlooking fraudulent certificates or inaccurately validating legitimate ones. The shortcomings of existing certificate validation systems underscore the urgent need for innovative solutions that address the inherent limitations of centralized databases and manual verification processes. Blockchain technology offers a promising alternative by providing a decentralized, tamper-resistant framework for storing and verifying certificate data. By leveraging blockchain, certificate validation systems can eliminate the need for centralized databases, thereby mitigating the risks associated with single points of failure and unauthorized access. Additionally, blockchain enables the implementation of smart contracts, which automate and streamline the verification process, enhancing efficiency and reducing reliance on manual intervention. Furthermore, blockchain-based certificate validation systems offer enhanced security through cryptographic techniques such as hashing and encryption. Certificate data stored on the blockchain is encrypted and linked to a unique cryptographic hash, ensuring its integrity and immutability. Verification of certificates can be performed in real-time by querying the blockchain, eliminating the need for time-consuming communication with issuing authorities. Moreover, blockchain-based systems can incorporate additional layers of security, such as multi-factor authentication or biometric verification, to further enhance the authenticity and trustworthiness of validated certificates.

DISADVANTAGES

- Specialized Link Method Complexity
- Verification Process Complexity
- Dependence on blockchain technology

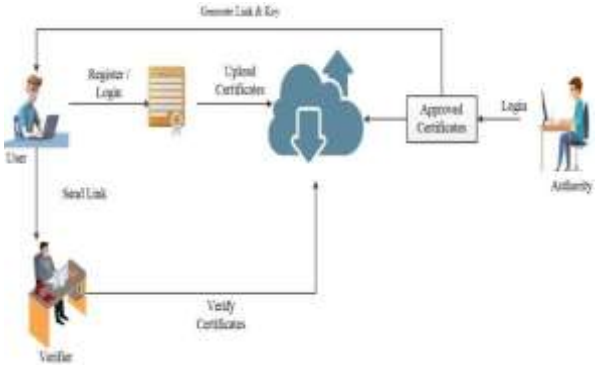
V. PROPOSED SYSTEM

The proposed OTP (One-Time Password) process-based certificate validation system leveraging blockchain technology represents a significant advancement in the security and integrity of certificate validation processes. Traditional methods of certificate validation are fraught with vulnerabilities, including security risks, tampering, and unauthorized access, necessitating a more robust solution. In this innovative system, certificates are intricately linked to the blockchain through a specialized link method, ensuring an immutable and direct connection between the certificate and the underlying blockchain transaction. This linkage enhances the transparency and trustworthiness of certificate validation, as all transactions are recorded and verified on the blockchain, making them resistant to tampering or alteration. Moreover, the integration of OTP access into the validation process adds an additional layer of security by enhancing user authentication. OTPs are temporary passwords that are dynamically generated and valid for only a single use or a short period, significantly reducing the risk of unauthorized access. By requiring users to input a unique OTP during the validation process, the system fortifies itself against potential security breaches and unauthorized attempts to access or manipulate certificate data. Verification of certificates can be performed in real-time by querying the blockchain, eliminating the need for time- consuming communication with issuing authorities. Moreover, blockchain-based biometric verification, to further enhance the authenticity and trustworthiness of validated certificates Any discrepancies or tampering with certificate information are immediately detected through a mismatch in hash values.

ADVANTAGES

- Intricate Link Method for Immutability
- Cross-Referencing Hash Values for Accuracy
- Transparent and Traceable Transaction

SYSTEM ARCHITECTURE



VI. FUTURE ENHANCEMENT

In the future, the proposed blockchain- based certificate verification system could include the integration of advanced cryptographic techniques for enhanced security and privacy. This could involve implementing zero-knowledge proofs or homomorphic encryption to allow verification without revealing sensitive information.

VII. CONCLUSION

The proposed blockchain-based certificate verification system presents a comprehensive and secure solution to the challenges of certificate validation. By leveraging blockchain technology, the system ensures the immutability and transparency of certificate transactions, enhancing trust and reliability in the certification process. The integration of a specialized link method, OTP access format, and hash value verification adds layers of security, effectively mitigating the risk of fraudulent activities such as counterfeiting or tampering with certificates.

REFERENCE

1. R. Tapwal, S. Misra and S. K. Pal, "CartelChain: A secure communication mechanism for heterogeneous blockchains", Proc. IEEE Int. Conf. Commun., pp. 5250-5255, 2022.
2. W. Qin, S. Chen and M. Peng, "Recent advances in industrial Internet: Insights and challenges", Digit. Commun. Netw., vol. 6, no. 1, pp. 1-13, 2020.
3. M. Wang, L. Rui, Y. Yang, Z. Gao and X. Chen, "A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network", IEEE Trans. Netw. Service Manag., vol. 19, no. 3, pp. 2664-2676, Sep. 2022.
4. S. Wang, H. Li, J. Chen, J. Wang and Y. Deng, "DAG blockchain-based lightweight authentication and authorization scheme for IoT devices", J. Inf. Security Appl., vol. 66, May 2022.
5. G. Xu, J. Dong, C. Ma, J. Liu and U. G. O. Cliff, "A certificateless signcryption mechanism based on blockchain for edge computing", IEEE Internet Things J., vol. 10, no. 14, pp. 11960-11974, Jul. 2023.
6. S. Zhang, Y. Liu, Y. Xiao and R. He, "A trust based adaptive privacy preserving authentication scheme for VANETs", Veh. Commun., vol. 37, Oct. 2022.
7. J. Liu, J. Zhao, H. Huang and G. Xu, "A novel logistics data privacy protection method based on blockchain", Multimedia Tools Appl., vol. 81, no. 17, pp. 23867-23887, 2022.
8. G. Xu, Y. Liu and P. W. Khan, "Improvement of the DPoS consensus mechanism in blockchain based on vague sets", IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4252-4259, Jun. 2020.
9. M. Shen et al., "Blockchain-assisted secure device authentication for cross-domain industrial IoT", IEEE J. Sel. Areas Commun., vol. 38, no. 5, pp. 942-954, May 2020.
10. L. Deng and R. Gao, "Certificateless two-party authenticated key agreement scheme for smart grid", Inf. Sci., vol. 543, pp. 143-156, Jan. 2021.