JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ORGANIZATIONAL DATA STORAGE SYSTEM USING BLOCKCHAIN TECHNOLOGY

Ms.N.Maragatham, Kankanala Navya, Dasu Sai Deepak, Bodduluri Harshitha

JANSONS INSTITUTE OF TECHNOLOGY

ABSTRACT:

In this blockchain-based project, we harness decentralized ledger technology to safeguard sensitive organizational information and facilitate secure access among authorized personnel within our organization. Records are protected and accessible within the blockchain framework. Organizational data, including proprietary documents, operational insights, and strategic plans, is securely stored in cryptographic blocks, each linked to the preceding one. These blocks ensure data integrity and confidentiality, with each piece of information associated with a digital identity representing authorized personnel or departments. This innovative approach not only enhances the security of organizational data but also enables swift retrieval from any location, at any time, fostering information sharing and collaboration while upholding stringent security standards. Consequently, blockchain technology assumes a pivotal role in modernizing organizational data management, reinforcing security measures, and boosting operational efficiency.

Keywords: Blockchain-based project, Decentralized ledger technology, Cryptographic blocks, Data integrity, Confidentiality, Digital identity, Security protocols.

INTRODUCTION

Within the realm of Security information management, both proposed and currently operational blockchain projects provide clues for useful applications in libraries and information organizations. This should not be too surprising given the close historical relationship between Private information management and librarianship. Within Security, blockchain continues to rapidly move from theoretical discussions to specific applications impacting areas as diverse as pharmacology and Private device supply chains, recruitment of Organizations for clinical trials, and improving security and interoperability of Private devices. In the realm of Security care, blockchain is a reality now. This is partly possible because of standards for Private information interoperability, equivalent conceptually to those in library and information science.

RELATED WORK

The implementation of the proposed blockchain-based organization data management system involves several key steps to ensure the seamless integration and functionality of the innovative solution. First and foremost, the foundational aspect is the establishment of the blockchain network. This involves deploying nodes across the organization infrastructure, forming a decentralized network that will collectively manage and validate cryptographic blocks. Smart contracts are then programmed to govern access control, ensuring that only authorized personnel or units with validated digital identities can contribute to or retrieve information from the blockchain.

Once the blockchain infrastructure is in place, the integration of organization records into cryptographic blocks commences. Classified documents, operational intelligence, and strategic plans are systematically encrypted and added to the tamper-proof chain. The linking of each block to the previous one establishes a chronological and secure ledger that preserves the integrity and confidentiality of organization data. Advanced cryptographic techniques, such as digital signatures, further fortify the security of the information stored within the blocks.

To enhance usability and facilitate secure access, a user-friendly interface is developed for authorized personnel. This interface ensures efficient interaction with the blockchain network, allowing seamless and instantaneous retrieval of military information from any location. User authentication mechanisms are integrated, ensuring that only individuals or units with the appropriate credentials can access specific segments of the blockchain.

Throughout the implementation phase, rigorous testing is conducted to validate the resilience and security of the blockchain-based system. This includes simulated cyber-attacks, stress testing, and validation of the smart contracts. Feedback from organization personnel is actively sought to fine-tune the user interface and address any usability concerns.

Upon successful implementation, the blockchain-based organization data management system stands ready to revolutionize how organization records are handled. The tamper-proof nature of the blockchain ensures data integrity, while decentralized access allows for enhanced collaboration and information sharing. This transformative solution not only mitigates the vulnerabilities associated with centralized systems but also elevates the overall security and efficiency of organization intelligence and record- keeping in contemporary war fare scenarios.

EXISTING SYSTEM

Currently, our organization relies on traditional centralized databases and systems for storing and managing sensitive information. Access to this data is typically restricted through conventional authentication methods, such as username and password combinations. However, this centralized approach poses security risks due to potential vulnerabilities in the system and the need to trust a single authority for data integrity and access control. Additionally, retrieving and sharing information across different departments or locations can be cumbersome and time-consuming.

Drawbacks

Security Vulnerabilities:

Centralized organization data systems are more prone to security breaches, given their single-point-of-entry nature. This makes them susceptible to unauthorized access and potential data leaks.

Data Tampering Risks:

The centralized structure increases the risk of data tampering, as malicious actors may exploit vulnerabilities to alter organization records. This compromises the integrity of crucial information.

Limited Accessibility:

Traditional systems face challenges in providing seamless and secure access to organization data across diverse geographical locations. This limitation hampers the timely sharing of information and collaborative efforts.

Hierarchical Structure:

The hierarchical nature of centralized systems can lead to inefficiencies and delays in accessing vital organization information, particularly when quick decision-making is crucial.

PROPOSED SYSTEM

In the proposed system, we aim to implement a blockchain-based solution to revolutionize our organization's data management practices. By leveraging decentralized ledger technology, we will ensure that sensitive information is securely stored in cryptographic blocks, with each block linked to the previous one to maintain data integrity. Access to this information will be governed by smart contracts, enabling fine-grained access control based on predefined permissions and digital identities. Authorized personnel will be able to retrieve and share data instantaneously from anywhere, at any time, facilitating seamless collaboration and improving operational efficiency. This innovative approach not only fortifies the security of our organizational data but also streamlines information management processes, paving the way for enhanced productivity and effectiveness across the organization.

FHIR – Fast Security Interoperability Resources – is a developing standard that defines data formats and elements, along with providing publicly accessible application programming interfaces (APIs) for the purpose of exchanging electronic Security records (EHR). It is the Security care equivalent of a completely normalized MARC with predefined access interfaces. FHIR offers the potential to extend EHRs outside the constructs of traditional electronic Security care systems to mobile and cloud-based applications, organizational device integration, and flexible/customized Security workflows.

This flexibility is important because blockchain technology will allow Security data to be collected over the life of an individual. The benefit to the staff is a complete organizational record that accurately details one's lifetime Security history. As the staff could make this data available to any Security care provider, individual Security outcomes should be improved. Furthermore, agglomerated data could also improve research as rich base of information to be analysed to help predict future Security concerns at the population level.

A critical factor in this approach is the staff has control over who has access to their data. They can provide access at varying levels, from full access to all of their Security records to just a limited subset based on the application. A staff visiting their dentist can restrict their Security data to just those aspects that would be relevant for dental practice, for example. Similarly, staff participating in research, such as drug trials, can limit the amount and type of data that is made available to researchers as well as what personal information the researchers can subsequently share. This same type of disclosure scheme could be applied within bibliographic systems to allow the patron to control their personal information as appropriate to the context, such as opting out of sharing circulation or electronic journal access information from recommender systems.

Currently, much work is being done on creating an environment where, eventually, a common database of staff information could be built using blockchain technology. This same idea could be applied to libraries and information organizations through the use of a common database of user information allowing for a common patron database that would allow universal access across library systems.

Merits

- Enhanced Security
- Immutable Data Integrity
- Secure Access Control
- Decentralized Accessibility

MODULE DESCRIPTION

This proposed system is capable of below 5 functions using the below methods written:

1. addUser - Adds a new user in the system and stores all of it's Security information in the Blockchain.

2. getUser - At any point of time and place, user details can be fetched using this method.

3. addOrganizationRecord - This method adds all the Organization record in Blockchain and related documents like Lab reports etc in IPFS.

4. getOrganizationRecord - This method can be invoked to get the details Organization records stored on Blockchain.

5. getOrganizationRecordDetails - This method can be invoked to get the details Organization records

SHA-256:

A **cryptographic hash** (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text A hash is not 'encryption' – it cannot be decrypted back to the original text (it is a 'one-way' cryptographic function, and is a fixed size for any size of source text). This makes it suitable when it is appropriate to compare 'hashed' versions of texts, as opposed to decrypting the text to obtain the original version.

Such applications include hash tables, integrity verification, challenge handshake authentication, digital signatures, etc.

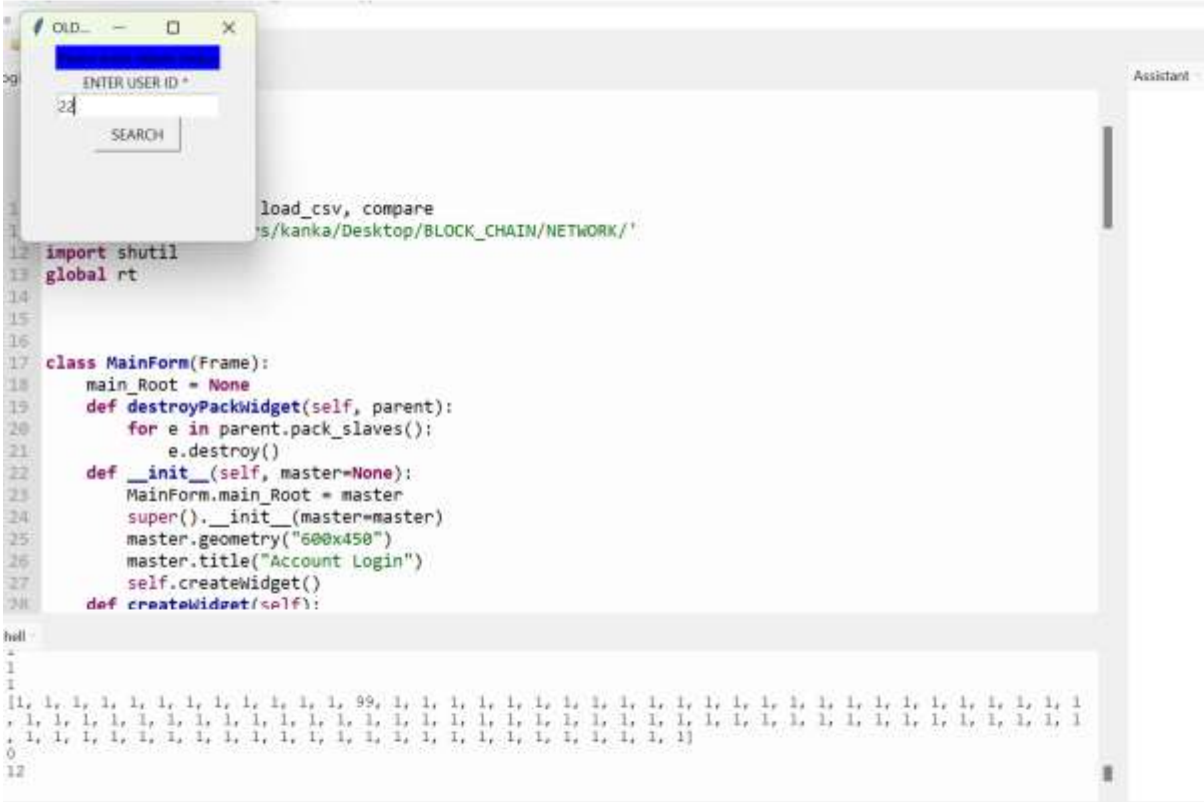
- '*challenge handshake authentication*' (or 'challenge hash authentication') avoids transmissing passwords in 'clear' – a client can send the hash of a password over the internet for validation by a server without risk of the original password being intercepted
- *anti-tamper* – link a hash of a message to the original, and the recipient can re-hash the message and compare it to the supplied hash: if they match, the message is unchanged; this can also be used to confirm no data-loss in transmission
- *digital signatures* are rather more involved, but in essence, you can sign the hash of a document by encrypting it with your private key, producing a digital signature for the document. Anyone else can then check that you authenticated the text by decrypting the signature with your public key to obtain the original hash again, and comparing it with their hash of the text.

Note that hash functions are not appropriate for storing encrypted passwords, as they are designed to be fast to compute, and hence would be candidates for brute-force attacks. Key derivation functions such as bcrypt or scrypt are designed to be slow to compute, and are more appropriate for password storage (npm has bcrypt and scrypt libraries, and PHP has a bcrypt implementation with password_hash).

SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2), and is one of the strongest hash functions available. SHA-256 is not much more complex to code than SHA-1, and has not yet been compromised in any way. The 256-bit key makes it a good partner-function for AES. It is defined in the NIST (National Institute of Standards and Technology) standard 'FIPS 180-4'.

RESULT

Successfully implemented blockchain-based system for secure data management, ensuring integrity and confidentiality. Enhanced security measures including encryption techniques and immutable logging mechanisms. Improved operational efficiency by providing instant, secure access to critical information. Identified significant market potential across diverse industries and global reach. Recommendations include continuous research, potential partnerships, and consideration of stakeholder feedback for further enhancement.



CONCLUSION

Security systems of the 21st century will consist of various devices connecting Organizations (e.g., remote Security services, wearable devices, etc.) with their caregivers. These systems generate data continuously and can be subject to malicious attacks while in transmission at various levels of the underlying communication network. The blockchain technology is gaining significant attention from individuals, as well as organizations of nearly all kinds and dimensions. It is capable of transforming the traditional industry with its features, which include decentralization, anonymity, persistency, and auditability. In future the network consists of nodes and computers that are spatially separated, there is a need for synchronization mechanisms to identify the order of block additions. So the further research on innovative solutions that promote blockchain as a service that allows various parties (networks, devices, users, etc.)

REFERENCES

1. Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, Mohamed Abid, HealthBlock: A secure blockchain-based healthcare data management system, Computer Networks, Volume 200, 2021, 108500,ISSN1389-1286,

https://doi.org/10.1016/j.comnet.2021.108500.(https://www.sciencedirect.com/science/article/pii/S1389128621004382)

2. I. T. Javed, F. Alharbi, T. Margaria, N. Crespi and K. N. Qureshi, "PETchain : A Blockchain-Based Privacy Enhancing Technology," in IEEE Access, vol. 9, pp. 41129-41143, 2021, doi: 10.1109/ACCESS.2021.3064896.keywords: {Blockchain; Data privacy; Encryption; Privacy; Cryptography; Access control; Differential privacy; Blockchain; Ethereum; privacy enhancing technology; privacy preservation; smart contract }

3. Zheng, BK., Zhu, LH., Shen, M. et al. Scalable and Privacy-Preserving Data Sharing Based on Blockchain. J. Comput. Sci. Technol. 33, 557–567 (2018). https://doi.org/10.1007/s11390-018-1840-5

4. Le Nguyen, B., Lydia, E. L., Elhoseny, M., Pustokhina, I., Pustokhin, D. A., Selim, M. M., ... & Shankar, K. (2020). Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua, 65(1), 87-107.

5. L. Liu and B. Xu, "Research on information security technology based on blockchain," 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 2018, pp. 380-384, doi: 10.1109/ICCCBDA.2018.8386546. keywords: {Peer-to-peer computing; Authentication; Distributed databases; blockchain; distributed; timestamp; decentralized; information security},

6. Chandramma R,Arif Al,Syed Rashid Anwar,Bhawna Chahar,AybarsOztuna,BadriaSulaimanAlfurhood,"A Review on Employment Opportunity in Defence Sector Using Blockchain Technology",2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)

7. Alaa Haddad,Mohamed Hadi Habaebi,Md Rafiqul Islam,Suriza Ahmad Zabidi,"Blockchain for Security Private Records Management System with Sharing Control",2021 IEEE 7th International Conference on Smart Instrumentation Measurement and Applications (ICSIMA)

8. Tanesh Kumar,Vidhya Ramani,Ijaz Ahmad,An Braeken,Erkki Harjula,Mika Ylianttila,"Blockchain Utilization in Security: Key Requirements and Challenges",2018 IEEE 20th International Conference on e-Security Networking Applications and Services (Securitycom)

9. Shashank Chauhan,Harsh Kripal Singh Tanwar,"Application of Blockchain Technology in Security: A Systematic Review",2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)

10. Mogi Jordan Christ,Rahmanto Nikolaus Permana Tri,Wiranto Chandra,Wang Gunawan,"Exploring Blockchain in Security Industry",2019 International Conference on ICT for Smart Society (ICISS)

11. Chang Liu,Shu Zhou,Irena Vodenska,Lou Chitkushev,Guanglan Zhang,Reza Rawassizadeh,"Blockchain Technology in Security: A Scientific and Technological Driving Force",2021 IEEE 34th International Symposium on Computer-Based Private Systems (CBMS)

12. Matthias Mettler,"Blockchain technology in Security: The revolution starts here",2016 IEEE 18th International Conference on e-Security Networking Applications and Services (Securitycom)

13. Barkha Kakkar,Prashant Johri,"Blockchain: A Security Perspective",2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)

14. Akruti Sinha,Akshet Patel,Mukta Jagdish,"Application of Blockchain in Security",2022 First International Conference on Artificial Intelligence Trends and Pattern Recognition (ICAITPR)

15. Ambuj Kumar Agarwal,Raj Gaurang Tiwari,Rajesh Kumar Kaushal,Naveen Kumar,"A Systematic Analysis of Applications Of Blockchain in Security",2021 6th International Conference on Signal Processing Computing and Control (ISPCC)