e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:06/June-2023 Impact Factor- 7.868 www.irjmets.com

E-DASTAVEZ

Ishan Mishra[*1], Dr. Santosh Kumar Dwivedi[*2], Mr. Shadab Ali[*3]

[*1]UG Student Of Department Of BCA, Shri Ramswaroop Memorial College Of Management Lucknow, Uttar Pradesh, India.

[*2]Professor, Head Of Department Of BCA, Shri Ramswaroop Memorial College Of Management Lucknow, Uttar Pradesh, India.

[*3]Assistant Professor, Department Of BCA, Shri Ramswaroop Memorial College Of Management Lucknow, Uttar Pradesh, India.

DOI : https://www.doi.org/10.56726/IRJMETS41324

ABSTRACT

Document verification is a critical process that ensures the authenticity and integrity of important records. Traditional verification methods often suffer from inefficiencies, vulnerabilities, and lack of transparency. This research paper introduces the concept of "E-Dastavez," a document verification system that utilises blockchain technology and the Internet of Things (IoT) with fingerprint and human verification. The objective of this study is to propose a secure and efficient solution that addresses the challenges associated with document verification. The research explores the integration of blockchain technology, IoT devices, fingerprint recognition, and human verification techniques. The findings demonstrate the effectiveness and potential applications of the proposed system in enhancing document verification processes.

I. INTRODUCTION

Document verification is a critical aspect in various domains, including government agencies, educational institutions, financial organisations, healthcare systems, and employment agencies. The verification of documents and the authentication of individuals are essential for ensuring trust, security, and regulatory compliance. However, traditional methods of document verification often rely on manual processes, which are time-consuming, error-prone, and vulnerable to fraudulent activities.

To address these challenges, this research paper proposes the utilisation of blockchain technology and Internet of Things (IoT) devices to enhance the document verification process. Blockchain, as a decentralised and immutable ledger, provides a secure and transparent platform for storing and verifying documents. By employing cryptographic hashing techniques, the integrity of documents can be ensured, and a tamper-resistant record of verification activities can be maintained. Additionally, the integration of IoT devices, specifically fingerprint scanners, offers a robust and reliable biometric modality for document and human verification.

The proposed system aims to leverage the power of blockchain and IoT to create a secure, efficient, and reliable document verification platform. By incorporating fingerprint recognition technology, the system enables accurate and convenient verification of both documents and individuals. This research paper will outline the workflow of the proposed system, analyze its effectiveness, and discuss the future implications and potential advancements in this field.

II. WORKFLOW

The proposed system follows a well-defined workflow to ensure seamless document verification. The workflow begins with client registration and profile management, where users can securely create accounts and manage their profile information. The next step involves document transfer, where users can upload their documents onto the platform. These documents undergo cryptographic hashing, generating unique identifiers that are stored on the blockchain network for secure and sealed storage.

The verification process comprises two main modules: document check and identity validation. In the document check module, the system utilises cryptographic verification techniques to validate the authenticity and integrity of the uploaded documents. By comparing the hashed values stored on the blockchain with the computed hashes, the system provides a verification status indicating the document's genuineness.

In the identity validation module, advanced biometric techniques, specifically fingerprint recognition, are employed to verify the identity of individuals. Users' fingerprints are compared with pre-registered data to ensure accurate identification. Machine learning algorithms may be utilized to enhance the accuracy and reliability of the verification process. Once both document and identity verification are successfully completed, the system generates a verification report and updates the blockchain record accordingly.

III. PROPOSED SYSTEM

The proposed system architecture integrates blockchain technology, IoT devices, and advanced biometric techniques for document verification. The blockchain coordination module ensures seamless integration with the blockchain network, managing transactional operations, data storage, and retrieval. The access control module handles role-based permissions and ensures appropriate access levels for different user types.

The fingerprint recognition module is responsible for capturing and processing users' fingerprints. It utilizes state-of-the-art fingerprint recognition algorithms and technologies to ensure accurate and reliable identification. The system incorporates fingerprint scanners or compatible IoT devices to capture high-quality fingerprint images for verification purposes.

The human verification module employs advanced biometric identification techniques to validate the identity of individuals. In addition to fingerprint recognition, other biometric modalities such as facial recognition or iris scans can be incorporated to enhance the security and reliability of the verification process. Machine learning algorithms may be utilised to train and improve the identification models based on collected data

IV. ANALYSIS

The analysis phase of the research focused on evaluating the performance and effectiveness of the proposed E-Dastavez system using blockchain and IoT technologies for document verification, with fingerprint-based document retrieval and human verification.

The system's accuracy was assessed by comparing the verification results with ground truth data. The system demonstrated a high level of accuracy in verifying the authenticity of documents. The cryptographic hashing techniques employed ensured the integrity of the documents stored on the blockchain, preventing tampering or unauthorised modifications. The system's ability to accurately match fingerprint samples with pre-registered data further enhanced the security and reliability of document retrieval.

Efficiency was a key aspect of the analysis. The proposed system streamlined the verification process, reducing the time and effort required compared to traditional methods. By leveraging blockchain technology, the system eliminated the need for manual verification and document handling, resulting in faster and more efficient operations. The integration of IoT devices, such as fingerprint scanners, facilitated seamless and automated document retrieval and human verification processes.

The analysis also revealed the potential applications of the proposed system. Government agencies can utilise this system for secure document verification and identity authentication. Educational institutions can verify academic certificates and authenticate student identities. Financial institutions can implement this system for efficient KYC processes and customer onboarding. Healthcare organisations can securely verify patient records and medical credentials. Employment agencies can conduct background checks and verify employee identities. The system's versatility allows it to be applied across various industries and institutions.

Although the analysis demonstrated the advantages and potential of the proposed system, certain limitations were identified. The system's effectiveness relies on the availability and reliability of the blockchain network. Any disruptions or issues with the network infrastructure may impact the system's performance. Additionally, the integration of IoT devices may require additional hardware and infrastructure investments.

In conclusion, the analysis phase confirmed the accuracy, efficiency, and potential applications of the proposed E-Dastavez system. The system's ability to securely verify documents using blockchain technology, along with fingerprint-based document retrieval and human verification, offers significant advantages in terms of security, efficiency, and trust. However, it is important to address the identified limitations and challenges to ensure the successful implementation and adoption of the system.

V. CONCLUSION

In conclusion, the research paper presents the E-Dastavez project, a document verification system that leverages blockchain technology, IoT, and advanced biometric techniques. The proposed system offers a secure, transparent, and efficient solution to address the challenges in document verification. By integrating blockchain technology, documents can be securely stored and verified, ensuring integrity and transparency. The use of IoT devices, specifically fingerprint recognition, enhances the verification process by providing reliable and accurate identification. The research findings demonstrate the effectiveness of the proposed system and its potential to revolutionise document verification processes across different sectors.

VI. FUTURE WORK

While this research provides a comprehensive framework for document verification, there are several avenues for future exploration and enhancement. Further research could focus on optimising the system's performance by incorporating emerging technologies, such as machine learning and artificial intelligence, to improve accuracy and efficiency. Additionally, the integration of additional biometric modalities and the exploration of multi-factor authentication techniques could further enhance the security and reliability of the system. Furthermore, scalability and interoperability aspects should be considered to ensure the system's compatibility with existing infrastructure and future technological advancements.

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to Dr. Santosh Kumar Dwivedi, Head of the Department, for his constant support, guidance, and encouragement throughout the research project. His valuable insights and expertise have been instrumental in shaping the direction of this research.

The authors would also like to extend their appreciation to Mr. Shadab Ali, the project guide, for his invaluable assistance and mentorship. His profound knowledge and guidance have been crucial in the successful completion of this research work.

The authors would like to acknowledge the support and resources provided by SRMCEM (Shri Ramswaroop Memorial College of Engineering and Management). The institution's infrastructure and facilities have played a significant role in facilitating the research and experimental activities.

Lastly, the authors would like to express their gratitude to all the individuals who contributed to this project in various ways, including their colleagues and participants who provided valuable insights and feedback during the research process.

The successful completion of this research would not have been possible without the collective efforts and support of all those mentioned above. Their contributions are greatly appreciated and have been integral to the accomplishment of this research work.

VII. REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: https://bitcoin.org/bitcoin.pdf

[2] Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from https://ethereum.org/whitepaper/

[3] Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? In: A. Pisano (Ed.), The Age of Cryptocurrency: Bitcoin and Digital Currencies for Beginners (pp. 51-65). Academic Press.

[4] Pop, C., Balanescu, M., Cristea, V., & Iordache, S. (2017). IoT-Blockchain Integration for Industrial Applications. Proceedings of the 41st International Conference on Telecommunications and Signal Processing (TSP), 512-516.

[5] Shafagh, H., Burkhalter, L., & Hithnawi, A. (2017). Towards Blockchain-based Auditable Storage and Sharing of IoT Data. Proceedings of the 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock), 45-50.

[6] Zhang, Y., Wen, M., & Xu, L. (2018). IoT System for Secure Data Sharing Based on Blockchain and IPFS. IEEE Internet of Things Journal, 5(3), 2123-2133.

[7] Kumar, V., Singh, R., Kumar, R., & Rani, P. (2019). A Review of Blockchain Technology in Internet of Things. Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 959-964.

[8] Pires, G., & Popovici, E. (2020). Biometric Authentication Techniques: Challenges and Future Trends. Proceedings of the 14th International Conference on Distributed Computing in Sensor Systems (DCOSS), 227-233.

[9] Carullo, M., Esposito, C., & Ficco, M. (2020). A Secure Architecture for Biometric Data Storage and Authentication in Cloud Environments. Future Internet, 12(5), 90.

[10] Chanson, M., Phan, R. C. W., & Lauradoux, C. (2020). Biometric Encryption and Fuzzy Extractors: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 22(4), 2502-2533.