Reduce Certificate Frauds in the Academic Field

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Shaik Arshiya Sultana , Chiramdasu Rupa , Ramanadham Pavana Malleswari , Thippa Reddy Gadekallu

In the digital age, ensuring the authenticity and security of academic certificates is a critical challenge faced by educational institutions, employers, and individuals alike. Traditional methods for verifying academic credentials are often cumbersome, time-consuming, and susceptible to fraud. However, the emergence of blockchain technology offers a promising solution to address these issues.

academic certificates encryption blockchain

1. Introduction

In the digital age, the importance of securely storing and verifying academic certificates is important. These certificates represent vital proof of an individual's educational achievements and serve as credentials for the various professional opportunities [1][2][3]. However, the traditional methods of issuing and verifying certificates are susceptible to fraud, manipulation, and loss, posing significant challenges to individuals, institutions, and employees. According to a survey, 60% of educational organizations are hit by phishing attacks. Targeting cloud data, the highest result of all verticals analyzed that the majority of educational organizations experienced phishing attacks (60%) and account compromise (33%) in 2020. Phishing was the most common incident, faced by all verticals analyzed in the report, but the frequency of this type of attack in the educational sector was much higher than the average of 40%. Additionally, 27% of educational organizations experienced ransomware, and 49% were unaware of the infection for days. The majority of respondents attribute their high level of vulnerability in the cloud to understaffed IT and security teams (53%), lack of expertise in cloud security (52%), and lack of budget (49%). To address these challenges, innovative technologies such as blockchain and encryption have emerged as powerful tools for enhancing the security and reliability of academic certificates [4][5][6][7]. Blockchain, the decentralized and immutable ledger technology that is used in cryptocurrencies like bitcoin offers a transparent and tamper-resistant framework for storing and managing digital records [8][9][10][11]. Encryption, on the other hand, ensures the confidentiality and integrity of data by encoding it using complex algorithms. It aims to explore the potential of blockchain and encryption in securing academic certificates, luteinizing the way educational credentials are managed and verified. By leveraging the inherent features of blockchain, such as decentralization, transparency, and immutability, coupled with robust encryption techniques, the integrity, authenticity, and accessibility of academic certificates can be significantly enhanced [12][13][14].

Figure 1 Represents a common blockchain environment for securing academic certificates. The user has to be authenticated by the educational institution authority, then only the user is allowed to enter the details in the front-end application. Later, the data is encrypted using the MetaMask extension and connects to any Ethereum network to store encrypted data on the blockchain.

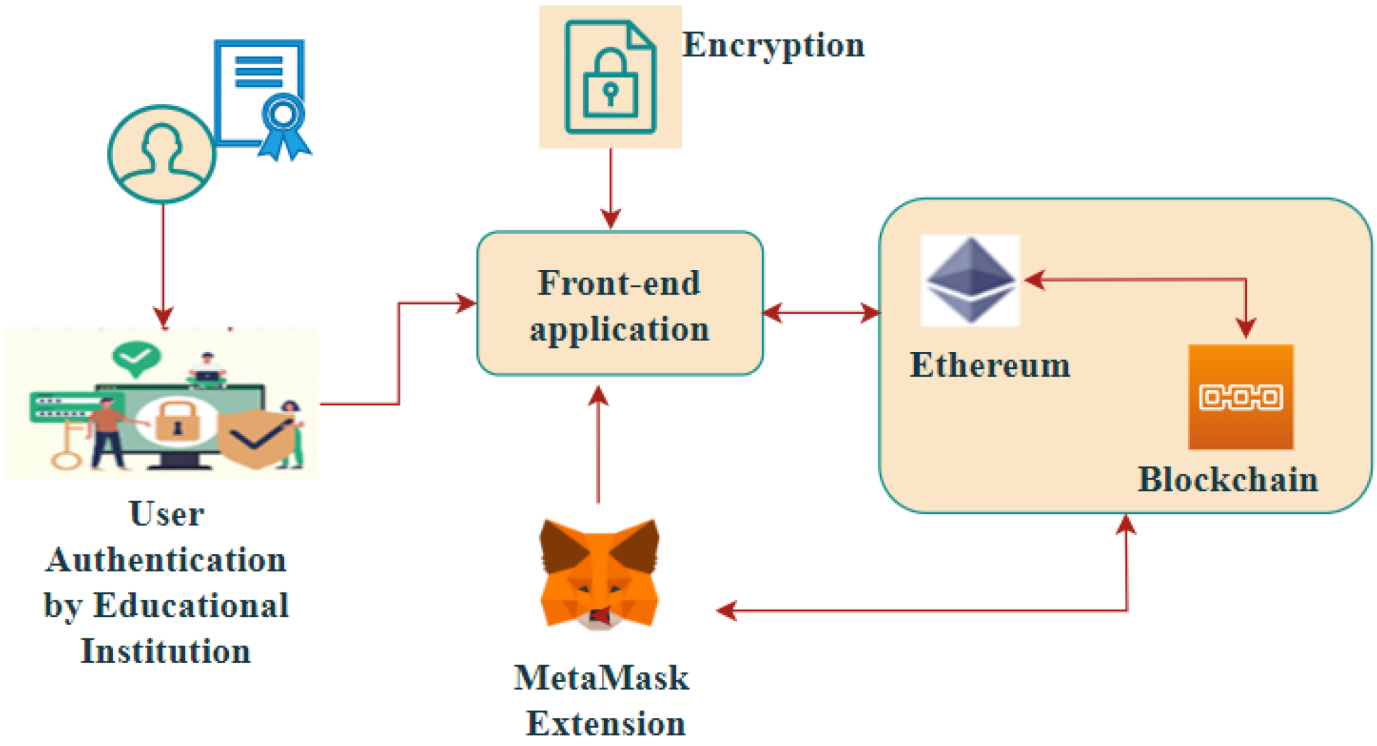

Figure 1. A generic Blockchain Scenario for securing Academic Certificates (Using MetaMask).

2. Reduce Certificate Frauds in the Academic Field

Sun et al. [11] proposed a storage solution for health care information security built on the hyperledger fabric and the attribute-based access control framework. The solution first makes use of attribute-based access management, which enables dynamic and fine-grained access to medical data and then stores the data on the blockchain, which can be made secure and impervious to tampering by creating appropriate smart contracts. Additionally, to reduce the strain on the blockchain's storage, this solution also uses IPFS technology. The advantage is high throughput when accessing medical information. Potential disadvantages of the proposed solution include scalability challenges, adoption complexities, governance and compliance considerations, access control complexity, and network and security risks.

Wang et al. [12] described a decentralized architecture for safe EHR exchange. A secure platform for health care facilities to communicate their encrypted EHR is created by the design, which makes use of the blockchain's smart contract technology. A constant-size attribute-based encryption (ABE) system is developed, in which the access policy is encoded in the search result on the blockchain, taking into consideration that fine-grained access control is required in actual EHR sharing services. The recommended remedy is a successful system that enables

authorized MedShare users to do multiple-keyword boolean searches across encrypted EHR. The outcomes show how effective MedShare is for exchanging EHRs. Potential limitations of the MedShare framework include scalability and performance challenges when dealing with a large volume of encrypted EHR data.

Zeng et al. [13] propose a framework for collaborative data training that is based on federated learning and blockchain technology. The gradients of the model are also encrypted and decrypted by the suggested homomorphic encryption approach to protect privacy. To be more specific, the framework is as follows: (i) they trained the local model using a novel capsule network for segmentation and classification of COVID-19 images; (ii) they used homomorphic encryption to secure the local model that encrypts and decrypts the gradients; and (iii) finally, the model is shared over a decentralized platform through the proposed blockchain-based federated learning algorithm.

Rahman et al. [14] proposed a solution to verify the authenticity and make the assertion of the decentralized system secure by deploying a blockchain-based academic credential authentication method. Academic certifications will be created by the system, authenticated, and corrected. Blockchain technology was used to develop a blockchain-based certificate authentication system. where the administrator might create, validate, and, if required, update the certificate. The administrator can also look up the number of times a certificate has been altered. To make fixes possible, they used two blockchains. This method will ensure prompt responses, dependable storage, and an end to questions regarding the validity of certificates. Any disruptions or failures in the blockchain network, such as network congestion, latency, or downtime, could impact the system's performance and availability.

Farouk et al. [15] proposed a decentralized, trustworthy, and highly regarded ledger that can be used by a student information system (SIS) to hold crucial data. The proposed models place a strong emphasis on data accessibility, which is exemplified by students' constant access to their data. This study suggests three approaches for implementing fully functional SIS on blockchains that store transactions like student marks, faculty member records, and course registration records, keeping away from being a super administrator or a centralized exposed storage where data integrity is at risk. The suggested model creates, validates, and publishes the certifications quickly to the interested parties without engaging a centralized administration. Ensuring interoperability and compatibility with other systems or platforms used in the education sector could pose challenges during implementation.

Ullah et al. [16] propose a decentralized distributed storage and sharing system based on blockchain that supports end-to-end encryption and granular access management. The suggested IoTChain paradigm uses the Ethereum blockchain as an auditable access control layer based on fine-grained permission on attribute-based access control (A-BAC) policy. The IoTChain concept, which combines the Ethereum blockchain and the interplanetary file system (IPFS), is designed for smart contracts. They share secret keys between data owners and consumers using the elliptic curve Diffie–Hellman key exchange protocol and an advanced encryption standard (AES) for encryption. The outcomes show that the strategy for IoT data is practical and cost-effective. The limitation here is the delays and impact on real-time data processing and also sharing in IoT applications.

Agyekum et al. [17] provided a proxy re-encryption strategy for safe data exchange in cloud settings. Identity-based encryption allows data owners to send their encrypted files to the cloud, while proxy re-encryption construction allows only authorized users to access the files. An edge device serves as a proxy server to conduct demanding calculations because the Internet of Things devices are resource-constrained. They improved the quality of service and made efficient use of the network capacity by utilizing some information-centric networking capabilities to provide cached material in the proxy. Additionally, the system paradigm is based on blockchain, a groundbreaking technology that permits decentralized data sharing.

Hao et al. [18] suggest a simple blockchain-based architecture for an intelligent autonomous access control system for Internet of Things devices. With the help of a token accumulation mechanism, the intelligent blockchain architecture makes it possible to store access policies, provide authentication services for data access control, and assess the trustworthiness of access request nodes. In particular, the blockchain network must confirm the user's access request before it can be granted. A compromised resistant consensus algorithm is modified and put into use to protect against no more than 1/3 compromised authenticators, ensuring the authenticity's dependability. It may require additional computational resources and introduce network overhead, which could impact the overall performance and scalability of the IoT system.

References

1. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. IEEE J. Biomed. Health Inform. 2022, 26, 1917–1927.
2. Qu, J. Blockchain in medical informatics. J. Ind. Inf. Integr. 2022, 29, 100258.
3. Liang, W.; Zhang, D.; Lei, X.; Tang, M.; Li, K.C.; Zomaya, A.Y. Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection. IEEE Trans. Emerg. Top. Comput. 2021, 9, 1410–1420.
4. El Azzaoui, A.; Chen, H.; Kim, S.H.; Pan, Y.; Park, J.H. Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems. Sensors 2022, 22, 1371.
5. Gao, J.; Yu, H.; Zhu, X.; Li, X. Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption. IEEE Syst. J. 2021, 15, 5233–5244.
6. Butt, G.Q.; Sayed, T.A.; Riaz, R.; Rizvi, S.S.; Paul, A. Secure Healthcare Record Sharing Mechanism with Blockchain. Appl. Sci. 2022, 12, 2307.
7. Liu, J.; Jiang, W.; Sun, R.; Bashir, A.K.; Alshehri, M.D.; Hua, Q.; Yu, K. Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain. IEEE J. Biomed. Health Inform. 2023, 27,

2231–2242.

8. Zhang, S.; Liu, Y.; Han, Z.; Yang, Z. A Lightweight Authentication Protocol for UAVs Based on ECC Scheme. Drones 2023, 7, 315.
9. Nagasree, Y.; Rupa, C.; Akshitha, P.; Srivastava, G.; Gadekallu, T.R.; Lakshmanna, K. Preserving Privacy of Classified Authentic Satellite Lane Imagery Using Proxy Re-Encryption and UAV Technologies. Drones 2023, 7, 53.
10. Du, R.; Ma, C.; Li, M. Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains. Tsinghua Sci. Technol. 2023, 28, 13–26.
11. Sun, Z.; Han, D.; Li, D.; Wang, X.; Chang, C.C.; Wu, Z. A blockchain-based secure storage scheme for medical information. J. Wirel. Commun. Netw. 2022, 2022, 40.
12. Wang, M.; Guo, Y.; Zhang, C.; Wang, C.; Huang, H.; Jia, X. MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain. IEEE Trans. Serv. Comput. 2023, 16, 438–451.
13. Kumar, R.; Kumar, J.; Khan, A.A.; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. Comput. Med Imaging Graph. 2022, 102, 102139.
14. Rahman, M.M.; Tonmoy, M.T.K.; Shihab, S.R.; Farhana, R. Blockchain-Based Certificate Authentication System with Enabling Correction. J. Comput. Commun. 2023, 11, 73–82.
15. Ali, S.I.M.; Farouk, H.; Sharaf, H. A blockchain-based models for student information systems. Egypt. Inform. J. 2022, 23, 187–196.
16. Ullah, Z.; Raza, B.; Shah, H.; Khan, S.; Waheed, A. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment. IEEE Access 2022, 10, 36978–36994.
17. Agyekum, K.O.B.O.; Xia, Q.; Sifah, E.B.; Cobblah, C.N.A.; Xia, H.; Gao, J. A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. IEEE Syst. J. 2022, 16, 1685–1696.
18. Hao, X.; Ren, W.; Fei, Y.; Zhu, T.; Choo, K.K.R. A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things. IEEE Trans. Serv. Comput. 2023, 16, 773–786.