Pragmatic Approach for Online Document Verification Using Block-Chain Technology

[1]Nilesh P. Sable, [2]Sachin R. Powar, [3]Queency Fernandes, [4]Nikita A. Gade, Akash B. Shingade

[1] Department of Information Technology, Bansilal Ramnath Agarwal Charitable Trust's, Vishwakarma Institute of Information Technology, Pune, India, drsablenilesh@gmail.com

[1, 2, 3, 4]JSPM's Imperial College of Engineering and Research Pune, India

ABSTRACT: As we all know, India has a plethora of universities, and many people graduate from them. Because it is possible for someone to falsify a degree, a secure based verification mechanism is required. It will be achieved in an existing system through the exchange of e-mails or postal mail; however, this is a time-consuming process that is insecure owing to human involvement. And, in order to solve these drawbacks, we implemented block chain technology into our system. When there is a security risk, block chain comes to mind. When it comes to data breaches, education is also not far away. For attackers, student data with little financial information has become a valuable commodity. At the same time, student verification is becoming a serious worry at educational institutions, which are being breached to generate phony identities and records. As a result, the greater the digitization of student information, the greater the need to protect student privacy.

Keywords: Block chain, Data Mining, SHA, Cloud computing.

I. INTRODUCTION

Any country's rapid expansion is dependent on its infrastructure, government regulatory policies, natural resources, skilled labor force, and a variety of other factors. The trained labor is one of the most essential variables in this. India has created multiple universities in response to the rising demand for trained workers in the industries, education, and health care sectors. According to official figures, India has a total of 1019 universities (as on UGC report dated 22-11-2021).

With the development in the number of institutions, enormous obstacles have arisen in the educational system as well as the university certification system. The issue of fraudulent degrees is a big problem that all universities, government sectors, public sectors, and private sector institutions are dealing with. Universities have their own verification system, but due to the lengthy process, it is not being used effectively. We provide an online certificate verification solution based on cloud computing that uses Block-chain technology to complete the verification procedure in a small amount of time.

Type of university	Number
State university	442
Deemed to be university	126
Central university	54
Private university	397

II. Block Chain

A block chain is a continually growing collection of information known as blocks. These blocks are encrypted and connected together. Each block contains a cryptographic hash of the previous block, as well as a timestamp and transaction data. The timestamp proves that the transaction data existed when the block was released, which is required to get into its hash. The timestamp confirms that the transaction data existed when the block was published in order to get into the hash. Because each block holds information about the previous one, they create a chain, with each new block strengthening the ones before it. As a result, block chains are resistant to data tampering since data in one block cannot be modified retrospectively without impacting the data in all previous blocks.

A. Structure

A block chain is a distributed, public digital ledger made up of information called blocks that is used to record transactions across multiple computers and make sure that no one block can be modified without impacting all subsequent blocks. This allows participants to review and audit transactions independently and for a low fee. A block chain database is run independently using a P2P network and a distributed time stamping server.

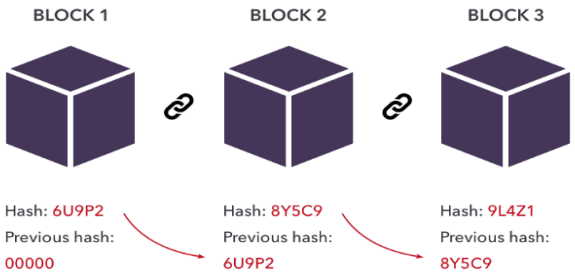

Figure 1: Block Structure

They are confirmed by extensive collaboration, which is fuelled by a sense of common good. This style of architecture encourages a consistent workflow with

minimum data security issues among participants. The use of a block chain eliminates the ability of a digital item to be reproduced indefinitely. It ensures that each value of unit was transmitted only once, solving the long-standing problem of duplicate spending. A block chain is a process of exchanging value. A block chain can protect title rights by creating a record that requires offer and acceptance when set up correctly to describe the trade agreement.

III. ALGORITHMS

In the proposed system we have implemented several algorithms for solving easily and automate a solution to the problem .The SHA algorithm is implemented for the purpose of hash generation .To validate and explore system performance using consensus algorithm for proof of validation. P2P software allows "peers" (separate computer systems) to exchange files by connecting over the internet.

Secure Hash Algorithms (SHA) is a set of cryptographic methods for keeping data safe. It converts data using a hash function, which is a mechanism based on compression algorithms, modular additions and bitwise operations. After that, the hash function returns a fixed-length string with no similarity to the original. These approaches are meant to be a one-way function, which signifies that after they've been changed into hash values, it's very hard to alter them back in its original content.

When utilizing SHA to encrypt passwords, the server just has to keep track of a single user's hash value instead of the actual password. This is beneficial if an attacker hacks into the database and only discovers the hashed functions, not the passwords themselves. If they try to use the hash value as a password, the hash function will convert it to another string and prohibit them from obtaining the information.

The sha-256 technique was used to generate hashes in the proposed system. One of the most secure hashing functions available is SHA-256. The US government mandates its agencies to use SHA-256 to protect some sensitive data. While the specific details of how SHA-256 works are classified, we do know that it is made up of a Merkle-Damgard structure obtained from a one-way compression function that was made up of the Davies-Meyer structure from a specialized block cypher.

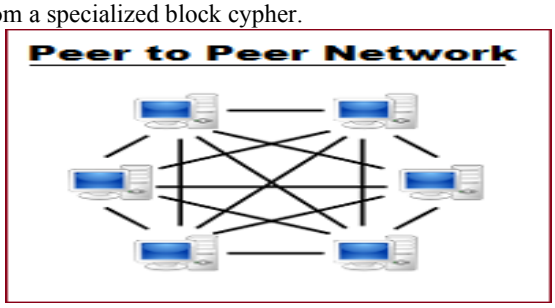

Figure 2: Peer to Peer Network (P2P)

P2P (peer to peer) is a decentralized and distributed communications methodology in which a group of devices or the nodes join to store and transport data, each functioning as a single peer. P2P communication takes place in this network without the use of a central administration or server, this means that all nodes have the same amount of power and do the same tasks.

B. CONSENSUS:

As we all know, block chain is a distributed decentralized network that allows for transparency, privacy, immutability and safety. Regardless the lack of a centralized system to authenticate and validate transactions, the Block chain believes every transaction to be completely safe and secure. It is only possible because of the consensus mechanism, which is an integral part of any Block chain platform.

Consensus Algorithm Each block added to the block chain is verified by all other nodes on the network to ensure that the node getting added is an authorized node. A consensus algorithm is used to complete this operation. They aid in the development of participant trust and network reliability. PoW, PBFT, and PoS are common consensus algorithms that are being used.

IV. PROPOSED MODULE

The system contains following modules:

Admin:

Admin is a system user who has access to data that has to be uploaded. An admin defines an access policy for accessing only those users with matching Enrollment and Name are given authorization to access the data.

Data User:

An authorized user who wishes to access data is referred to as a data user. The user creates an account with an Authority and receives a single Enrollment. If the Enrollment and Name satisfy an access policy connected with a document, the end user by entering proper Enrollment and Name, you will be able to check data and obtain access to educational database.

Distributed block chain: The block chain is a distributed ledger that represents the current state of the systems delegated access privileges. The Root User Authority and the Authorities (banking, medicine, marketing, etc.) manage permissions to interact with the block chain.

V. PROPOSED SYSTEM

As shown in Fig. 3, the suggested model's process is broken down into the following steps:

Step 1: University Admin uploads the documents.

Step 2: The uploaded document will be stored in database.

Step 3: A unique hash is created using the attributes: - admin name, email, contacts number, name of the student, student enrolment number, student name, system time, previous block and the time required for mining. The numbers of attributes are variable.

Step 4: The data with new hash value will be connected to the previous block.

Step 5: User with his unique id and password will login and request for the verification of his document.
Step 6: Admin upon receiving the request will verify if the user is the student of the particular university or not.
If yes then the request is approved and if not then the request is denied.
Step 7: The user's information is compared to the information recorded in the block chain. If the data is correct then document will be verified.
Steps 1 to 7 describe the whole data verification procedure and data flow. To eliminate data fraud, this will utilize secure cloud computing combined with block chain technology services.

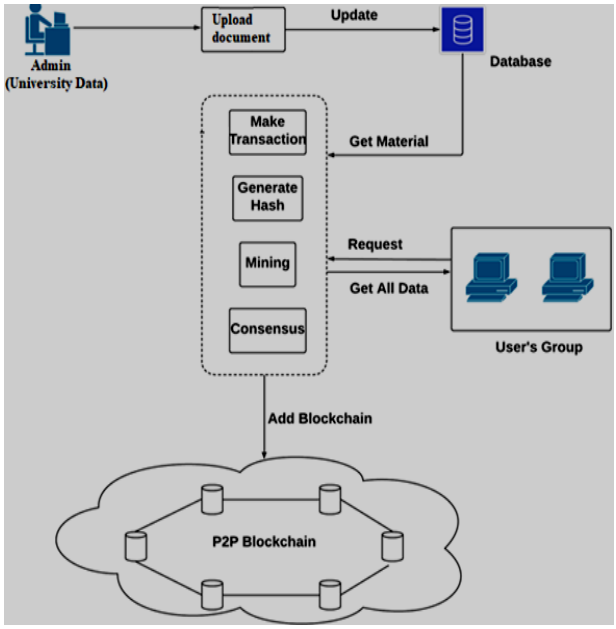

Figure 3: System Architecture

VI. CONCLUSION

We've developed an online certificate verification system that employs block-chain technology to enable online document verification. The online certificate verification system provides a cost-effective, simple to verify and maintain solution for introducing the cloud computing architecture to the online certificate verification system across all sorts of users with a single click. The block-chain concept is primarily being used to validate user credentials and offer data verification via a secure manner. Furthermore, depending on the needs of the system, this might be expanded to different types of data verification systems.

REFERENCES

[1] C. G. San Jose, "Document Security System Using Improved Hash Algorithm on Pre-processing Operation", Journal of Advanced Research in Dynamical and Control Systems, vol. 11, no. 11-, pp. 972-978, 2019. Available: 10.5373/jardcs/v11sp11/20193123.
[2] F. Kaspar, H. Rust, U. Ulbrich and P. Becker, "Verification and process oriented validation of the MiKlip decadal prediction system", Meteorologische Zeitschrift, vol. 25, no. 6, pp. 629-630, 2016. Available: 10.1127/metz/2016/0831.
[3] B. Houtan, A. Hafid and D. Makrakis, "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare", IEEE Access, vol. 8, pp. 90478-90494, 2020. Available: 10.1109/access.2020.2994090.
[4] G. Dagher, J. Mohler, M. Milojkovic and P. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", Sustainable Cities and Society, vol. 39, pp. 283-297, 2018. Available: 10.1016/j.scs.2018.02.014.
[5] Y. Sharma, "A Survey On Privacy Preserving Methods Of Electronic Medical Record Using Block chain", Journal Of Mechanics Of Continua And Mathematical Sciences, vol. 15, no. 2, 2020. Available: 10.26782/jmcms.2020.02.00004.
[6] V. Saxena and S. Pushkar, "Risk Reduction Privacy Preserving Approach for Accessing Electronic Health Records", International Journal of Healthcare Information Systems and Informatics, vol. 16, no. 3, pp. 46-57, 2021. Available: 10.4018/ijhisi.20210701.oa3.
[7] Y. Park, Y. Kim and J. Shim, "Block chain-Based Privacy-Preserving System for Genomic Data Management Using Local Differential Privacy", Electronics, vol. 10, no. 23, p. 3019, 2021. Available: 10.3390/electronics10233019.
[8] G. George and L. Jayashree, "A survey on user privacy preserving blockchain for health insurance using Ethereum smart contract", International Journal of Information Privacy, Security and Integrity, vol. 5, no. 2, p. 111, 2021. Available: 10.1504/ijipsi.2021.120354.
[9] K. Gu, N. Wu, Y. Liu, F. Yu and B. Yin, "WPKI Certificate Verification Scheme Based on Certificate Digest Signature-Online Certificate Status Protocol", Mathematical Problems in Engineering, vol. 2018, pp. 1-19, 2018. Available: 10.1155/2018/7379364.
[10] Y. Yuan, J. Zhang, W. Xu and Z. Li, "Identity-based public data integrity verification scheme in cloud storage system via blockchain", The Journal of Supercomputing, 2022. Available: 10.1007/s11227-021-04193-6.