International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 03 | March - 2021 ISSN: 2582-3930

CERTIFICATE VALIDATION USING BLOCKCHAIN

VARSHA.V

Asso.Prof. Mr. J. JAYAPANDIAN

Krishnasamy College of Engineering and Technology, Cuddalore.

Abstract - In the digital world, each and everything is digitalized in which the certificate of SSLC, HSC, and academic certificate are digitalized in the educational institution and provided to the students. Students are difficult to maintain their degree certificates. For the organization and institution, verification and validation of certificates are tedious and cumbersome. This project will help to store the certificate in the blockchain system and provide security. First, the paper certificates are converted into digital certificates. The chaotic algorithm is used to generate the hash code value for the certificate. Then the certificates are store in blockchain. And these certificates are validated by using the mobile application. By using blockchain technology system can provide a more secure and efficient digital certificate validation.

Key Terms: Blockchain, digital certificate, hashing, Ethereum, merkle tree.

I. Introduction

Now-a-day, education has become essential part of life, still needed to maintain reputation and trust in certification. Everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document 3rd person cannot validate the originality of the certificate. The blockchain is a chain of blocks and blocks are immutable in a distributed environment, it which storage devices are not all connected to a common processor.

It is a database of records/public ledger of all transactions/digital events that have been performed and information is shared within participating parties. Each entry in the system is verified by common consent of the participants in the system. Once information is entered into the blockchain it cannot be erased. It could provide a system that is transparent and secure. Blocks (Ordered Records) are added to blockchain with timestamp and a link to a previous block. Verifying a diploma/degree certificate today takes a good amount of time and requires human resources to request confirmation of details from universities. A possible solution is Blockchain; Blockchain for education may be a new concept. By using this technology, No need for a central authority to validate certificates. A college won't have to send a copy of transcript and prove to anyone that one have his/her degree.

Building a platform that will be open, accessible and one piece of software at a time and students can get Blockchain-based educational certifications. Blockchain-based educational certifications are the digital certificate and registered on the Ethereum Blockchain that will be cryptographically signed and tamper proof. Another person can view the certificate online, and no 3rd party validation is required for these digital certificates.

II. Literature view

1. The research paper Blockchain and smart contract for digital certification written by author “Jiin-chiou etal” in the year of 2018 explains that first, generate the electronic file and calculate hash value for it. Then, the system creates a QR-code.

Pros: Certificate granting are open and transparent in the system.

Cons: QR-code must be scanned with Smartphone and internet connection is required.

2. The paper Blockchain based certificate transparency and revocation written by author “Zewang Jingqiang Lin etal” in the year of 2019 says that CAs signed certificates and their revocation status information of an SSL/TLS web server are published by the subject and append it to the global certificate blockchain. Blockchain act as public logs to monitor CAs certificate signing and revocation operations.

Pros: Avoids the certificate fraudulent.

Cons: Certificate validation delay and false sense of security.

3. The paper Decentralized Digital Certificate Revocation system based on blockchain written by "DSV madala Etal" in the year of 2018 explains the consortium blockchain technology is collaborative management of digital certificate revocation lists by multiple CAs and introduces secret sharing scheme OCSP (Online Certificate Status Protocol) is used.

Pros: Trusted and rehable CRL.

Cons: False sense of security.

4. The research paper Certificate validation through public ledgers and blockchain written by author "Macro baldil etal" in the year of 2017 defines that CRLs are distributed through the use of a private blockchain, shared among CA(Certificate Authority). CAs are responsible for issuing certificate to requestors who meet the requirements and maintain CRLs. The users just need to read certificates.

Pros: Provide reliability.

Cons: CA ecosystem is fragile and prone to compromises.

The main advantage of this technology provides is its ability to exchange transactions without relying on trusted third party entities of any means. It can also provide data integrity, in-built authenticity and user transparency.

III. Proposed Methodology

In this paper, address this challenge by proposing the novel concept of *key-aggregate searchable encryption (KASE)*, and instantiating the concept through a concrete KASE scheme. The proposed KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former.

To support searchable group data sharing the main requirements for efficient key management are twofold:

1. First, a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files.

2. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files.

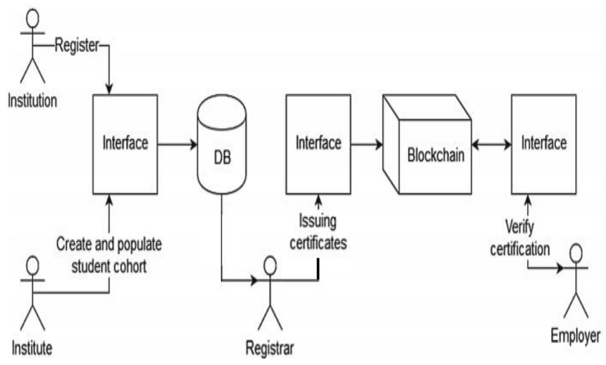

Figure 1: Proposed model for certificate validation using blockchain

In Addition with that we are implementing the Efficient Cryptography algorithm changing the file extension for the security purpose. And also implementing the user rights into account that user can modify the content after the uploading of file also. User can change the content of the file.

IV. Functions

1. User Interfaces: User interface design which we use to this project is netbeans and android studio. For server communication we develop an IDE using Netbeans. Using android studio, an android application to share and scan the QR code. TestRPC is a Node.js based Ethereum client for testing and development. It uses ethereumjs to simulate full client behavior and make developing Ethereum applications much faster.

User login: Like most popular data sharing products (e.g., Dropbox and citrix), our system relies on password verification for authenticating users. To further improve the security, multi-factor authentication or digital signatures may be used when available.

Data uploading: To upload a document, the owner runs KAE. Encrypt to encrypt the data and KASE. Encrypt to encrypt the keyword cipher texts, then uploads them to the cloud. The cloud assigns a docID for this document and stores the encrypted data in the path file Path, and then inserts a record into the table docs. In addition, the owner can encrypt the keys using his/her private key and store them into the table docs.

Data sharing: To share a group of documents with a target member, the owner runs KAE Extract and KASE. Extract to generate the aggregate keys, and distributes them to this member, then inserts/updates a record in table sharedDocs. If the shared documents for this member are changed, the owner must re-extract the keys and update the eld docID Set in table sharedDocs.

Keyword Search: To retrieve the documents containing an expected keyword, a member runs KASE. Trapdoor to generate the keyword trapdoor for documents shared by each owner, then submits each trapdoor and the related owners identity OwnerID to the cloud. After receiving the request, for each trapdoor, the cloud will run KASE. Adjust the trapdoor for each document in the docIDSet and run KASE. Test to perform keyword search. Then, the cloud will return the encrypted documents which contains the expected keyword to the member.

Data Retrieving: After receiving the encrypted document, the member will run KAE. Decrypt to decrypt the document using the aggregate key distributed by the documents owner.

2. Block Creation: A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block a hash code will generate for security.

3. Android based Block chain code generation: In this module, based on certificate numbers Block code will generate. While creating Blockchain code user can increase the count based on their needs. The major advantage of this module user can share the Block chain code to another person in case of necessity. When user scan the Certificate an OTP will be send to the registered mobile for verification.

Blocks: A block contains set of valid transactions that are in hash form and make a Merkle Tree(hash tree). Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. This linking forms a block of chain. This process is iterative and that confirms that previous block is reliable and correct. In this way, go back to genesis block.

Block time: In blockchain block time refers to the time when network can create 1 more block in the chain. It time vary from blockchain to blockchain some blockchain allows new block as frequently as every five seconds. This time also include the time in which data becomes verifiable. In crypto-currency term shorter block time means faster transaction. In Ethereum Blockchain Blocktime is approximate14~15seconds, while for Bitcoin is approx10 minutes.

Decentralization: Blocks are stored in different locations (nodes) so blockchain eliminates a number of risks which comes if data is in single location/storage. In which, don't have no central point of failure. Data stored on the blockchain is generally considered incorruptible, while centralized data is more easily controlled, information and data manipulation are possible.

4. **Verification**: In this module user will upload the certificates like 10th mark list, 12th mark list, college certificates, and government certificates and so on. Before upload, those certificates will verified by the corresponding sector, if upload school certificate, the certificate number will check with corresponds school database server if that certificate is verified after that it will be stored on server otherwise it will discard.

V. Conclusion

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

VI. Future work

Future technological evolution where everything is possible with internet and applications. Using blockchain technology sharing data, voting mechanism, Identity security, cryptocurrency exchange, real estate processing, and also payment can be secured. In future blockchain applications might be used for security and to avoid fraud in originality/Identity.

VII. References

1. Lyndon Lyons and Andreas Bachmann Jan Seffinga, "The Blockchain (R)evolution– TheSwissPerspective,",Switgerland,2017.
2. Don Tapscottand Alex Tapscott, "Realizing the Potential of Blockchain-A Multi-stakeholder Approach to the Stewardship of Blockchain and Crypto-currencies," in*WorldEconomicForum*,2017.
3. Alex Tapscott, BLOCKCHAIN REVOLUTION: Understanding the 2nd Generation of The Internet and the New Economy, 2017.
4. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, WhitePaper.
5. George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?, "in*IEEE*,2014.

6. Nicola Dimitri, The Blockchain Technology: Some Theory and Applications, 2017, MSM-Working Paper No. 2017/03.
7. Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander Jesse Yli-Huumo, "Where Is Current Research on Blockchain Technology?—A Systematic Review, "October 2016.
8. Nirmala Singh and Sachchidan and Singh, "Blockchain: Future of financial and cybersecurity, "in *IEEE*, Noida, 2016.
9. EnginZeydanandSuaybSbArslanGültekinBerahanMermer,"Anoverviewofblockchaintechnologies:Principles,opportunitiesand challenges,"in*IEEE*,Turkey,2018.
10. Narn-Yih Lee, Chien Chi and Yi-Hua Chen Jiin-Chiou Cheng, "Blockchain and smart contract for digital certificate", in *IEEE*, Japan, 2018.
11. Henrique Rocha, Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "Smart Inspect: solidity smart contract inspector," in *IEEE*, Italy, p.2018.
12. GWYND'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online]. https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-ireland-other-159-countries-no-kidding-335114.html
13. Abdul Wadud Chowdhury. (2017, Nov.) https://medium.com. [Online].https://medium.com/oceanize-geeks/blockchain-and-the-future-of-digital-trust-354acc279acc
14. Nick Grossman. (2015, June) https://www.nickgrossman.is. [Online].https://www.nickgrossman.is/2015/the-blockchain-as-time/

BIOGRAPHY:

Miss. V. Varsha

A Master of Computer Applications Third year student at Krishnasamy College of Engineering and Technology, Cuddalore. She was born on June 6, 1999. She is interested in developing mobile application in Android Operating System. She also likes to create Web Sites and Web Applications.