International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Certificate validation using Secure Computing

Mr. Pavan Kumar[1], Koya Jayasree[2], Kumaram Sathwika[3], Nandala Sandhya Rani[4]

[1]Associate Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India.

[2,3,4]UG-Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India.

ABSTRACT

In this project to secure academic certificate and for accurate management and to avoid forget certificate we are converting all certificates into digital signatures and these digital signatures will be stored in Block chain server , this Block chain server support tamper proof data storage and nobody can hack or alter its data and if by an chance if its data alter then verification getfail at the next block storage and user may get intimation about data alter. In the Blockchain technology same transaction data stored at multiple servers with hash code verification and if data alter at one server then it will detect from other server as for same data hash code will get different. For example, in Block chain technology data will be stored at multiple servers and if malicious users alters data at one server, then its hash code will get changed in one server and other server left unchanged and this changed hash code will be detected at the verification time and future malicious user changes can be prevented. In the Blockchain each data will be stored by verifying old hash codes , if old hash codes remain unchanged then data will be considered as original and unchanged and then new transaction data will get appended to Blockchain as new block. For each new data storage all blocks hash code will be verified.

INTRODUCTION

1. PROJECT OVERVIEW

The project consists in designing and implementing the system which covered the above solutions. The project also involves a comprehensive evaluation of the system security, and the assessment outcomes provide compelling evidence to prove that implementation is practical, reliable, secured, which might give some hints of important architectural considerations about the security attributes of other blockchain-based systems.

In this section, we discuss the implementation from the point of view of system architecture, database architecture. The system architecture and database architecture show how the system is designed from the engineering point of view.

The issuing applications are responsible for the main business logic which include the certificates applying, examining, signing and issuing. The issuing applications are designed to merge the hash of the certificate in a Merkle tree and send the Merkle root to Blockchain amidst signing by the majority of community members. Also, the issuing applications involved the revocation of certificate. The issuing applications are responsible for the main business logic which includes the applying for, examining, signing and issuing of the certificates. The issuing applications are designed to merge the hash of the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

certificate with a Merkle tree and send the Merkle root to the Blockchain. Also, the issuing applications deal with the revocations of certificates.

The verification application focuses on checking the authenticity and integrity of the certificates that have been issued. It includes two main components: a web-based page and an Android-based application. They use the same mechanism, and fetch the transaction message through the blockchain API and compare the transaction message with the verification data from the receipt. The mechanism can be briefly described in the following way: check the authentication code is valid; check the hash with the local certificate; confirm the hash is in the Merkle tree; ensure the Merkle root is in the blockchain; verify the certificate has not been revoked; validate the expired date of the certificate. Also, it has to be mentioned that for the convenience of sharing the certificates, the Android-based application allows for verification of the documents by scanning the QR code directly. The blockchain acts as the infrastructure of trust and a distributed database for saving the authentication data. Typically, the authentication data consist of the Merkle root generated using hashed data from thousands of certificates. The MongoDB is employed as our database since the MongoDB successfully manages JSON-based certificates and provides high availability and scalability.

Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies are thriving, including the most popular— Bitcoin, Ether, and Ripple [2]—the value of which has surged recently. People are beginning to pay attention to blockchain, the backbone technology of these revolutionary currencies. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses.

Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain [1]. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together.

2 PURPOSE

Counterfeit academic certificates have been a longstanding issue in the academic community. Not until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, a technique which is mainly implemented by conflating the hash value of local files to the blockchain but remains numerous issues, did an effective technological approach protecting authentic credential certification and reputation appear.

Based on Block-certs, a series of cryptographic solutions are proposed to resolve the issues above, including, utilizing a multi-signature scheme to ameliorate the authentication of

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation; establishing a secure federated identification to confirm the identity of the issuing institution.

LITERATURE SURVEY:

Year	Title	Methodology	Research Proposal	Algorithms
2016	Towards Certificate Verification in Certificate Management System	Recursive Verification Approach-Iterative Model State Based Model 1)Certificate Authorisers 2)Users	CMS is used to generate, distribute, store and verify certificates.	Verification Principle 1)Certificate Path Development 2) Certificate Path Verification
2018	Cloud Based Online Certification Verification System	Uses Cloud Computing Architecture for minimising cost and time	Cloud helps to provide the quality services at the time of high load by using the number of resources. Cloud computing supports mechanism and policies for the distribution of load among the resources and provide unlimited throughput by adding server.	Cloud Virtualisation
2021	Digital Certificate Verification Scheme for Smart Grid using Fog Computing	The fog node can be used for this purpose with much better resources closer to the edge. Keeping the resources closer to the edge strengthen the security aspect of smart grid networks. Similarly, a fog	The proposed scheme has reduced storage, communication, processing overhead, and latency for certificate verification at edge devices. Furthermore, the proposed scheme	Online Certificate Status Protocol (OCSP)
		node can act as an intermediate Certification Authority (CA) (i.e., Fog Node as an Intermediate Certification Authority (FONICA)).	reduces the attack surface, even if the attacker becomes a part of the network.	
2020	An Enhanced Web Based Certification Verification System	OOADM-Object Oriented and Design Methodology	Enhanced Web based certificate verification system that was able to verify and authenticate certificates.	OOAD

1. EXISTING PROBLEM

The certificate are stored in centralized manner and verified manually, so it takes too much time to verify. There is no safety to the certificate that are given to any private sectors (banks). But, the data may be changed, deleted or modified. Certificates are easily hacked and make duplicate of that certificate. Students bring their certificates on interview places. There is no security for certificates.

2. PROPOSED SOLUTION

In this study, a blockchain certificate system was developed based on relevant technology. The system's application was programmed on the Ethereum platform and is run by the EVM. In the system, three groups of users are involved, Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained.

SYSTEM REQUIREMENTS

The project involved analyzing the design of few applications so as to make the application more users friendly. To do so, it was really important to keep the navigations from one screen to the other well ordered and at the same time reducing the amount of typing the user needs to do. In order to make the application more accessible, the browser version had to be chosen so that it is compatible with most of the Browsers.

System requirements include

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Hardware requirements and software requirements

REQUIREMENT SPECIFICATION

Software Requirements

For developing the application following are the Software Requirements:

- Operating System : Windows 8
- Coding Language : Python 3.7

Hardware Requirements

For developing the application following are the Hardware Requirements:

- System : MINIMUM i3.
- Hard Disk : 40GB.
- RAM : 4GB.

METHODOLOGY:

• The system planned a replacement dynamic certificate generation approach victimization its own custom blockchain

• The first student applies for Associate in Nursing e-certificate on the online portal with transfer all academic documents

• The web portal is authenticating a sure third party that validates all documents from the university, school, colleges, etc.

• Once with success verification has done from university, school, faculties it'll store information into the blockchain and same time it generates the distinctive certificate id or QR code and returns it to the scholar.

• Student will submit the received QR code or certificate id to the organization rather than a physical text of documents

• Organizations will submit QR code or id to the portal and pool the e-certificate of the various student and build the validation.

MODELING AND ANALYSIS

A) REGISTER MODULE:

• Upon first logging the user have to register themselves for uploading their files.

• The next step is to login with the registered email and then uploading of files.

• The student finds a message displaying "File uploaded Successfully" after completion of the process.

B) LOGIN MODULE

• The users logged in check for any notifications in their module or through emails.

• The requester requested for a file will be notified through emails or through the module notification. • The user after verifying whether it is trustworthy gives response to the user.

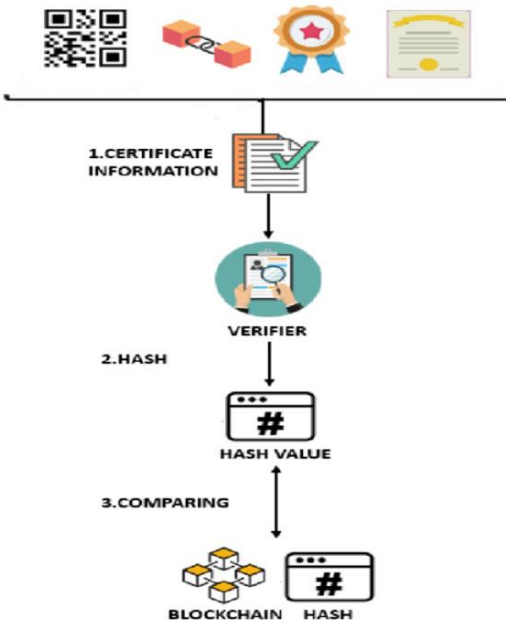
C) SAVE CERTIFICATE AND DIGITAL SIGNATURE

Using this module admin user can upload student details and student academic certificate and then application convert certificate into digital signature and then signature and other student details will be saved in Blockchain database

D) VERIFY CERTIFICATE

In this module verifier or companies or admin will take certificate from student and then upload to application and then application will convert certificate into digital signature and this digital signature will get checked/verified at Blockchain database and if matched found then Blockchain will retrieve all student details and display to verifier and if match not found then this certificate will be considered as fake or forge

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



IMPLEMENTATION

6.1 MODULES:

1. **Save Certificate with Digital Signature** : Using this module admin user can upload student details and student academic certificate and then application convert certificate into digital signature and then signature and other student details will be saved in Blockchain database.

1. **Verify Certificate** : In this module verifier or companies or admin will take certificate from student and then upload to application and then application will convert certificate into digital signature and this digital signature will get checked/verified at Blockchain database and if matched found then Blockchain will retrieve all student details and display to verifier and if match not found then this certificate will be consider as fake or forge.

RESULTS:

To implement this project, we have taken some certificates and this certificates are stored inside 'certificatetemplates' and you can use those or you own certificates to upload to Blockchain and below is the certificate screen shots.

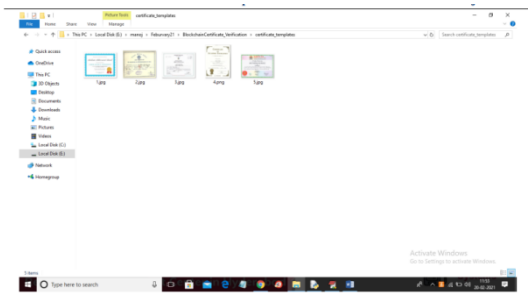


FIG:Certificates

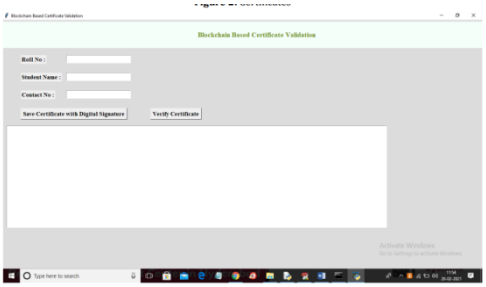


Fig:Graphical User Interface

In above screen enter student details and then click on 'Save Certificate with Digital Signature' button to convert certificate into digital signature and then saved in Blockchain.

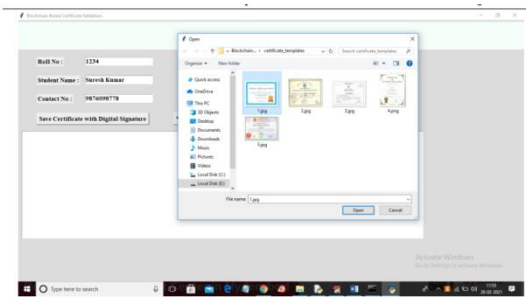


Figure 4: Save Certificate With Digital Signature

In above screen entered some student details and then click on 'Save Certificate with Digital Signature' button and then selecting and uploading '1.jpg' file and then click on 'Open' button to get below screen

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

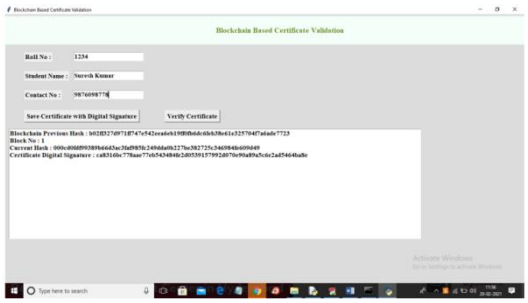


Figure 5: Verify Certificate

In above screen we can see Blockchain generated previous hash with block no 1 and its current hash and then keep on generating new blocks with each certificate upload and while running you can see that previous hash of new record will get matched with current hash of old record and this matched hash code proof that Blockchain verify old and new hash code before storing new block to confirm data is not altered. So above details stored at Blockchain and now verifier can click on 'Verify Certificate' button and upload same or other images to get below result.

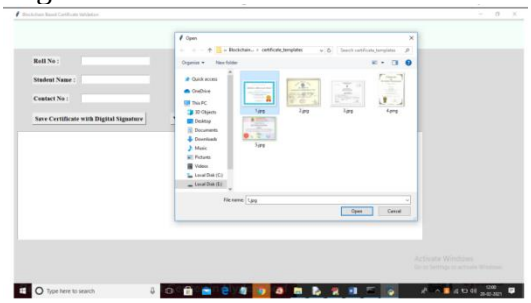


Figure 6 In above screen selecting and uploading '1.jpg' file and then click on 'Open' button to get below result.

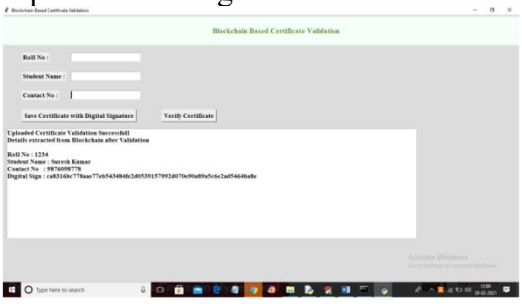


Figure 7 In above screen we uploaded same and correct image so application matched digital signature and then retrieve details from Blockchain and now try with some other image

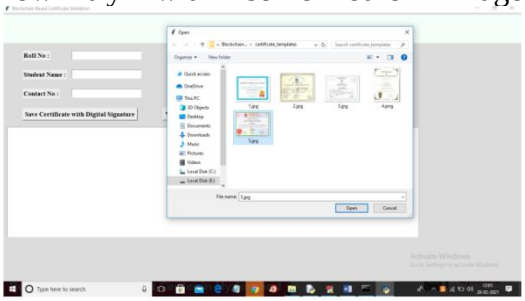


Figure 8

In above screen selecting and uploading '5.jpg' file and then click on 'Open' button to get below result

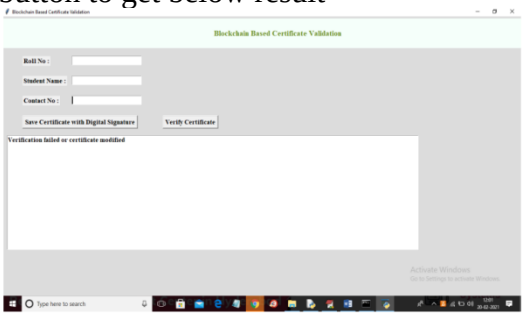


Figure 9

In above screen verification got failed as uploaded certificate not matched with stored certificates in Blockchain. Similarly you can upload any other certificate and convert them to digital signature.

CONCLUSION and FUTURE WORK:

In June 2016, the MIT media lab released their blockchain-based credential system which is more secure, more reliable and harder to forge, in contrast to existing technologies that based on the third party arbitration. However, there are some serious authentication defects and vulnerable revocation mechanism which limits the prevalence and application of the project. In our project, to solve these problems and make its concept more practical, we proposed and designed a set of innovative cryptographic protocols which includes multi-signature, BTC-address-state-based revocation

mechanism and trusted federated identity.

Among these protocols, the multi-signature scheme most notably increases the difficulty of forging owing to the fact that each issuing progress is obliged to be signed by the majority of the academic committee members. Besides, it enhances the safety of the private keys storing for the reasons that the private keys are possessed by separated devices and people. Besides, BTC-address-based revocation mechanism improved the stability of the certificate revocation because BTC address is accessible and stable at any time. What's more, the protocol of our project can be used in other related realms such as digital right protecting and contract proof. Case in point, our protocol enables the two companies to attach their contract onto the block chain with multi signature, which is different from the traditional third party-based work mode and dispel the worries of forging credentials.

Moreover, we implemented a blockchain-based certificate system, which embraced all the above protocols, by utilizing Java and JavaScript. This system has remedied the defect in Blockcerts to a certain extent, which makes the theory of blockchain-based certificate more practicable.

Lastly, there are some limitations remained to be discussed, albeit, these considerations fall outside the scope of this paper: Our project is based on the Bitcoin blockchain, the maintenance of which relies on thousands of participants in the cryptocurrency ecosystem. Admittedly, it is imprudent to assume that the Bitcoin would work well continuously in the future because myriad types of stakeholders influence blockchain ecosystem or business model. In the years to come, we will adopt multiple blockchain sources such as Hyperledger and Ethereum to eliminate the factors of instability.

REFERENCES:

[1] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling, BIS2018: Business Information System. Workshops, vol. 339 of Lecture Notes in Business Information Processing, Springer, pp. 185-196, 2018.

[2] Gayathiri, A., Jayachitra, J., & Matilda, S (2020). Certificate validation using blockchain. 2020 7th International Conference on Smart Structures and Systems (ICSSS). doi:10.1109/icsss49621.2020.9201988

[3] Song, Hesheng, and Carlos Enrique Montenegro-Marin. "Secure prediction and assessment of sports injuries using deep learning based convolutional neural network." Journal of Ambient Intelligence and Humanized Computing 12.3 (2021): 3399-3410.

[4] Chang, Jinping, Seifedine Nimer Kadry, and Sujatha Krishnamoorthy. "Review and synthesis of Big Data analytics and computing for smart sustainable cities." IET Intelligent Transport Systems (2020).

[5] Batoo, Khalid Mujasam, et al. "Behavior-based swarm model using fuzzy controller for route planning and E-waste collection." Environmental Science and Pollution Research(2021): 1-15.d management for internet data centers," IEEE Transactions on Smart Grid, vol. 3, no. 1, pp. 183–192, 2012.