BLOCKCHAIN BASED CERTIFICATE VALIDATION

M.Pradeep Kumar[1]., N.Sruthi[2].,A.Manasa[3]
1 Assistant Professor, Department Of CSE., Malla Reddy College Of Engineering For Women.,Maisammaguda.,
Medchal.,Ts, India (✉pradeepit09@gmail.com)
2, 3 B.Tech CSE, (20RG5A0507, 20RG5A0509),
Malla Reddy College Of Engineering For Women., Maisammaguda., Medchal., Ts, India

ABSTRACT

The primary objective of this project is to prevent certificate forgery and ensure proper maintenance of academic credentials. To realize these capabilities, we are transforming all certificates into digital signatures and storing them on a Blockchain server, which allows for secure data storage and cannot be hacked. In order to provide a security feature, identical data is saved in separate blocks. If the data has been tampered with, the following block's verification will fail, and the user may be notified.

Key words :

Blockchain and Digital Signature are two relevant terms.

INTRODUCTION

Fake degrees and diplomas have been a problem in the academic world for years. An efficient technological approach protecting authentic credential certification and reputation did not appear until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, which is primarily implemented by conflating the hash value of local files to the blockchain but remains numerous issues. To address these problems, several cryptographic solutions are proposed, all of which are built on top of Blockers. These include using a multi-signature scheme to improve certificate authentication, implementing a safe revocation mechanism to increase the reliability of certificate revocation, and setting up a secure federated identification to verify the identity of the issuing institution. In Blockchain technology, identical transaction records are stored on multiple servers, each of which has its own unique hash code for verification purposes. If any of these records are tampered with, the change will be immediately apparent on the other servers because the hash code will have changed. For instance, in Blockchain technology, data will be stored at multiple servers, and if malicious users alter data at one server, its hash code will get changed in one server and other servers will be left unchanged; this changed hash code will be detected at verification time and future malicious user changes will be prevented. New transaction data is added to the Blockchain as a new block only if the existing hash codes for that data stay unaltered, at which point the new data is regarded to be the same as the original. The hash codes of all stored blocks are checked before any new data is added.

Techniques

The first student to apply for an electronic Associate in Nursing degree via the system's site has already submitted all required application materials and will get their degree once the system's replacement dynamic certificate generation technique based on the system's own bespoke blockchain is fully operational.

Every document submitted to the online portal by a university, school, college, etc. is verified by an independent, trusted third party.

• Once verification from the educational institution has been completed successfully, the data will be stored in the blockchain and the unique certificate id or QR code will be generated and sent to the student at the same time.

A QR code or certificate id will replace paper copies of papers submitted by students to organizations.

• Businesses will upload their QR code or id to the site, where they will be combined with the electronic certificates of other students to form the validation.

Analysis and Modelling

A) MODULE TO REGISTER:

Users must first register in order to upload files, which must be done at the initial login.

After that, you can begin uploading files by logging in with the email address you used to sign up.After finishing the procedure, the student should get a notification reading "File uploaded Successfully."

B) Modulus de indicia de session

• Logged-in users look for new messages in their module or in their inbox.

• When a file is requested, the requester will get an email or a notice from the module.

• The user provides a response to the user after determining the reliability of the information.

C) RETAIN CERTIFICATE AND ELECTRONIC SIGNATURE

The module allows the administrator to upload student information and academic certificates, which are subsequently converted into digital signatures and stored in a Blockchain database.

D) Authenticate Certificate

In this section, a verifier, company, or administrator will collect a student's certificate, upload it to the application, and then have the certificate converted into a digital signature. If a match is found, the Blockchain database will retrieve all relevant student information and display it to the verifier; otherwise, the certificate will be flagged as a forgery.

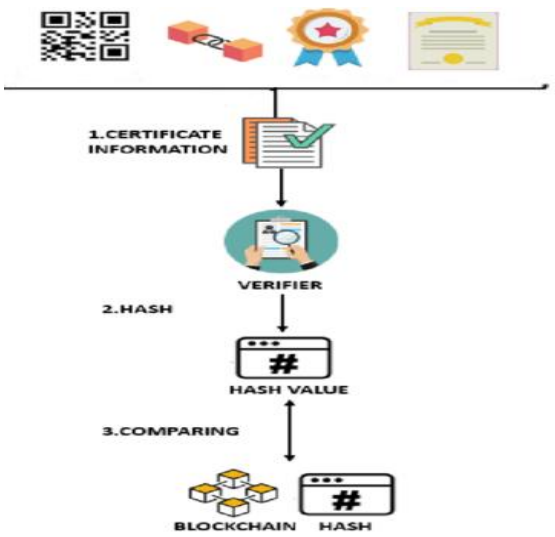

Figure 1: Blockchain based Certificate Validation

CONCLUSIONS AND RESULTS

Screenshots of the certificates we used for this project's implementation are provided below. These templates may be used to create new certificates or to upload existing ones to a blockchain.

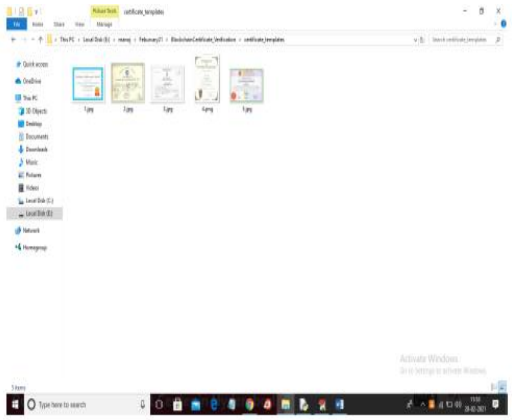

Figure 2: Certificates

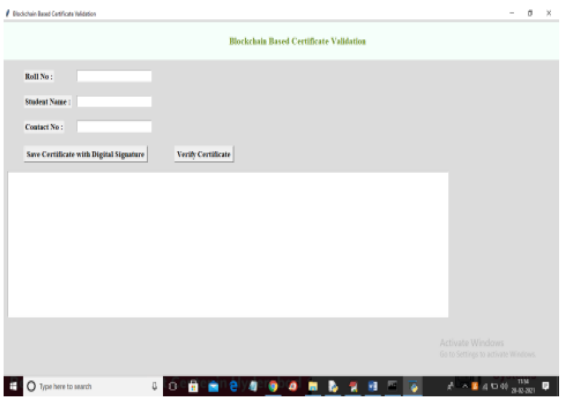

Figure 3: Graphical User Interface

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

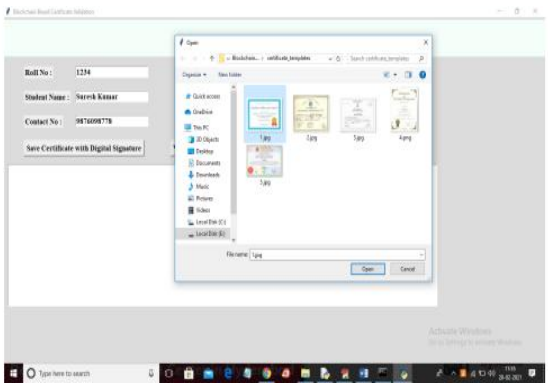

Figure 4: Save Certificate with Digital Signature

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

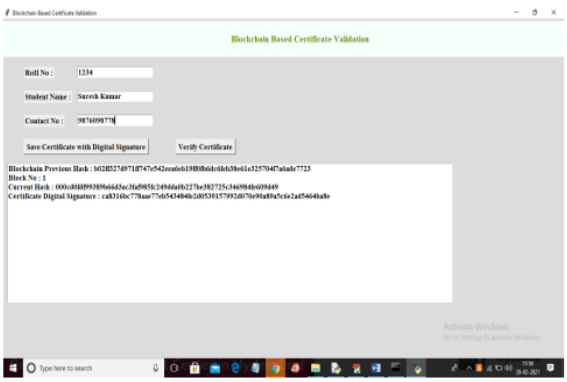

Figure 5: Verify Certificate

In the above image, we can see that Blockchain has generated a previous hash with block no. 1 and its current hash, and that it will continue to generate new blocks with each certificate upload. Furthermore, while Blockchain is running, the previous hash of a new record will get matched with the current hash of an old record, proving that Blockchain verifies old and new hash codes before storing a new block to ensure data integrity. After the above information has been entered into the Blockchain, the verifier can upload the same or similar images by clicking the "Verify Certificate" button.

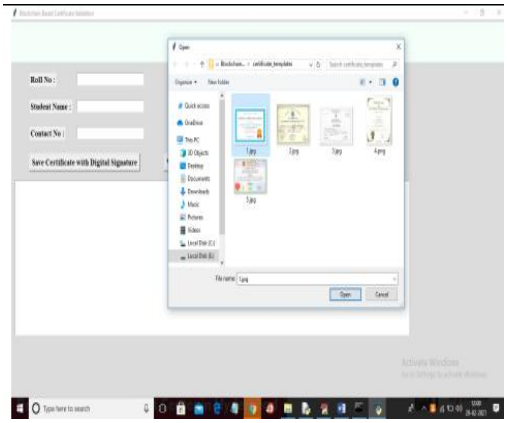

Figure 6

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

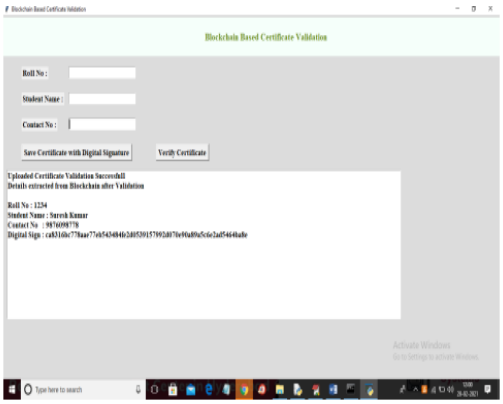

Figure 7

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

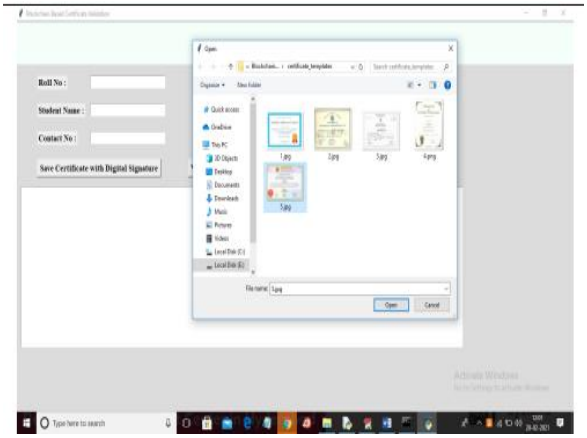

Figure 8

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

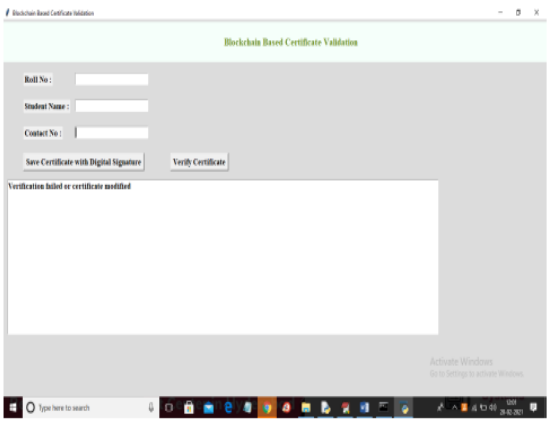

Figure 9

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

The system is transparent and open throughout the application and automatic awarding of certificates. This means that any company or organization may use the system to enquire about any certification. The results of the evaluation show that the system is secure enough for corporate application requirements. In the end, we ran a battery of tests to evaluate the security of the system from several angles, including the integrity of its data, its network, and its protocols.

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