SECURE STORAGE OF E-CERTIFICATES USING BLOCKCHAIN

Ms. BALA BHARGAVI SWETHA[1], Ms. ALLA JASWANTHI[2], Ms. PASUPULETI ANUHYA[3], Ms. VASANTHALA BHAVYA SRI[4], Mrs. ACP.RANJANI[5]

1 .BTech, Vijaya Institute of Technology For Women, Enikepadu, Vijayawada, Andhra Pradesh, India. Email : bhargaviswetha99@gmail.com
2. BTech, Vijaya Institute of Technology For Women, Enikepadu, Vijayawada, Andhra Pradesh, India.
3. BTech, Vijaya Institute of Technology For Women, Enikepadu, Vijayawada, Andhra Pradesh, India.
4. BTech, Vijaya Institute of Technology For Women, Enikepadu, Vijayawada, Andhra Pradesh, India.
5. Associate Professor, Computer Science and Engineering, Vijaya Institute of Technology For Women, Enikepadu, Vijayawada, Andhra Pradesh, India. Email : ranjani.vvnk@gmail.com

ABSTRACT

In this project, we are converting all certificates into digital signatures in order to secure academic certificates, for accurate management, and to prevent certificate forgery. These digital signatures will be stored in a blockchain server because this blockchain server supports tamper-proof data storage, meaning no one can hack or alter its data. If by chance, if its data alter, verification will fail at the next block storage, and the user may be informed about the data alter. Similar transaction data is saved across many servers in blockchain technology with hash code verification. If data is altered on one server, it will be discovered on the other server since the hash code will change. For instance, in Blockchain technology, data is stored across multiple servers. If malicious users change data at one server, the hash code will change there while remaining unchanged on the other servers. This changed hash code will be discovered during verification, preventing further malicious user changes. Each piece of data in a blockchain is saved by comparing it to older hash codes; if the older hash codes are unmodified, the data is regarded as original and unaltered, and a new block of transaction data is added to the blockchain. Every new block of data storage will have its hash code validated.

1 INTRODUCTION:

The academic world has long struggled with the problem of fake academic credentials. An effective technological strategy protecting authentic credential certification and reputation didn't emerge until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, a method that is primarily implemented by fusing the hash value of local files to the blockchain but still has many issues. Based on Blockcerts, a number of cryptographic fixes are suggested to address the aforementioned problems. These fixes include the implementation of a multi-signature scheme to improve certificate authentication, a safe revocation mechanism to increase the dependability of certificate revocation, and a secure federated identification to verify the identity of the issuing institution.

The system that addressed the aforementioned problems was designed and put into operation as part of the project. The project also includes a thorough assessment of the system security, and the assessment results offer compelling proof that the implementation is workable, dependable, and secure. Additionally, they may provide some hints about crucial architectural considerations regarding the security characteristics of other blockchain-based systems.The implementation is covered in this part from the standpoints of system and database architecture. The database architecture and system architecture both demonstrate how the system was created from an engineering standpoint. The primary business logic, which covers certificate applying, examining, signing, and issuing, is handled by the issuing apps. The certificate's hash will be combined in a Merkle tree by the issuing applications, which will then send the Merkle root to Blockchain while the majority of the community members sign it. The cancellation of certificates was also a part of the applications for issue. The primary business logic, including applying for, reviewing, signing, and issuing certificates, is handled by the issuing applications. The certificate's hash and a Merkle tree are combined by the issuing software, which then sends the Merkle root to the Blockchain. The applications for issuing certificates also cover the cancellation of certifications. The verification application focuses on examining the validity and reliability of the given certifications. There are two main parts to it: an Android application and a web website. They employ the same approach and retrieve the transaction message via the blockchain API before comparing it to the verification information on the receipt. The mechanism can be summed up as follows: confirm the authenticity of the authentication code; validate the hash against the local certificate; confirm the hash is in the Merkle tree; confirm the Merkle root is in the blockchain; confirm the certificate has not been revoked; and confirm the certificate's expiration date. It should be noted that the Android-based application enables direct document verification by scanning the QR code, making it easier to share certifications. The blockchain serves as a distributed database for storing the authentication data as well as the infrastructure of trust. The Merkle root, which is created using hashed information from thousands of certificates, typically makes up the authentication data. Since the MongoDB successfully supports JSON-based certificates and offers high availability and scalability, the MongoDB is used as our database.

2. LITERATURE SURVEY AND RELATED WORK

The way that people live has changed as a result of developments in information technology, the widespread use of the Internet, and the widespread use of mobile devices. Digital coins known as virtual currency, which were initially created for usage online, are now widely used offline. The ease of the Internet has led to the growth of many virtual currencies, the most well-known of which are Bitcoin, Ether, and Ripple [2], the value of which has lately increased. The blockchain, the core technology behind these innovative currencies, is starting to attract attention. Blockchain has a decentralised, untouchable database with a wide range of possible applications. Blockchain is a decentralised database that's frequently used to log various transactions. The transaction is added to a block that already contains records of numerous transactions once consensus among the various nodes has been obtained. The hash value of a block's most recent connection counterpart is contained in each block. A blockchain is created when all the blocks are connected to one another [1]. Data are decentralised because they are dispersed among numerous nodes (the distributed data storage). As a result, the nodes jointly maintain the database. A block in a blockchain is only considered genuine when it has been verified by numerous parties.

3 Implementation Study

Modules:

1) **Save Certificate with Digital Signature:**

   Using this module, an admin user can upload student information and academic certificates. The certificates will then be converted into digital signatures and preserved in a blockchain database together with other student information.

2) **Check the certificate:**

   In this module, the verifier, the company, or the administrator will collect the student's certificate and upload it to the application. The application will then convert the certificate into a digital signature, which will be checked at the Blockchain database. If a match is found, the blockchain will retrieve all the student's information and display it to the verifier; if not, the certificate will be deemed to be fake or forged.

4 PROPOSED WORK AND ALGORITHM

It takes too long to validate since the certificate is manually verified and kept in a centralised location. The certificates issued to any private sector (banks) are not secure.However, the data can be edited, removed, or changed. It is simple to compromise certificates and create copies of them. On the day of the interview, students bring their certificates. Certificates lack any security.

Based on the technology used in this study, a blockchain certificate system was created. The system's application is run by the EVM and was created on the Ethereum platform. Three user groups are present in the system: Certificates are issued by schools or certifying agencies, who also have access to the system and can search its database. The method is used by the authorities to provide certificates to students after they have met specified standards. The students can ask questions concerning any certificates they have obtained after receiving their certificate. The programme

1 Enter Roll number, Student name and contact number.

2 Nov click on save certificate with digital signature. And upload the Certificate.

3 Now by clicking on the verification we are getting the data about the certificate validation like certificate contains signature and all.

"Chinese" and "China" are related, there is a great deal of space between them. To record information about long-term dependencies, we must employ LSTM rather than the conventional RNN model.

4 Prediction: Last, we concatenate the latent vectors of each view for fraudulent activity prediction, which is named late fusion. Multi-view learning based on late fusion can avoid losing information as in the case when multiple views are combined to create a single view. One key piece of information that we want to preserve is the sequence of keystrokes. By using multi-view, we are able to maintain each view separately but then use multiple views to make predictions. We use two separate points of view. A variable number of characteristics and samples are present in each view VI. Concatenating the two views into a single view, as shown in Fig. 2a, is one strategy that can be used. This method is also known as early fusion. This, however, is ineffective since each view of a session has a distinct amount of characteristics and records. We choose to employ multi-view deep learning with late fusion instead of early fusion to combine several views into one view. We first decide to model each perspective independently. The latent vector representation of each view is then discovered using a deep learning model.

5 RESULTS AND DISCUSSION

SCREENSHOTS

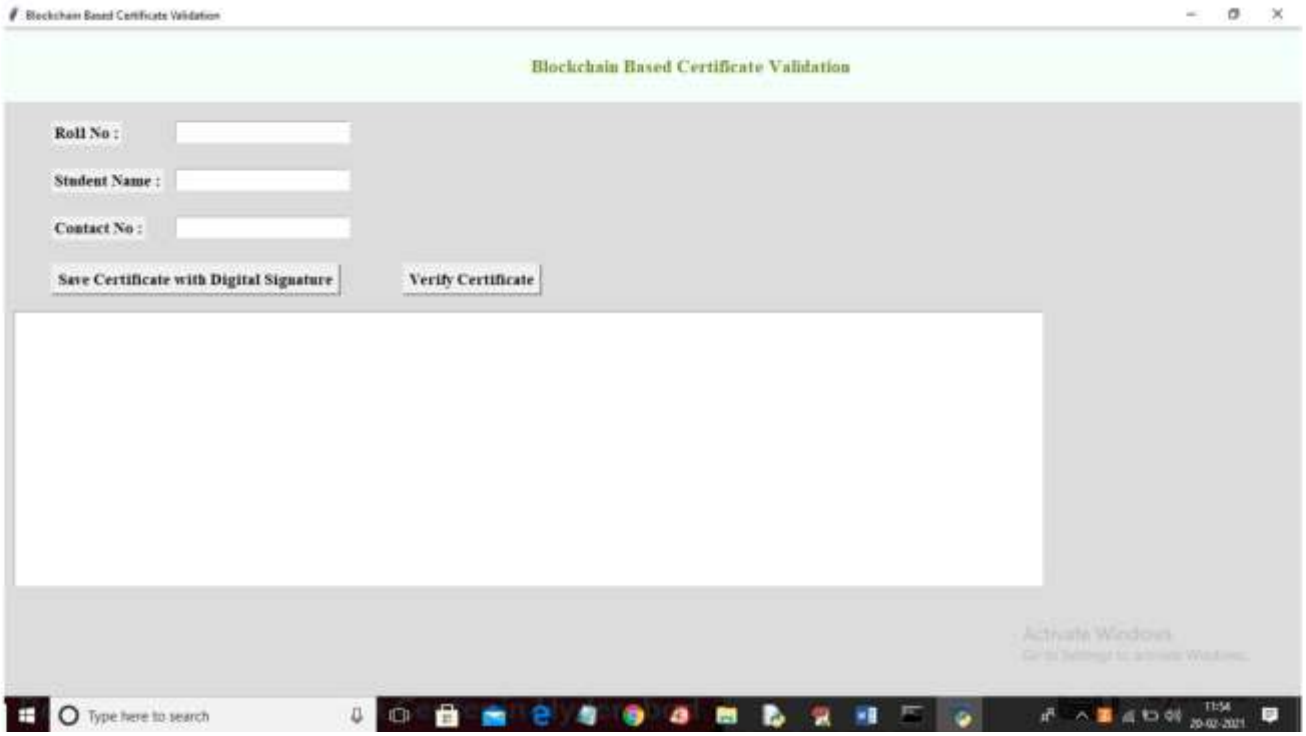
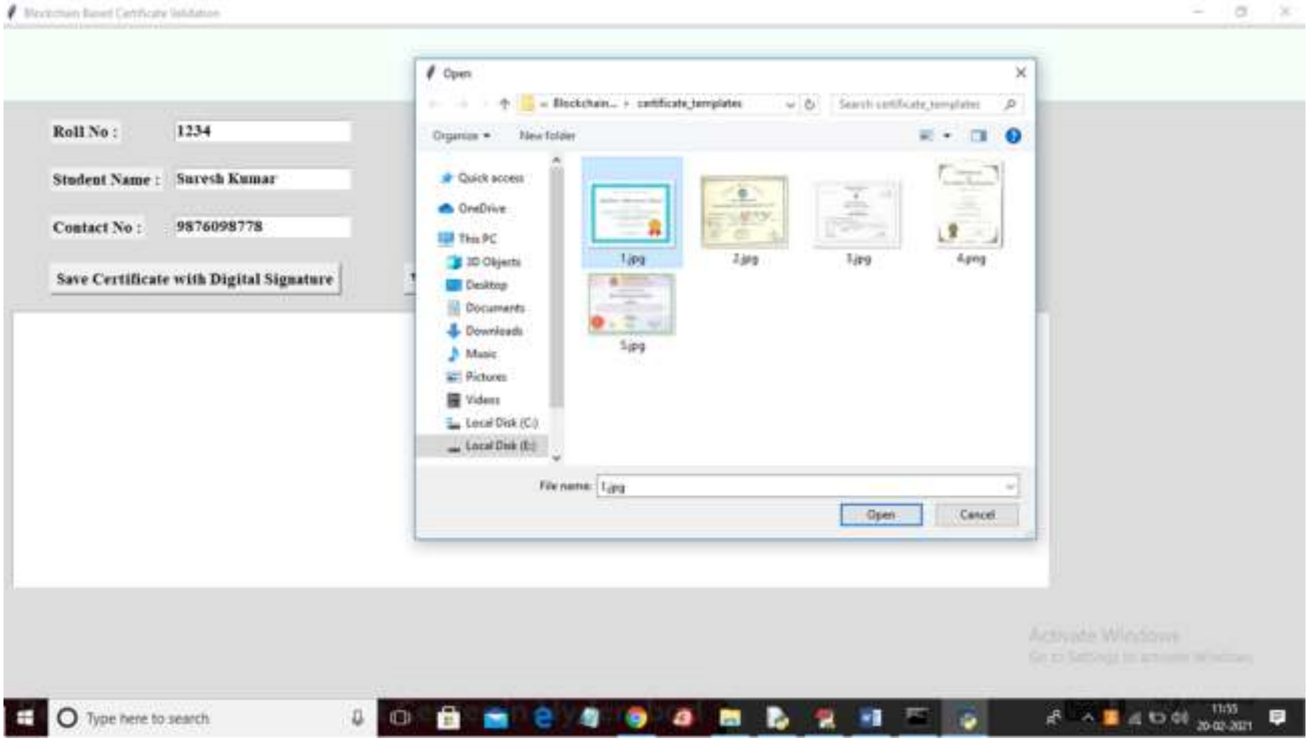

Blockchain Based Certificate Validation
Blockchain Based Certificate Validation
Roll No :
Student Name :
Contact No :
Save Certificate with Digital Signature
Verify Certificate
Activate Windows
Go to Settings to activate Windows.
Type here to search
11:54
20-02-2021

Fig 1 - student details and then click on 'Save Certificate with Digital Signature' button to convert certificate into digital signature and then saved in Blockchain



Blockchain Based Certificate Validation

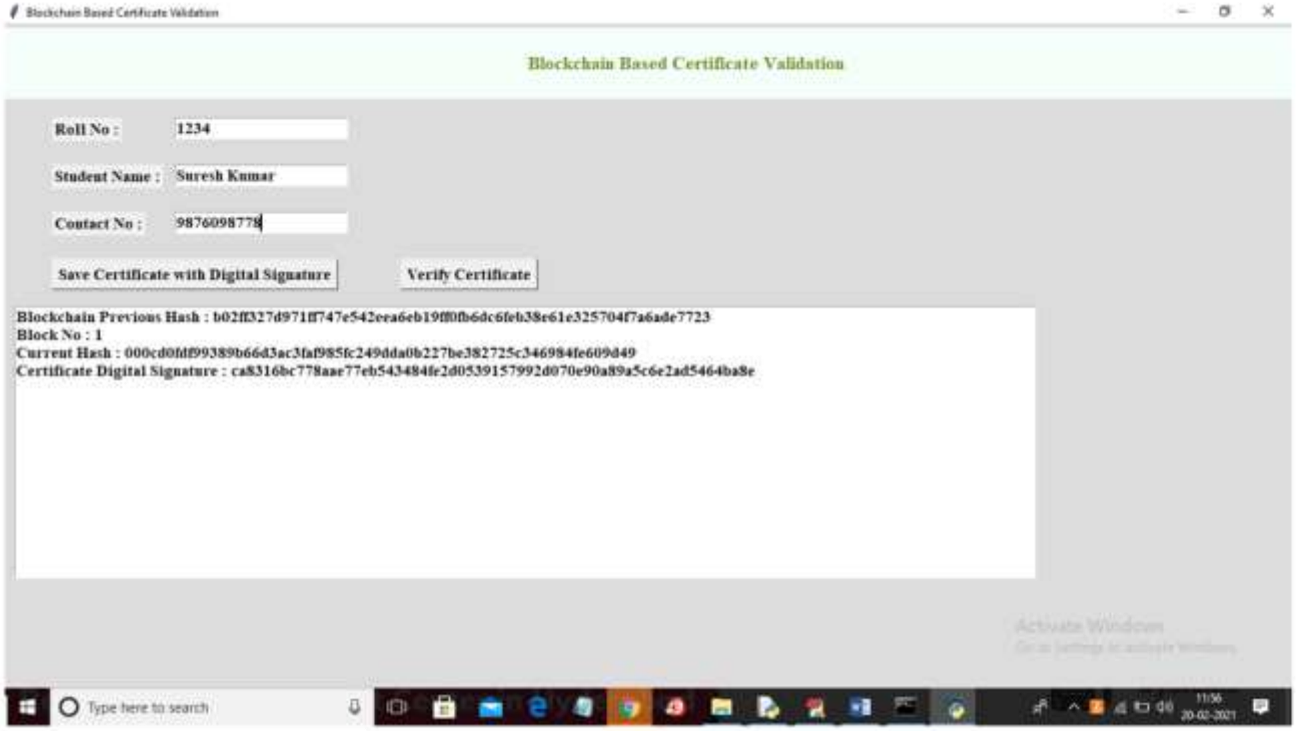
Roll No : 1234

Student Name : Suresh Kumar

Contact No : 9876098778

File name: 1.jpg

Fig-2: 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


Blockchain Based Certificate Validation
Blockchain Based Certificate Validation
Save Certificate with Digital Signature
Verify Certificate
Type here to search

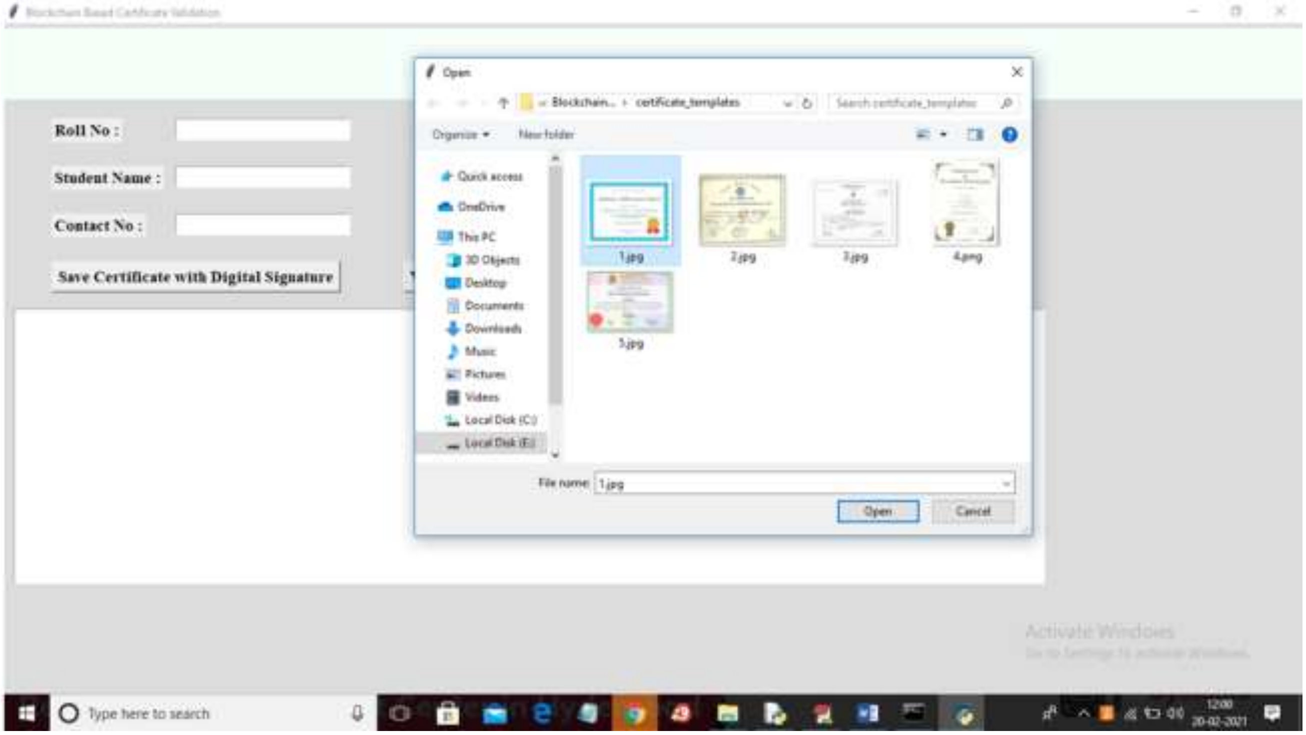
Roll No : 1234

Student Name : Suresh Kumar

Contact No : 9876098778

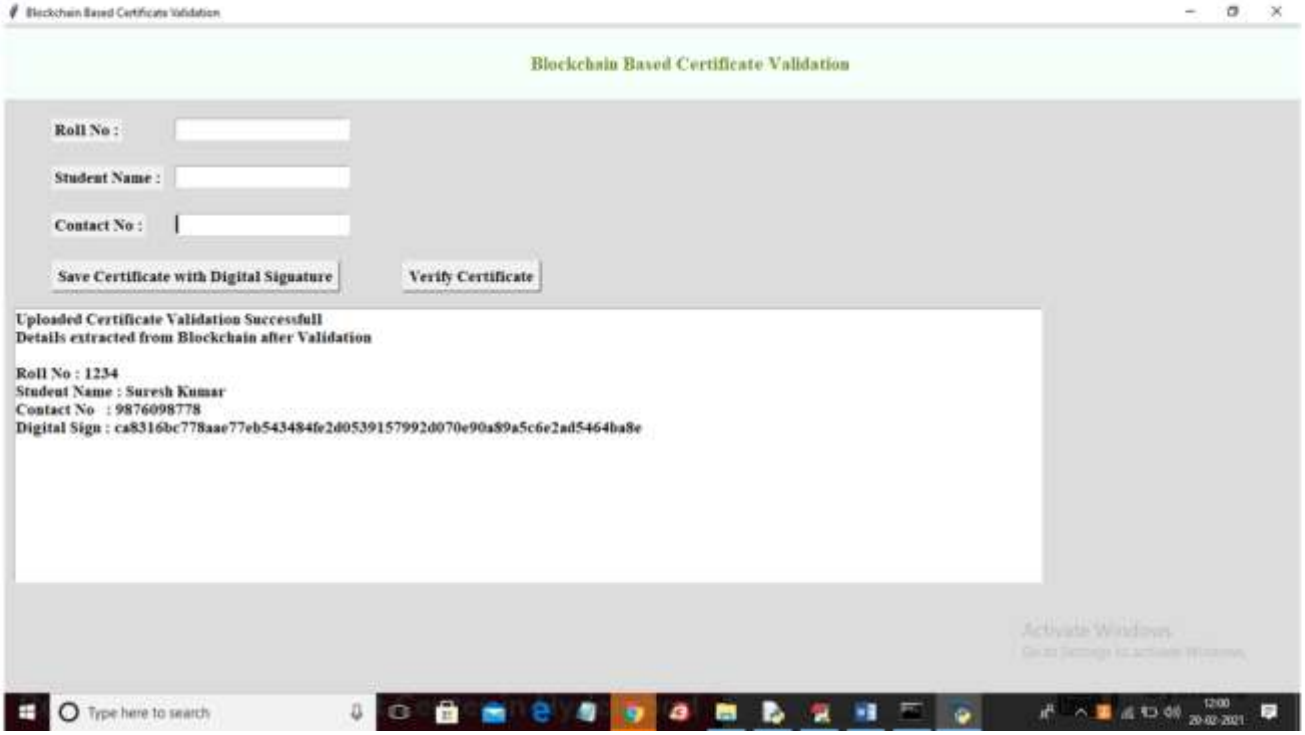
```
Blockchain Previous Hash : b02ff327d971ff747e542eea6eb19ff0fb6dc6feb38e61e325704f7a6ade7723
Block No : 1
Current Hash : 000cd0fdf99389b66d3ac3faf985fc249dda0b227be382725c346984fe609d49
Certificate Digital Signature : ca8316bc778aae77eb543484fe2d0539157992d070e90a89a5c6e2ad5464ba8e
```

Fig-3: 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.



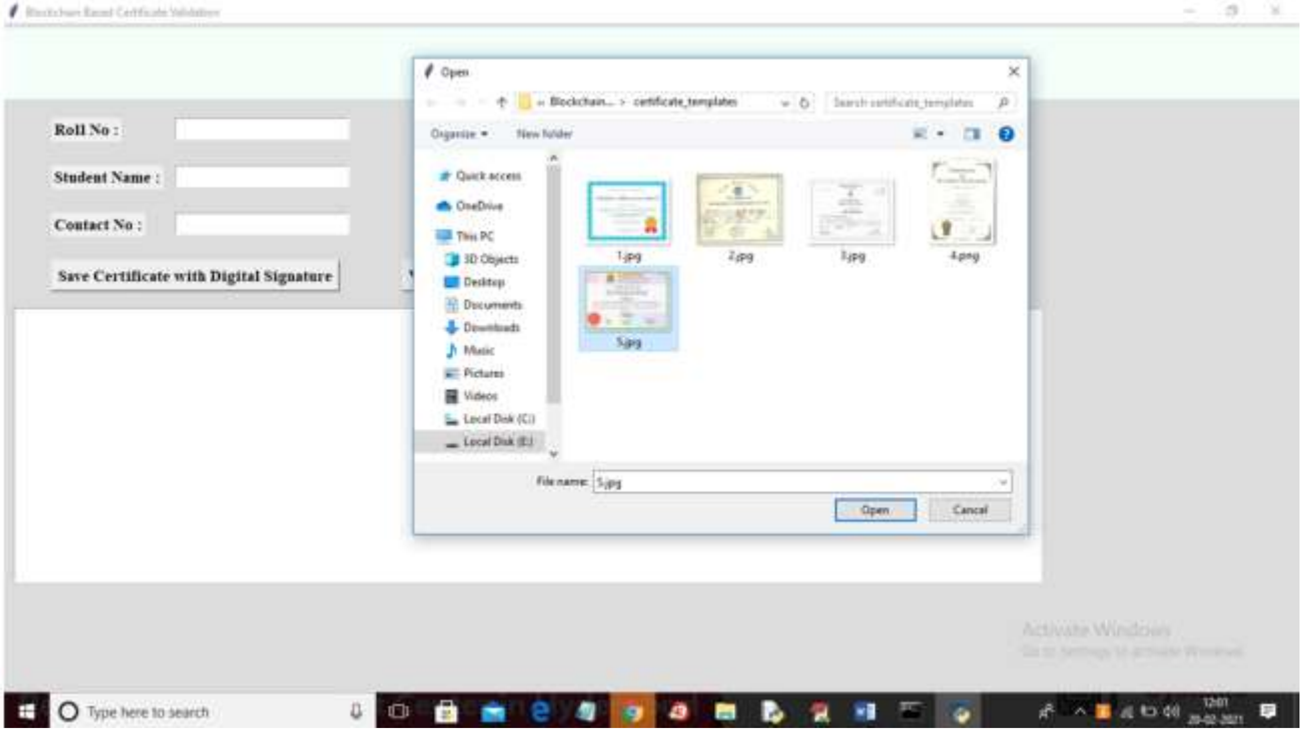
File name: 1.jpg

Fig-4: selecting and uploading '1.jpg' file and then click on 'Open' button to get below result.


Blockchain Based Certificate Validation
Blockchain Based Certificate Validation
Roll No :
Student Name :
Contact No :
Save Certificate with Digital Signature
Verify Certificate
Activate Windows
Go to Settings to activate Windows.
Type here to search
12:00
20-02-2021

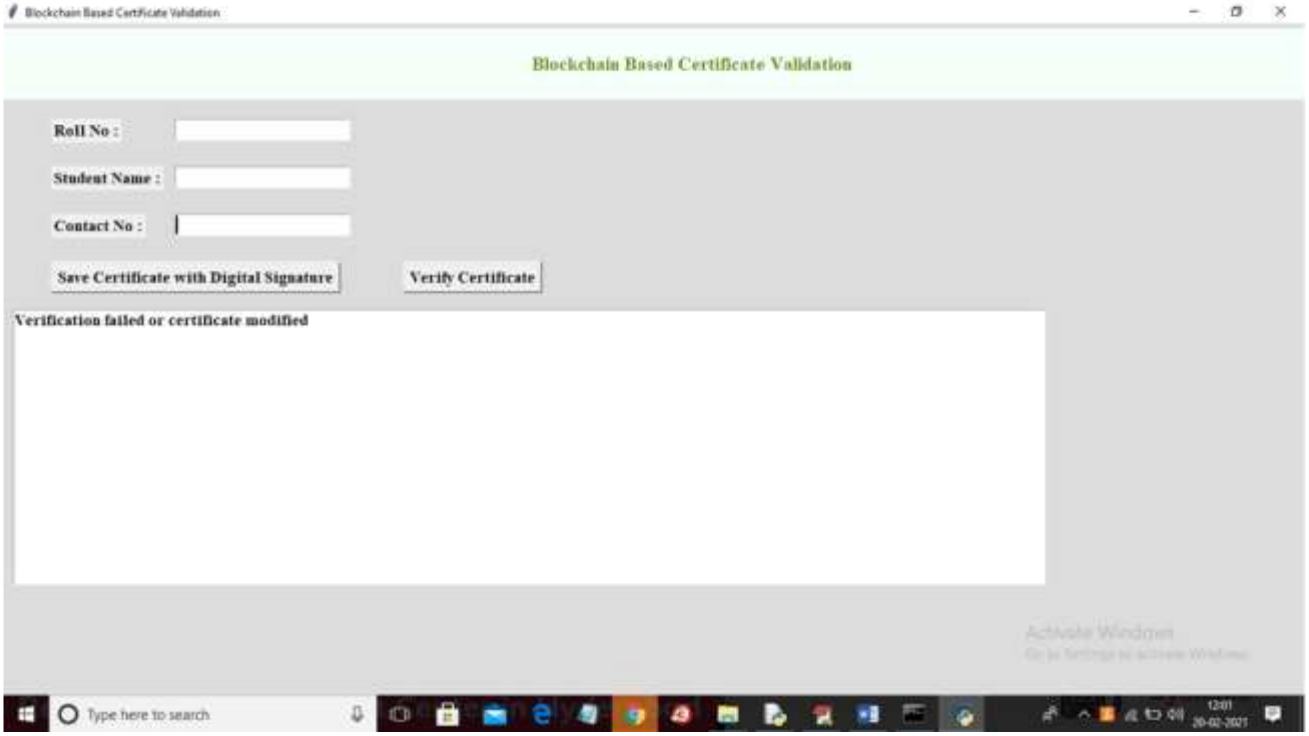
```
Uploaded Certificate Validation Successfull
Details extracted from Blockchain after Validation

Roll No : 1234
Student Name : Suresh Kumar
Contact No   : 9876098778
Digital Sign : ca8316bc778aae77eb543484fe2d0539157992d070e90a89a5c6e2ad5464ba8e
```

Fig-5: we uploaded same and correct image so application matched digital signature and then retrieve details from Blockchain and now try with some other image.



File name: 5.jpg

Fig-6: selecting and uploading '5.jpg' file and then click on 'Open' button to get below result.


Blockchain Based Certificate Validation
Blockchain Based Certificate Validation
Roll No :
Student Name :
Contact No :
Save Certificate with Digital Signature
Verify Certificate
Activate Windows
Go to Settings to activate Windows.
Type here to search

Verification failed or certificate modified

Fig-7: screen verification got failed as uploaded certificate not matched with stored certificates in

Blockchain.

6 CONCLUSION AND FUTURE WORK:

In contrast to current solutions that rely on third party arbitration, the MIT Media Lab published their blockchain-based credential system in June 2016. It is more secure, more dependable, and difficult to forge. However, the project's prevalence and scope are constrained by certain significant authentication flaws and a weak revocation mechanism. In our project, we developed and designed a series of novel cryptographic protocols, including multi-signature, BTC-address-state-based revocation mechanism, and trustworthy federated identification, to overcome these issues and make its concept more workable.

Given that each issuing progress must be signed by the majority of the academic committee members, the multi-signature method among these protocols significantly raises the difficulty of forging. Additionally, because the private keys are held by various devices and persons, it improves the security of the private key storage. Additionally, the stability of the certificate revocation was increased by the BTC-address-based revocation process because BTC addresses are always accessible and reliable. Additionally, this strategy decreased the likelihood that revocation would fail because the cancellation process used the same multi-signature technique that involved several signatories. Through the trusted path and federated identity, trusted federated identity creatively demonstrated the validity of the certificate. Additionally, the protocol of our study can be used to other related fields like contract proofing and digital right protection. As an illustration, our protocol allows the two businesses to link their contract to the block chain using multisignature, as opposed to the conventional third party-based work mode, which allays concerns about credentials forging.

Additionally, we used Java and JavaScript to develop a blockchain-based certificate system that incorporated all of the aforementioned protocols. This solution has partially fixed the flaw in Blockcerts, making the principle of a blockchain-based certificate more workable. Finally, we carried out a number of security evaluations from the angles of operational safety, data security, network security, and protocol security. The results of the assessment offer convincing proof that the system is secure enough to adhere to enterprise application standards.

Last but not least, there are still some restrictions that need to be considered, even if they are outside the purview of this paper: Our project is built on the Bitcoin blockchain, which is supported by thousands of users throughout the cryptocurrency community. It is unwise to presume that the Bitcoin system will continue to function well in the future because a wide range of stakeholders can affect the blockchain ecosystem or business model. In the coming years, we'll use a variety of blockchain technologies, including Hyperledger and Ethereum, to do rid of the sources of instability.

7 REFERENCES

1. Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome, https://www.ithome.com.tw/news/105374.
2. JingyuanGao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age, https://www.bnext.com.tw/article/47456/bitcoinether-li tecoin-ripple-differences-betweencryptocurrencies.
3. Smart contractswhitepaper, https://github.com/OSELab/learning-blockchain/blob/master/ethereum/smart-contracts.md.

4. Gong Chen, Development and Application of Smart Contracts, https://www.fisc.com.tw/Upload/b0499306-1905- 4531-888a-2bc4c1ddb391/TC/9005.pdf.

5. Weiwei He, Exempted from cumbersome auditing and issuance procedures, several national junior diplomas will debut next year.iThome, https://www.ithome.com.tw/news/119252.
6. Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the EthereumBlockchain",Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.

7. Yong Shi, "Secure storage service of electronic ballot system based on block chain algorithm", Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.
8. ZhenzhiQiu, "Digital certificate for a painting based on blockchain technology", Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
9. Weiwen Yang, Global blockchain development status and trends, http://nmarlt.pixnet.net/blog/post/65851006-%E5%85% A8%E7%90%83%E5%8D%80 %E5%A1%8A%E9 %8 F%88%E7%99%BC%E5%B1%95%E7%8F%BE% E6 %B3%81%E8%88%87%E8%B6%A8%E5%8B%A 2.
10. Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

11. Chris Dannen, IntroducingEthereum and Solidity, https://www.apress.com/br/book/9781484225349.
12. Jan Xie, Serpent GitHub, https://github.com/ethereum/wiki/wiki/%5B%E4%B 8% AD%E6%96%87%5DSerpent%E6%8C%87%E5%8D %97 Solidity , https://solidity.readthedocs.io/en/latest/index.html.