iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50126

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

An Application for E-Certificate Verification and Validation using Blockchain

Harika Pampana[1], Sai Priya Reddy[2], Shaik Madeena[3], Rohit Goud[4], Associate Prof. Bijaya Kumar Sethi[5]
Department of CSE, Vardhaman College of Engineering, Telangana, India

Abstract: ***According to statistics from the Indian Ministry of Education, there are roughly one million graduates each year. Some of them will continue their education at high schools or university institutions while others will be prepared to find employment.***
The students various great performance certificates, score transcripts, diplomas, etc., will serve as a crucial point of reference for admission to new institutions or jobs when they have completed their studies. Only the names of the schools and the students are entered when issuing different honours or certificates.
Events that lead to the graduation certificate being forged are frequently recognised since there is no reliable anti-forge system. The digital certificate system based on blockchain technology would be suggested as a solution to the issue of certificate forgery A digital certificate with anti-counterfeit and verifiability could be created thanks to the blockchain's changeable property. This is the process for issuing a digital certificate in this system. Create an electronic copy of the paper certificate along with any related data and insert it into the database first.
In the meantime, determine the electronic file's hash value. Last but not least, add the hash value to the block in the chain system.
A linked QR-code and an inquiry string code will be generated by the system and attached to the paper certificate. By scanning the paper certificate with a phone or conducting online searches, the demand unit will be able to confirm its legitimacy. By utilising the blockchain's customizable qualities, the solution not only increases the legitimacy of diverse paper-based certificates, but also significantly lowers the danger of certificate loss.

I. INTRODUCTION

2008 saw the debut of blockchain, according to Satoshi Nakamoto. Blockchain is one of the internet ledgers that offers transparent and decentralised data sharing. In this project, we create an Android app that offers safe verification of our certificates. So, there is a great need for an effective process that can ensure that the information in such certifications is original, which indicates the document has come from a trustworthy and approved source and is not falsified. using data from current pupils, an electronic certificate generating system manually produces the certificates. The verification process is comparable across several centralised techniques.

The many network attacks, such as SQL injection, collusion, brute force, etc., cannot be protected against by centralised approaches. Using a decentralised methodology, blockchain approach. Fog networking, also referred to as fogging, is pushing the limits of computing programmes, data, and services away from the centralised cloud and towards the logical stream of the network edge. Instead of using network switches and gateways that are integrated into the LTE network for primary control, the fog networking system works to construct control, configuration, and management via the Internet backbone. By utilising edge server nodes, the fog computing architecture may be seen as a highly virtualized computing infrastructure that offers hierarchical computing capabilities. The numerous apps and services are organised by these fog nodes to store and process the data close to end users. With the aid of edge server nodes, we can clarify the fog computing architecture as a highly virtualized computing infrastructure that offers hierarchical computing capabilities.

These fog nodes coordinate a variety of services and apps to process and store content close to end users. This research to design and develop a system for dynamic and secure e certificate generation system using smart contracts in a blockchain environment. In this work, we also illustrate our own blockchain in an open-source environment with a custom mining strategy as well as a smart contract .

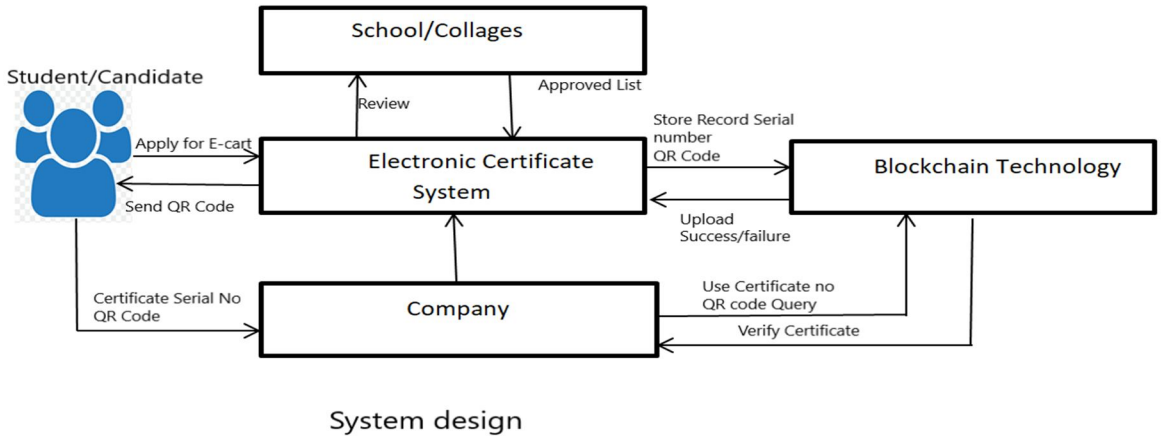


Fig 1: Block Diagram

The initiative aims to reduce database fraud from different attacks, increase transaction transparency, and do away with the cumbersome certificate verification process for organisations. extra to boost system confidence.system for creating electronic certificates by hand using information about present students. Different centralised methods handle verification in a similar way.The project's goal is to show that centralised defences fall short against a variety of network assaults similar to SQL injection, collaboration, and roared force, etc. a decentralised method using block chain technology. The manual creation of certificates using a blockchain-based decentralised system based on the data of present students is done in order to improve the user experiencee . Many use scenarios for electronic certificate transaction, which face comparable Communication and info sharing issues, would surely benefit greatly from an interoperable design. From a more technical perspective, significant investigation is required to identify the most feasible design approach for developing an Blockchain technology is used to create an interoperable environment while maintaining critical security and confidentiality. considerations in E-certificate transactions.

II. LITERATURE REVIEW

A. Blockchain and Reasonable Contract for Digital Certificate

To address the issue of certificate forgery, a blockchain-based digital certificate system would be developed. Digital licences with verification and anti-copying can be created thanks to the immutability of blockchains. Following is the procedure for issuing digital certificates using this technique. The hash price of an electronic file created from the linked alternative connected information of a paper certificate is first determined.In the chain structure, the block retains the hash price.The system creates a query string code and a QR code for the certificate, which are then printed on document proof. Through online searches or mobile phone scanning, a requirement device is available to verify the validity of the paper certificate. Due to the blockchain's immutability, the system increases the legitimacy of different paper-based certificates while at the same time electronically lowering their loss risks.

B. Validation through Public Ledgers and Blockchain

PKIs are essential for the continued existence of internet services that rely on certificate-based verification, including email, social networking, cloud services, e-government, trade sector, and online banking, among many others. One of the most frequent point of failure for contemporary PKIs is the security and dependability of award cancellation records, which must always be accessible and genuine. (public key infrastructures) . Historically, The certification body kept track of the CRL for a group of certificates (CA) that granted them, adding one POF to the system.We frequently propose a remedy to this issue wherein a number of CAs pool their CRLs into a robust, open ledger. For this, we frequently take into account the blockchain-based public database model, which was developed for use with cryptocurrencies and is currently a well-liked choice for numerous online applications with strict security and dependability requirements.

C. A flexible and lightweight blockchain protocol is "Proof-of-Property"

The approach described in this paper builds on Ethereum's principle that the system state should only be present in however, it extends this idea by incorporating pertinent elements of this system state in fresh transactions. As a result, it is not necessary to transfer the blockchain in its entirety at first, and various participants can now view inbound transactions. These concepts will allow use cases that call for scalable blockchain technology but don't necessarily demand an endless and exhaustive group action history

D. Secure knowledge cradle management using Blockchain and sensible contracts

They use blockchain as a platform in this work to create reliable knowledge cradle selection, verification, and administration. The created system effectively records changeless knowledge paths through the utilising open cradle paradigm and sensible contracts (OPM). The study shows that the proposed framework will successfully and firmly capture, check or validate cradle knowledgeand guard against harmful modifications to the captured knowledge, provided that the majority of participants are truthful.

E. Secure storage service for supported block chain algorithm for electronic voting

In this essay, the authors use the free and open-source Blockchain technology to create a cutting-edge concept for an electronic judicial system that would be used in regional or governmental elections Increased voting turnout is possible thanks to the blockchain-based system's security, dependability, and anonymity as well as people's increased confidence in the governments.

F. An historical Study of Localized Applications Based on Blockchain

This paper provides a thorough empirical investigation on a detailed dataset of 734 distributed applications (dapps) that was gathered from three well-known open localised application Ethereum, State of the Dapp, and DAppRadar are examples of markets. We typically look at how dapps are identified and offer the ephemeral patterns of how logical contracts are organised within a dapp. We frequently draw some conclusions from the findings to aid dapp users and devs in better comprehending and deploying dapps.

G. sCompile: Critical Path Analysis and Identification for Practical Contracts

Another method to automatically identify critical programme methods (with multiple perform calls as well as inter-contract perform calls) It is intended that during a reasonable contract, the methods will be ranked in terms of how important they are, discarded if they are impractical, or otherwise given user-friendly cautions for user review. Prioritizing those that undoubtedly violate crucial properties while identifying crucial methods that entail financial group action. Only high hierarchical crucial methods are used with symbolic execution approaches for quantifiability. This strategy was implemented in a tool called Compile that was used to apply 36,099 reasonable contracts. The experiment's findings demonstrate the efficiency of Compile, with one reasonable contract typically taking five seconds to construct.

III. METHODOLOGY

Today's students graduate with a range of diplomas. Students produce these certifications while looking for employment in the public or private industries, where these types of certificates must be manually established. Although it can be challenging to spot them, instances where students also fabricate false certificates do occur. The teaching network has long been concerned about the problem of fake academic credentials. Their verification can be very challenging due to the ease with which such certificates can be produced and the necessity of personally inspecting them. The block chain-based virtual certificate store also aids in resolving this problem.

A. Disadvantages Of Existing System The Basic Disadvantages Include

For educational organizations, several methods have been developed to protect electronic certificates and store them safely in the cloud. Digital signatures, which provide verification, integrity, and non-repudiation in digital documents, are one of the technologies that emerge in the security fields. The primary tool for handling this need is block chain, and when combined with various hashing methods, it becomes an effective method for data security. Additionally, it aids in eliminating the requirement for ongoing certificate verification.

B. Proposed System

The proposed system uses sampling and quantization to convert the academic and athletic certificates into digital certificates. The blocks are then supplemented with the certificates and the digital certificates' hash values. the unpredictable method that generated a hash number. The hash value, timestamp, and hash of the preceding block are all included in each block. By joining these components, block chain is produced. The school registers pupil information by entering information like a name and email address in our interface (application), and this data is then stored in the database.

Together, the application and the certificate the registrar provided form a block chain .Information about the pupil will enable the organisation or verifier to validate the certificate. To create dynamic certificates, the algorithm recommended using a separate, proprietary block chain. The first student applies for an e-certificate online and uploads it along with all the necessary academic paperwork. The web portal authenticates a trustworthy third party who checks all papers from the institution, school, colleges, etc. The block chain will simultaneously keep data and a special certificate id or QR code is created and given back to the student once university, school, and college verification has been successfully completed. The student can show the group the QR code or certificate ID they were given in place of submitting a physical copy of the document. Companies can add a QR code or an ID to the website, combine the associated student's e-certificate, and produce the validation.

C. Modules

To avoid certificate forgery we are adding certificate verification mechanism using Block chain technology and this project consists of 3 modules

1) *Admin:* Admin is an education authority which login to system using username and password as ‘admin’ and ‘admin’. After login admin will upload student details and certificate and this details will be uploaded to Block chain and Block chain associate each certificate with unique hash code called as digital signature. QR CODE will also be generated on Hash code and affix on student certificate and this QR CODE can be scanned from mobile to get details from Block chain and if QR CODE exists in Block chain then certificate validation successful.
2) *Company:* Company user can sign up and login to system and then scan and upload certificate and then application will generate digital signature and matched with those signature stored in Block chain and if certificate is original then same signature will be generated and authentication will be successful.
3) *Scanner Module:* This is a standalone module which will maintain by education institution and companies and using this module they can scan QR CODE to get details from Block chain.

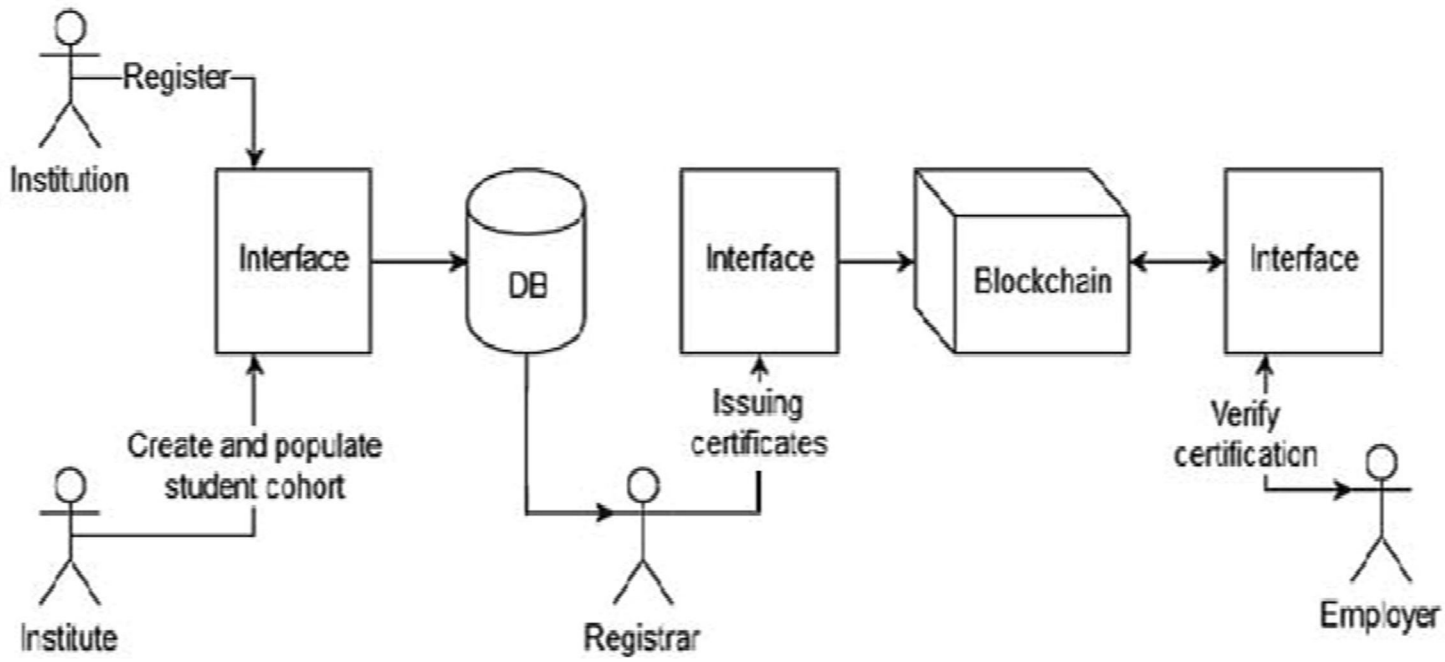


Fig 2: System Architechture

D. Advantages of Proposed System

1) Using blockchain technology, supply chain applications may be moved from centralised servers (single server storage) to decentralised Blockchain servers (where data will be stored at multiple nodes or server).

2) In Blockchain innovation, similar exchange information is saved money on numerous servers with hash code check, and assuming information changes on one server, it is found on another server in light of the fact that the hash code for similar information changes.

3) It has a larger storage capacity.

4) It keeps track of all category, order, and other information.

5) Control over Fraud.

6) Transparency system.

7) Eradicate the problem.

IV. IMPLEMENTATION

The Project is designed and developed by using Secure Hash Algorithm, mining and validation.

The Secure Hash Algorithm (SHA) is a family of cryptographic hash functions that are widely used in computer security applications. The algorithms in the SHA family are designed to generate a fixed-size output (typically 160, 224, or 256 bits) from a variable-length input message. The most widely used member of the SHA family is SHA-256, which produces a 256-bit hash value. It is used in a wide range of security applications, including digital signatures, password storage, and file integrity checks. The basic operation of the SHA algorithm involves dividing the input message into fixed-size blocks and processing each block through a series of mathematical operations. The result of this processing is a fixed-size output, which is known as the hash value. One of the key properties of a cryptographic hash function is that it is practically impossible to generate the same hash value from two different input messages. This property is known as collision resistance and is essential for the security of the hash function. In addition to collision resistance, SHA-256 also provides other security features, such as preimage resistance (which makes it difficult to determine the input message from the hash value) and resistance to birthday attacks Overall, the SHA family of algorithms provides a robust and widely used solution for cryptographic hashing needs.

In validation order to make sure that the data entered by a person is legitimate, an input validation algorithm is used. A programme might ask for a score between 0 and 50, for instance, and use an input validation algorithm to make sure that figures below 0 and above 50 are rejected. We must create a SOLIDITY contract with functions to keep and authenticate certificate details in order to store data in the blockchain. This solidity contract must be deployed on the Ethereum blockchain before returning the address where the contract was deployed. We can use this address in Python code to store and retrieve certificate information.

V. EXPERIMENTAL RESULTS

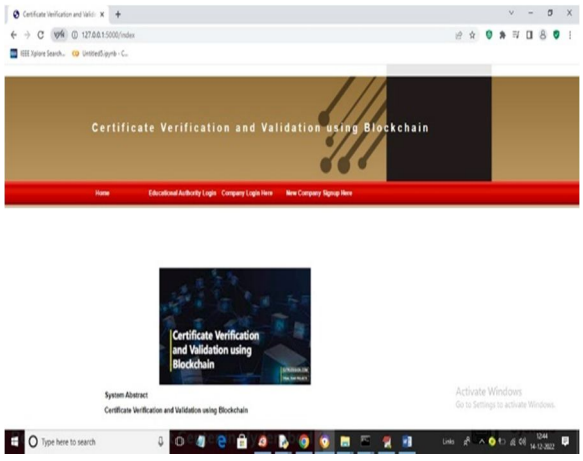


Fig.3: Main screen

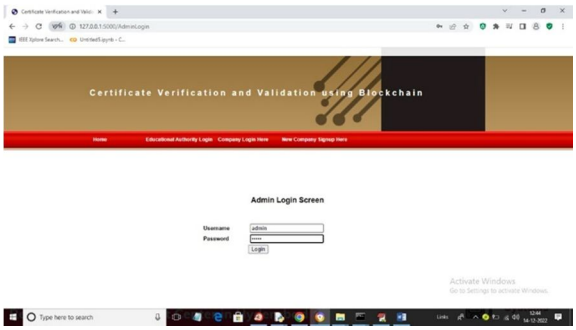


Fig.4: Admin Login

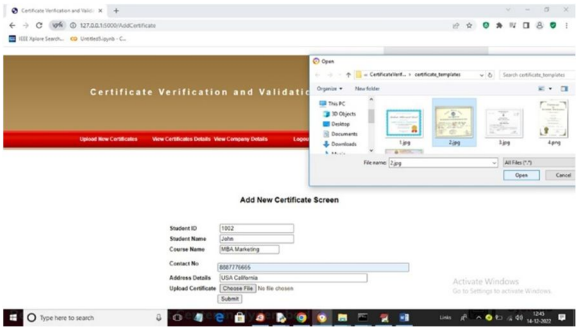


Fig.5: Certificate Upload

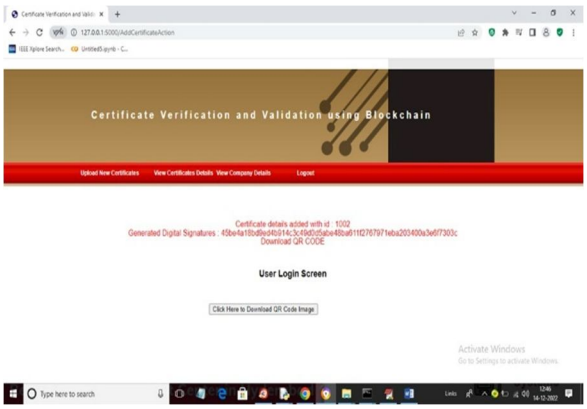
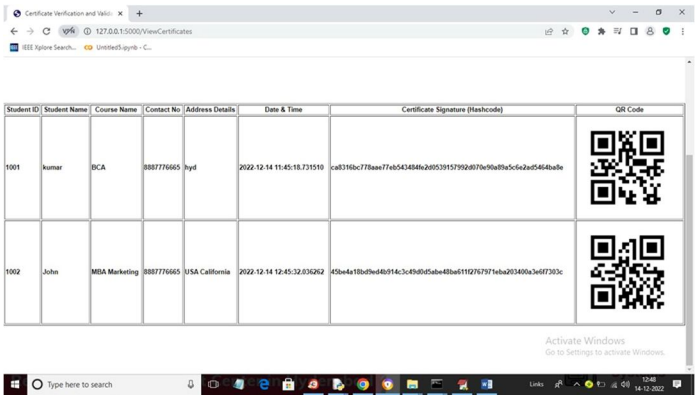


Fig.6: Download QR code



Student ID	Student Name	Course Name	Contact No	Address Details	Date & Time	Certificate Signature (Hashcode)	QR Code
1001	kumar	BCA	8887776665	hyd	2022-12-14 11:45:18.731510	ca8316bc778aae77eb543484fe2d053915799 2d070e90a89a5c6e2ed5464ba8e	
1002	John	MBA Marketing	8887776665	USA California	2022-12-14 12:45:32.036262	45be4a18bd9ed4b914c3c49d0d5abe48ba611f2767971eba203400a3e6f7303c	

Fig.7: View Certificates Uploaded

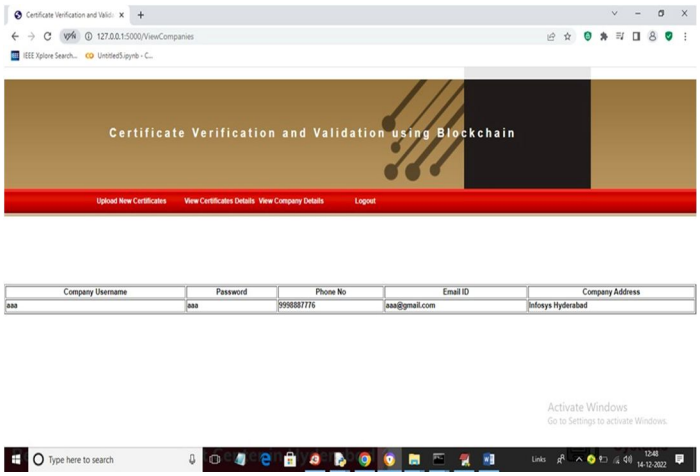


Fig.8: View Registered companies

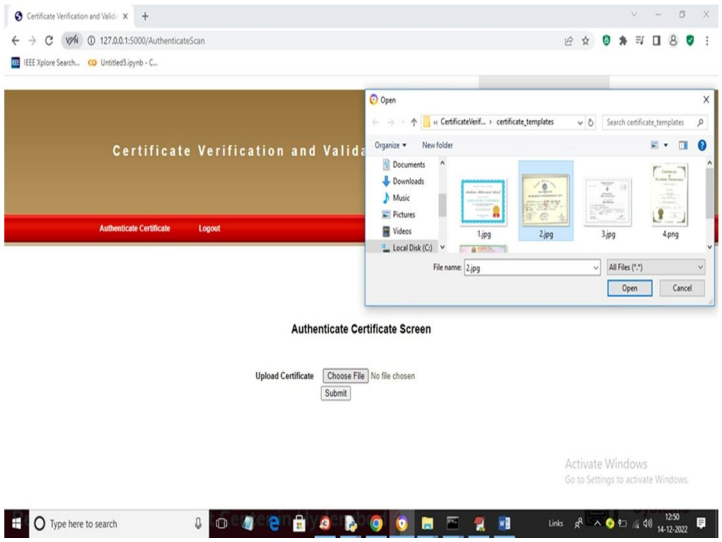


Fig.9: Upload Certificate to authenticate in company module

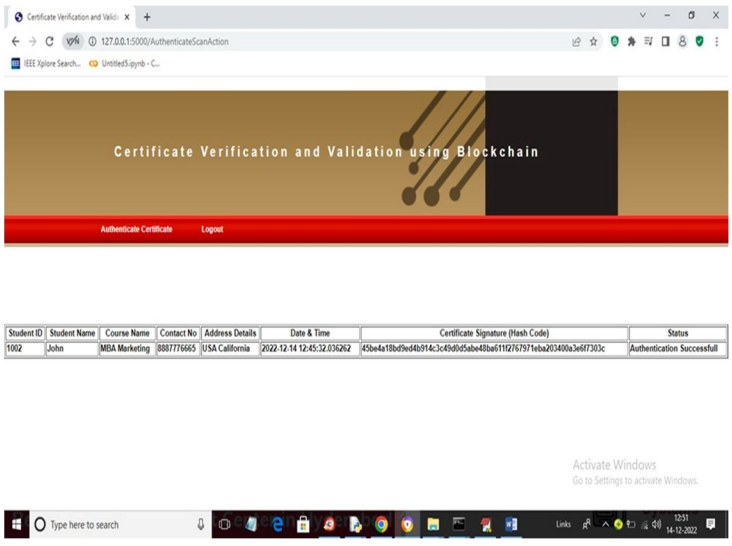


Fig.10: Authentication Successful

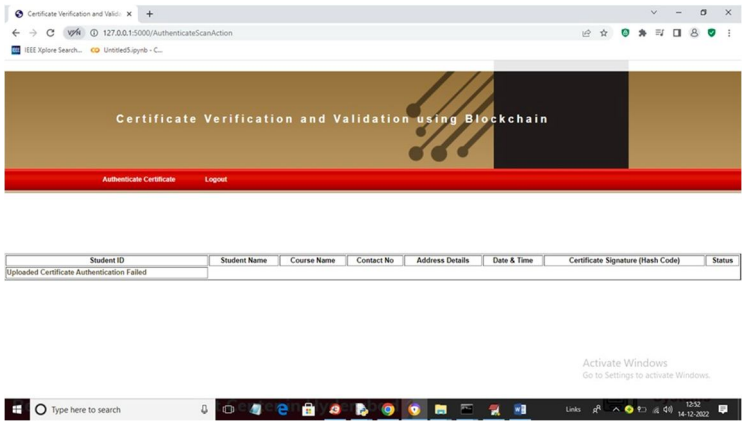


Fig.11: Authentication Failed

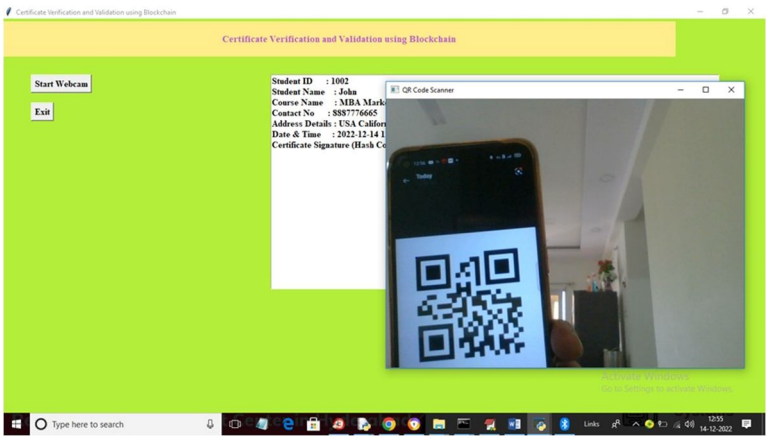


Fig.12: QR code Authentication Successful

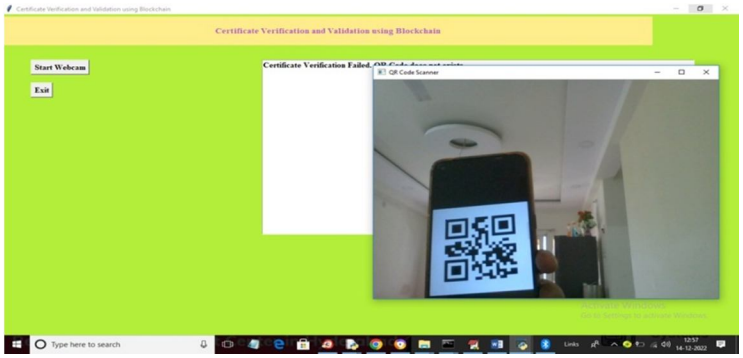


Fig.13: QR code Authentication Failed

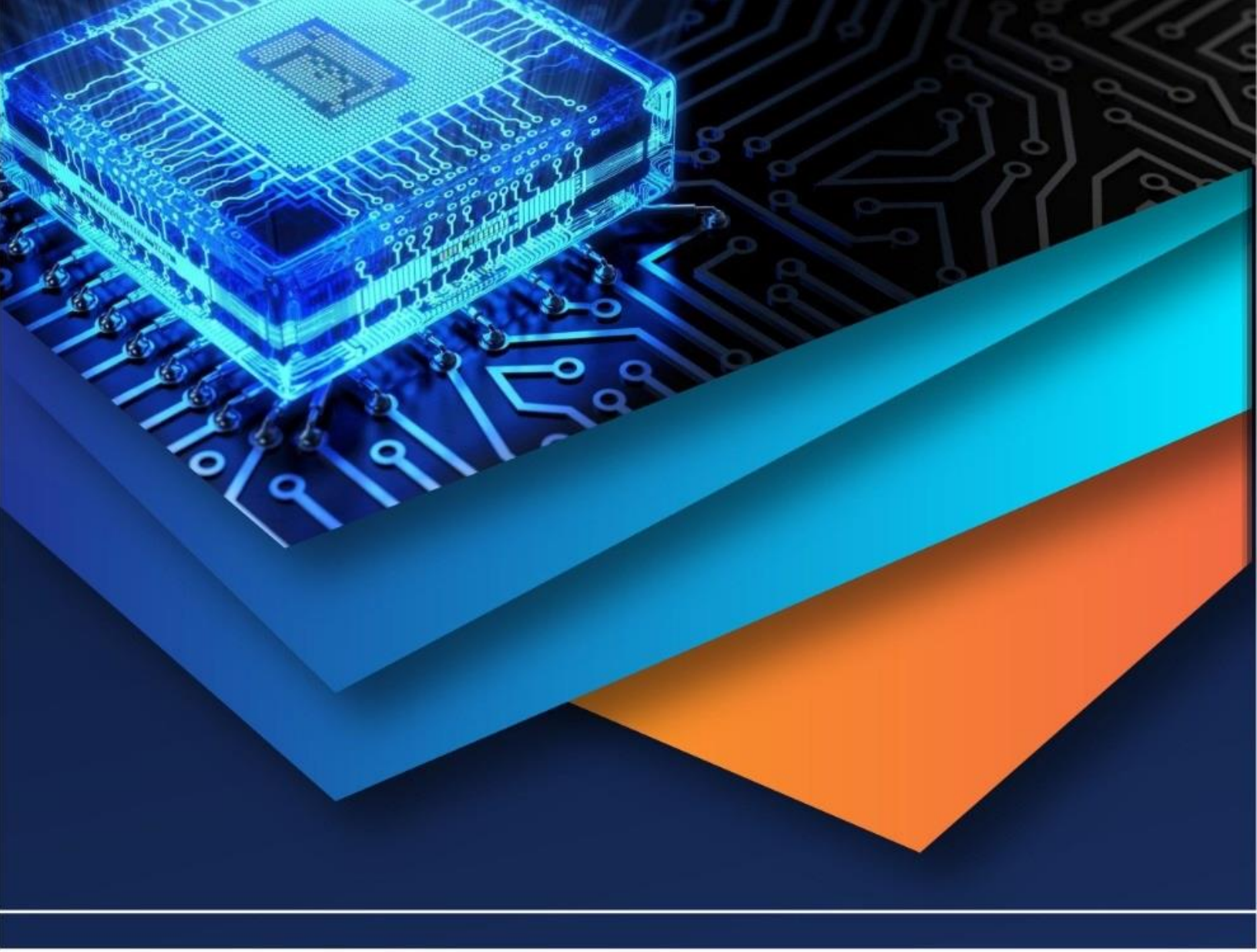
VI. CONCLUSION

Due to the complexity of the E-certificate transaction and the need for more reliable and efficient information technology systems, there are many study directions in the application of Blockchain technology to this type of transaction. Many E-certificate transaction use cases would surely benefit greatly from an interoperable design given the similar data sharing and communication problems they encounter. From a more technical standpoint, extensive research is required to identify the most feasible design approach for developing a compliant ecosystem using Blockchain technology while balancing significant security and confidentiality issues in E-certificate transactions. To educate software engineers and subject matter experts on the potential and restrictions of this new technology, more research on secure and effective software practises is required whether or not to create a decentralised application leveraging an existing Blockchain.

We proposed a solution to the problem of certificate forgery based on blockchain technology. Providing security to the data is very important. By using the unchallengeable property of blockchain, we can provide more security for data and reduce the certificate forgery. The application can allow the user to view and validate the certificate. This system guarantees information accuracy and security and easy for people to manage digital certificates.

REFERENCES

[1] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.
[2] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.
[3] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.
[4] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain
[5] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.
[6] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, " Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.
[7] S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology.
[8] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY