IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 13, Iss 04, 2024

CERTIFICATE VALIDATION USING BLOCKCHAIN

Shiva Prasad1, T.Vyshnavi2, M.Shriya3, P.SaiKiran4, K.Prabhas5, A. Swathi[6]

[1,6] Assistant Professor, Department of CSE, Balaji Institute of Technology and Science, Laknepally,

Warangal, India

[2,3,4,5] B.Tech Student, Department of CSE, Balaji Institute of Technology and Science, Laknepally,

Warangal, India

ABSTRACT

Blockchain technology can be used to validate certificates by generating digital certificates that are easy to verify and resistant to counterfeiting. In the digital world, each and every thing are digitized in which the academic certificates digitalized in the educational institution and provided to the students. The increase in security breaches compromise user's privacy of academic digital certificate. The institution and organization find it very difficult to validate and verify the digital certificates. By using blockchain technology we can provide a more secure and efficient digital certificate validation. First, generate the electronic file of a paper certificate accompanying other related data into the database,meanwhilecalculatetheelectronicfileforitshashvalue.Finally,store thehashvalueintotheblockinthechainsystem.Itwillprovidethedemandunit to verify the authenticity of the paper certificate through mobilephone scanning orwebsiteinquiries.Throughtheunmodifiablepropertiesoftheblockchain,the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates. In this project to secureacademiccertificateand foraccuratemanagement and to avoid forgecertificatewareconvertingallcertificatesintodigitalsignaturesandthese digital signatures will be stored in Block chain server as this Block chain server supporttamperproofdatastorageandnobodycanhackoralterits dataandifby achanceifitsdataalterthenverificationgetfailedatnextblockstorageanduser may get intimation about data alter.

Keywords: Certificatevalidation,Cryptography,Digitalcredentials, Authentication, Secure verification.

1. INTRODUCTION

The project aims to combat certificate forgery, a growing concern in education and employment. Conventional methods are manual and paper-based, prone to forgery, time-consuming, and error-prone. The project leverages Blockchain technology to overcome Traditional drawbacks.

Blockchain is a decentralized, immutable data storage system which generates unique hash codes for data integrity. Ethereum is used as the underlying blockchain platform for deploying Solidity smart contracts to store and verify certificatedatasecurely.Theprojectaimstocombatcertificateforgery,agrowing concern in education and employment. Conventional methods are manual and paper-based, prone to forgery, time-consuming, and error-prone. The project leveragesBlockchaintechnologytoovercomeTraditionaldrawbacksBlockchain is a decentralized, immutable data storage system which generates unique hash codes for dataintegrity. Ethereum is used as the underlyingblockchainplatform fordeployingSoliditysmartcontractstostoreandverifycertificatedatasecurely, Blockchain is a distributed database that is widely used for recording distinct transactions.Onceaconsensusisreachedamongdifferentnodes,thetransaction isaddedtoablockthatalreadyholdsrecordsofseveraltransactions.Eachblock contains the hash value of its last counterpart for connection.All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together, under blockchain, a block becomes validated only once it has been verified by multiple. Objectives Inthisstudy,wedevelopedadecentralizedapplicationanddesignedacertificate system based on Ethereum blockchain. This technology was selected because it is incorruptible, encrypted, and trackable and permits data synchronization. Blockchain technology can be used to validate certificates by generating digital certificates that are easy to verify and resistant to counterfeiting.

Overall, certificate verification is a crucial process that verifies the integrity of digital certificates, ensuring secure communication, data exchange, and trusted identities. Traditional certificate validation methods rely on centralized trust authorities, which can be vulnerable to single-point failures. By leveraging blockchain's inherent security features, certificate validation can be made more efficient and trustworthy.

2. LITERATURESURVEY

Recent studies reveal about digital certificate validation, certificate validation, hybrid blockchain, verification and validation. Based on recent investigation we are highlighting the security, transparency, decentralization, automation, scalability, interoperability, improved trust, compliance, cost-effectiveness, faster verification.Thesehighlightsdemonstratethepotentialofblockchaintechnology to transform certificate validation processes, making them more trustworthy. In investigation process we came to know that from recent studies researchers developed various innovative solutions for certificate validation using blockchain, including blockchain-based certificate verification systems, smart contrast-based certificate validation, decentralized certificate authorities, and certificate transparency protocols. They have also designed identity verification systems, decentralized certificate revocation lists.When conducting a literature surveyoncertificatevalidationusingblockchain,it'sessentialtoexploreresearch papers, articles, and projects by various authors and institutions who have made significant contributions to this field. MIT Media Lab – Blockcerts(2016) was developed as an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. They used some models such as Open Badges, lockcerts, certified data, decentralized identifier (DID), verifiable credentials, smart contrast-based certificate validation. Sony Global Education (2016) partnered with IBM to develop a blockchain-based system for managing educational records and certificates. This system ensures that credentials are securely stored and easily verifiable. European Union Blockchain Observatory and Forum (2018) the EU Blockchain Observatory has explored the use of blockchain for various applications, including certificate validation. They have conductedresearchonhowblockchaincanenhancetransparencyandsecurityin credentialing systems.University of Nicosia-Digital Currency and Blockchain Technology (2017)The University of Nicosia was one of the first institutions to issue academic certificates on the blockchain. They have also conducted extensive research on the potential of blockchain in various sectors, including education.Thestudyfocusesonexploringthepotentialofblockchaintechnology to secure. This involves researching how blockchain's decentralized and immutable nature can be leveraged to prevent certificate tampering and forgery and ensure data integrity and authenticity and transparently validate digital certificates,suchasacademiccredentials,professionalcertifications,andidentity documents.

The article proposed to enhance the security, transparency, and efficiency of certificatevalidationprocesses.Itaimstointroducetheconcept,explainbenefits, describearchitecture,discussimplementation,evaluateperformance,andexplore futuredirectionsofblockchain-basedcertificatevalidation.seekstocontributeto scientific communities, industry publications, conference proceedings, technical reports,whitepapers,businessandtechnologymagazines,onlineplatforms, educationalresources,researchpapers,andcasestudies.Bypublishingthearticle, authors aim to share expertise, experiences, and research, contributing to the growth and adoption of

blockchain technology in certificate validation, and transforming the way digital certificates are verified, ensuring their authenticity, integrity, and trustworthiness.

Additionally, when implementing certificate validation using blockchain, it's crucialtochoosetherightblockchainplatform,defineaclearusecase,anddesign a secure architecture that is decentralized, immutable, and transparent. Develop smartcontractscarefully,ensuringtheyaresecure,efficient,andwell-tested.Test and iterateon the design and implementation, collaborating with stakeholders to ensureasmoothuserexperience.Continuouslymonitorandmaintainthesystem to prevent errors and attacks, staying up-to-date with changing laws and regulations. provide user-friendly interfaces and ensure scalability to handle a high volume of certificate validations.By following these guidelines, you can create a secure, efficient, and trustworthy certificate validation system using blockchain technology, transforming the way digital certificates are verifiedand authenticated.

3. EXISTINGSYSTEM

Severalexistingsystemsutilizeblockchainforcertificationvalidation,including blockcerts, opencerts, Uport, certifID. These systems utilize blockchain technology to create secure, decentralized, and transparent certificate validation mechanisms, ensuring the authenticity and integrity of digital certificates. The certificate is 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 privatesectors(banks).thedatamaybechanged,deletedormodified.Certificates are easily hacked and make duplicate of that certificate. Students bring their certificates on interview places. There is no security for certificates. Existing systemslikeBlockcerts,OpenBadges,andCertifiedDataareusefulincertificate validation using blockchain as they provide a secure, decentralized, and transparent way to issue, store, and verify digital certificates. These systems utilize blockchain technology to ensure the authenticity and integrity of certificates, preventing tampering and fraud. They also enable real-time verification, making it easier for employers, educational institutions, and other organizations to validate credentials. Additionally, these systems provide a permanent and immutable record of certificates, reducing the risk of loss or damage. By leveraging blockchain technology, existing systems offer a reliable and trustworthy solution for certificate validation, increasing the confidence of stakeholders in the validity of digital certificates.

In conclusion, existing system in certificate validation uses blockchain ledger, smartcontracts,digitalsignatures,publicandprivatecryptography,decentralized verification,privacyanddatasecurity,thesesystemsdemonstratetheapplication of blockchain technology to certificate validation, utilizing its core features to enhance the reliability, security, and efficiency of credentialing processes.

4. PROBLEMSTATEMENT

The current certification validation processes across various industries, such as education, professional certification, and identity verification, face significant challenges. Traditional methods of verifying academic degrees, professional certifications,andothercredentialsareoftenslow,costly,andvulnerabletofraud. With the growing number of forged certificates and misrepresented qualifications, employers and institutions need a more secure and efficient method to validatecredentials.Existing certification systems rely on centralized databases and manual processes that are prone to errors, delays, and security breaches.Verifying the authenticity of a certificate typically requires contacting theissuinginstitutionorrelyingonthird-partyverificationservices,whichcanbe time-consuming and costly. Furthermore, there is a lack of transparency and accountabilityinthecertificationprocess,makingitdifficulttotrackanychanges or alterations made to the credentials over time.

5. PROPOSEDSYSTEM

Using blockchain andQR code technology for certificateverification is a secure andefficientwaytoauthenticatedocuments.Here'sahigh-leveloverviewofhow youmightimplementablockchainQRcode-basedcertificateverificationsystem Createadigitalcertificatefortherecipient,containingrelevantinformationsuch as the recipient's name, the issuing authority, the date of issuance, and details abouttheachievementorqualification.Generateauniqueidentifier(hash)forthe certificate,preferablyusingcryptographichashingalgorithmssuch asSHA-512. Chooseablockchainplatform(e.g.Ethereum,Hyperledger,oracustomsolution) for storing certificate data. Ensure that the chosen blockchain supports smart contracts. create a smart contract that stores the certificate details along with its uniqueidentifier on the blockchain.The smart contract should include functions for certificateverification. Linking Certificate to QR Code: Generate a QR code containingtheuniqueidentifieroralinktothesmart contractontheblockchain. Embed the QR code on the digital or physical certificate.

Aproposed system for certificate validation using blockchain is useful in that it providesasecure,transparent,anddecentralizedwayofverifyingcertificates.By utilizing advanced blockchain technology, the system ensures the integrity and authenticity of certificates, eliminating the need for centralized trust authorities and reducing the risk of single-point failures. The system automates certificate validation and revocation processes, increasing efficiency and reducing manual

errors.Additionally, it provides a transparent and publicly accessible ledger for certificatevalidation,ensuringthatalltransactionsarevisibleandauditable.This results in faster verification, improved trust, and increased compliance with regulatory requirements. Furthermore, the system enables interoperability between different systems and organizations, making it easier to verify certificates across different platforms.

In conclusion, the proposed system represents a decentralized, secure, and transparent framework for issuing, storing, and verifying digital certificates. It utilizes blockchain technology to create an immutable and tamper-proof record ofcertificates,ensuringtheirauthenticityandintegrity.Thesystemenablesreal- time verification, allowing employers, educational institutions, and other organizations to quickly validate credentials. It also provides a self-sovereign identity solution, giving individuals control over their own certificates and data. The proposed system is designed to be scalable, flexible, and interoperable, allowing for seamless integration with existing systems and frameworks. By leveraging blockchain technology, the proposed system offers a reliable, trustworthy,andefficientsolutionforcertificatevalidation,transformingtheway digital certificates are verified and authenticated.

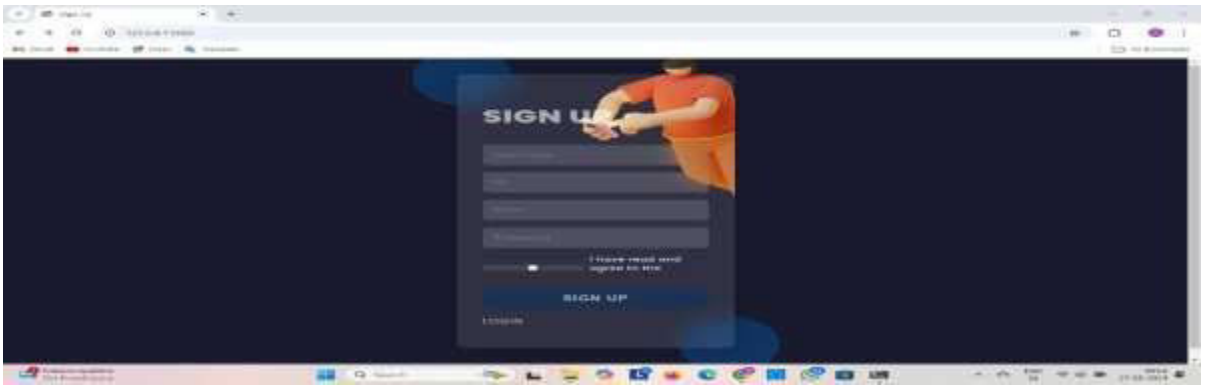
6. ADVANTAGESOFPROPOSEDSYSTEM

- Byusingtheunmodifiablepropertyofblockchainprovidemoresecurity.
- Confidentialityistransparentwitheachtransactionvisibletoallthepeers.
- Runanapplicationinofflinemode.
- Certificateisvalidatedrapidly
- Provideaccurateandreliableinformation.

ISSN PRINT 2319 1775 Online 2320 7876
Research Paper Journal Volume 13, Iss 04, 2024

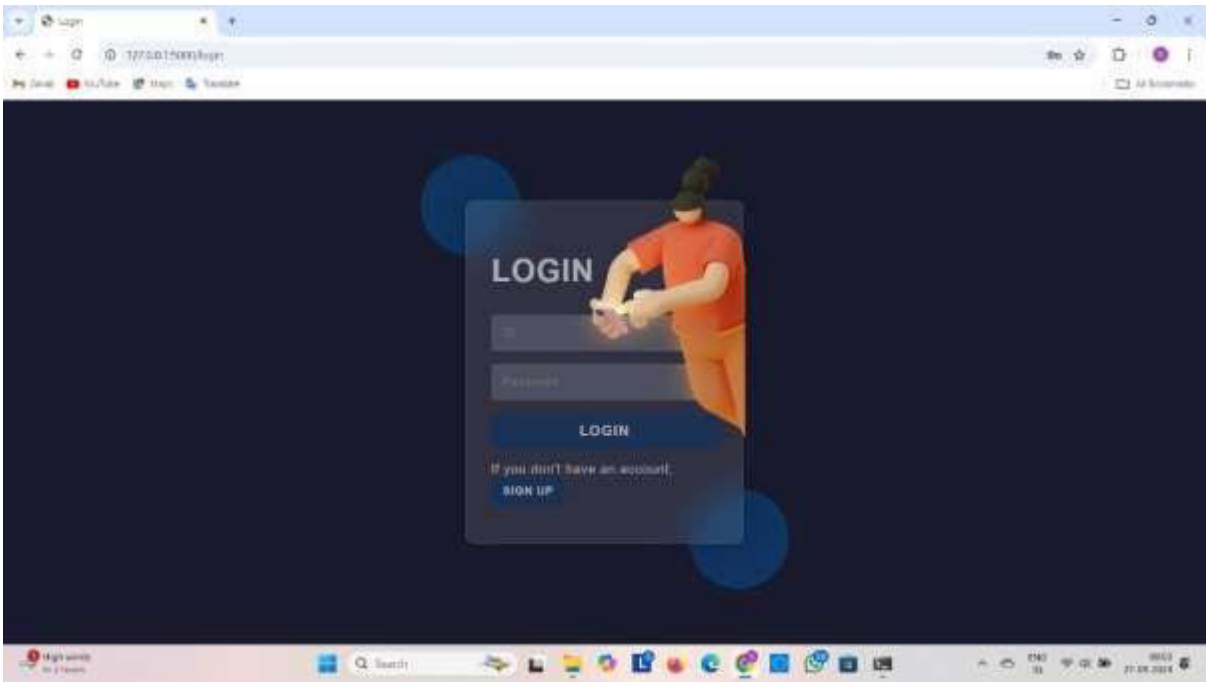
7. RESULT

SIGNUP



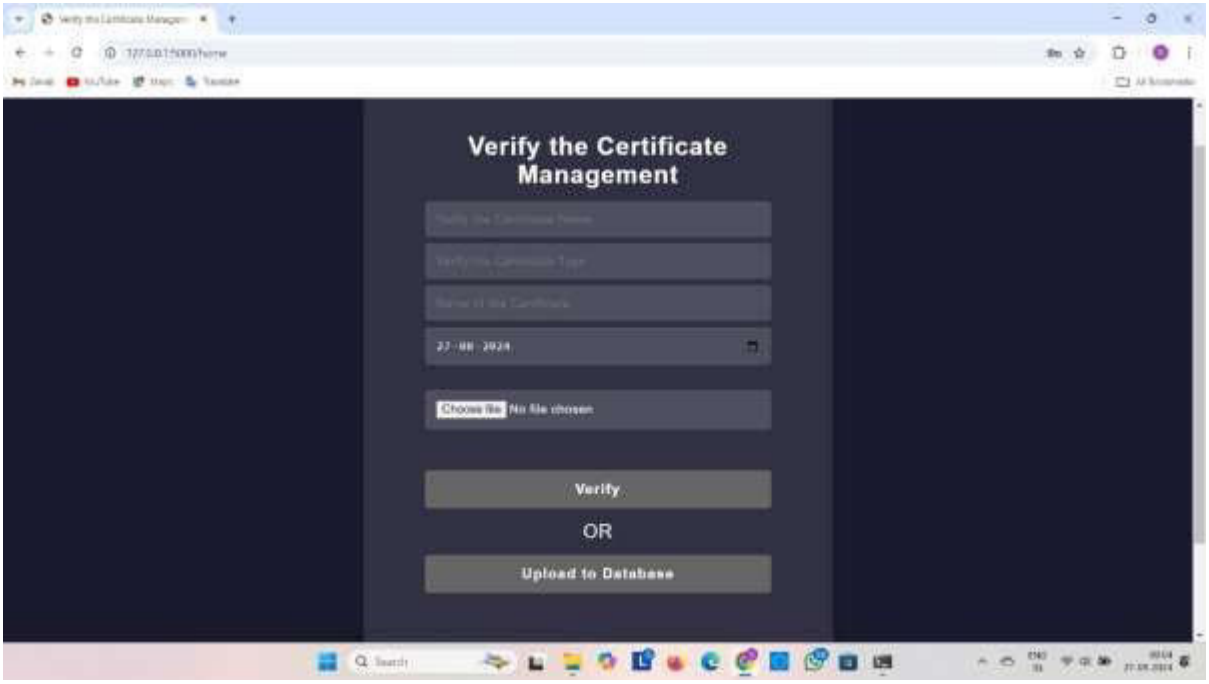
TheaboveOutputrepresentstheCertificatevalidationSignUpPage.

LOGINFORM



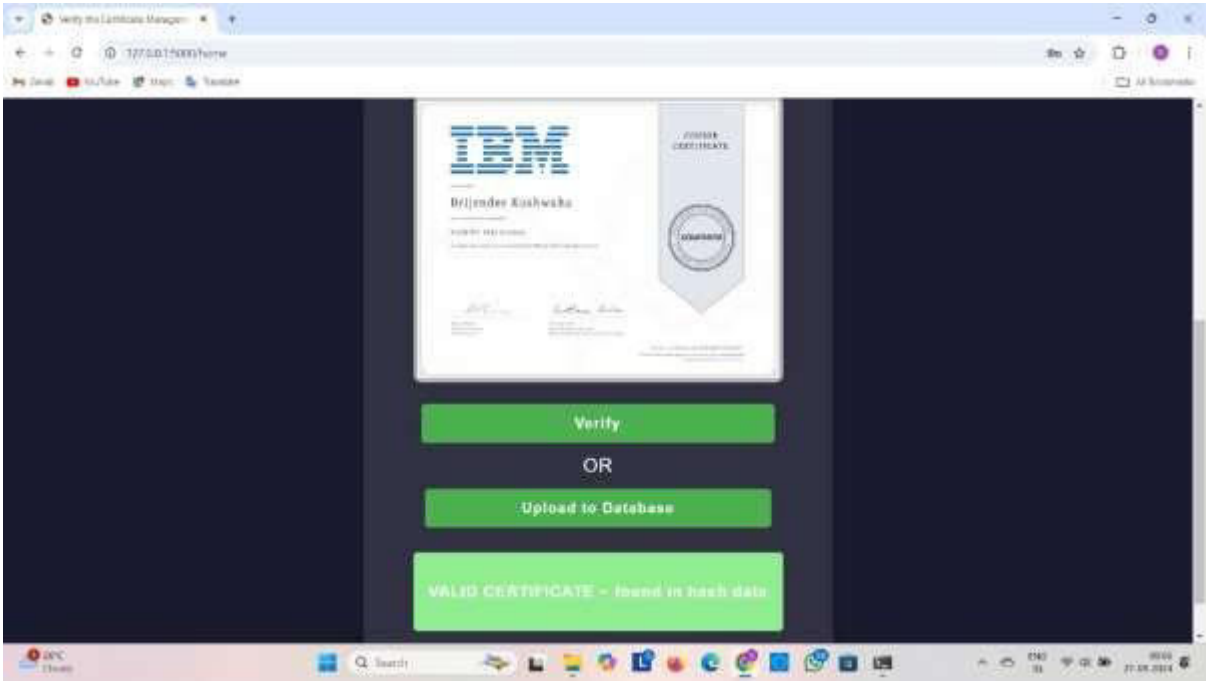
TheaboveOutputrepresentstheCertificatevalidationLoginPagewiththe details.

VERIFYCERTIFICATEMANAGEMENT



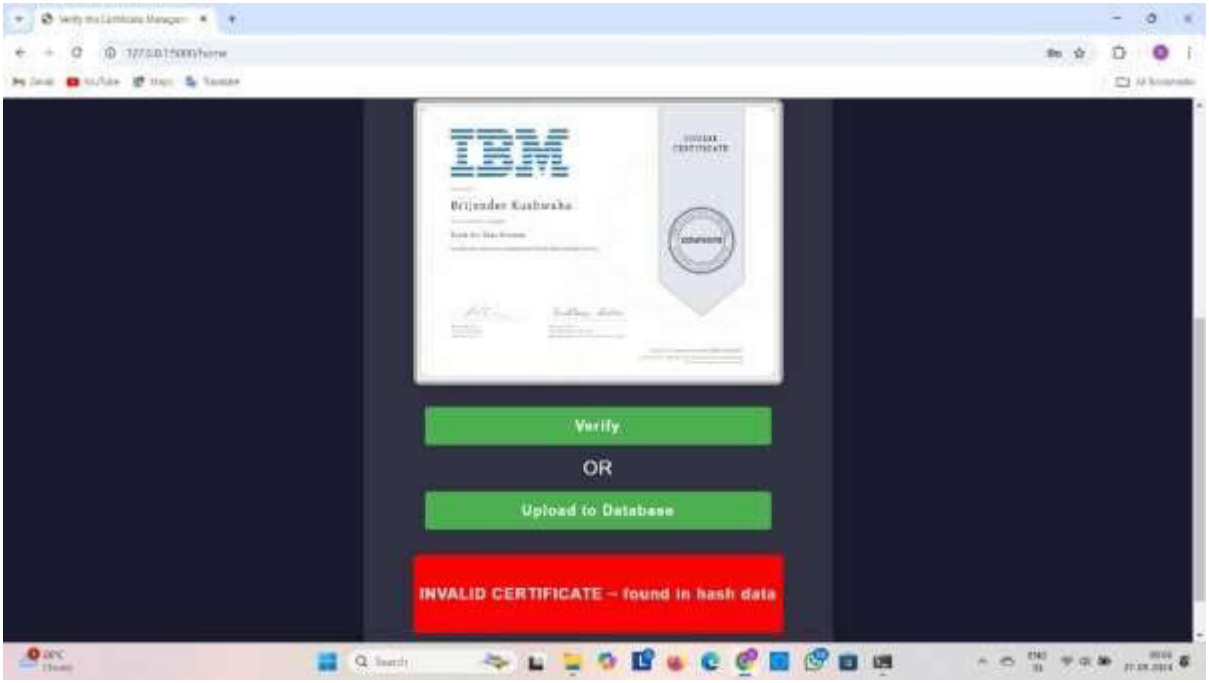
TheaboveoutputrepresentstheCertificatevalidationCredentialsPagetofill the details.

CERTIFICATEVALIDATIONPAGE



TheaboveoutputrepresentstheCertificatevalidationValidpage.

CERTIFICATEVALIDATIONINVALIDPAGE



TheaboveoutputrepresentstheCertificatevalidationInvalidPage.

8. CONCLUSION

Inconclusion,theproject"Certificatevalidationusingblockchain"weenhanced certificate security and integrity through Blockchain, preventing certificate forgery.Itstreamlinesthecertificateverificationprocess,reducingmanualeffort and time for verification. Blockchain ensures tamper-proof record-keeping, instilling trust in the verification process. The project offers a user-friendly interface for easy certificate upload, verification, and access, benefiting educational authorities and employers alike.

9. REFERENCES

- DavidA.Basin,CasJ.F.Cremers,TiffanyHyun-JinKim,AdrianPerrig, Ralf Sasse, and Pawel Szalachowski.ARPKI: attack resilient public-key infrastructure. In Proceedings of the 2014ACM SIGSAC Conference on Computer and Communications Security, pages 382-393.ACM, 2014.

- RFC5280:InternetX.509PublicKeyInfrastructureCertificateand Certificate Revocation List (CRL) Profile. Page 69.

- LaurentChuat,PawelSzalachowski,AdrianPerrig,BenLaurie,andEran Messeri. Efficient

gossip protocols for verifying the consistency of certificatelogs.In2015IEEEConferenceonCommunicationsandNetwork Security, pages 415-423. IEEE, 2015.

- P.Eckersley,Iranianhackersobtainfraudulenthttpscertificates:Howclose To a web security meltdown did we get https://www.eff.org/deeplinks/2011/03/iranian-hackers

BIBILOGRAPHY

Iam **T.VYSHNAVI**.Iamcurrentlyinmy7thsemesterofComputer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "MySQL APPROCH FOR "CERTIFICATE GENUINITY USING BLOCKCHAIN".

I am **M. SHRIYA**. I am currently in my 7th semester of Computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "MySQL APPROCH FOR "CERTIFICATE GENUINITY USING BLOCKCHAIN".

Iam**P.SAIKIRAN**.Iamcurrentlyinmy7thsemesterofComputer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "MySQL APPROCH FOR "CERTIFICATE GENUINITY USING BLOCKCHAIN".

Iam**K.PRABHAS**.Iamcurrentlyinmy7thsemesterofComputer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research interest is done based on "MySQL APPROCH FOR "CERTIFICATE GENUINITY USING BLOCKCHAIN".