INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

Digital Document Verification with QR Using Blockchain

[1]Mr. A. N. Gharu, [2]Mr. Pratik Pandharinath Gavali, [3]Mr. Pranav Ramesh Marathe,

[4]Mr. Darshan Bhausaheb Nikam, [5]Mr. Lalit Subhash Pagar

Department of Computer Engineering, MET's Institute of Engineering, BKC, Adgaon, Nashik, Maharashtra, India

ABSTRACT: This paper delves into the transformative integration of block chain, QR codes, and Firebase Cloud within the domain of document creation and verification. The foundation of this evolution lies in the application of block chain technology, characterized by its decentralized ledgerand smart contracts. Through these features, documents attain an unprecedented level of integrity, facilitated by an indelible digital signature. The inclusion of QR codes as integral components in document verification brings a user-friendly dimension to the process. By being affixed to documents, QR codes act as gateways to corresponding block chain entries, incorporating essential information such as timestamps and cryptographic hashes. This amalgamation streamlines the verification process, offering both speed and security. The final layer of this technological triad involves the strategic integration of Firebase Cloud, a scalable and real-time cloud database. This addition ensures not only secure storage but also efficient retrieval of block chain-anchored documents. The synergistic collaboration of block chain's immutability, QR code-enabled swift verification, and Firebase Cloud & dynamic storage capabilities creates a resilient ecosystem, redefining standards in documentsecurity, authenticity, and accessibility.

KEYWORDS: Block chain, Quick Response, QR Codes, Security, Cryptographic Hash, Digital Signature, Digital Signature, Block chain Technology, Smart Contracts, Cloud Computing, Cloud Database, Real Time, User Friendly.

I. INTRODUCTION

In an era marked by the relentless pursuit of technological advancement, the fusion of block chain technology, QR codes, and cloud computing has ushered in a new frontier for document creation and verification. This synergy not only enhances the security and authenticity of documents but also revolutionizes the way we perceive and handle sensitive information. This paper delves into the intricate web of block chain based document creation, the integration of QR codes for seamless verification, and the utilization of Firebase Cloud for secure storage and retrieval The cornerstone of this paradigm shift lies in the utilization of block chain for document creation. Block chain, a decentralized and tamper-resistant ledger, ensures the integrity and immutability of information. By employing smart contracts and cryptographic hashing, documents can be created with an indelible digital signature, providing an unparalleled level of trust. Each block in the block chain encapsulates a unique set of data, creating a chronological and transparent chain of information. This innovation not only mitigates the risk of fraud but also establishes a robust foundation for the subsequent phases of document verification. To democratize the process of document verification, the integration of Quick Response (QR) codes emerges as a powerful solution. QR codes, when affixed to documents, serve as gateways to their corresponding block chain entries.

These codes encapsulate crucial information, including timestamps, document IDs, and cryptographic hashes, allowing for rapid and secure verification. Users can simply scan the QR code with a compatible device, instantly retrieving the document's history and confirming its authenticity this marriage of blockchain and QR technology not only simplifies verification but also enhances accessibility and user experience. The final piece of this revolutionary puzzle involves leveraging Firebase Cloud for secure storage and retrieval of blockchain-anchored documents. Firebase offers a scalable and real-time cloud database that seamlessly integrates with blockchain applications. Through programmed interactions, documents are securely uploaded to the cloud, ensuring redundancy and accessibility. This not only enhances the durability of the document repository but also facilitates efficient retrieval when needed. The combination of blockchain immutability and Firebase Cloud's dynamic storage capabilities creates a resilient ecosystem for safeguarding critical information.

II. LITRATURE SURVEY

A QR code is a quick response code. To access information present in a QR code, we have to scan it by using any type of scanner in order to get stored information. Data is not safe in the system where there is a need for instant sharing of files in a limited time. To overcome problems, in this paper we present JWT (JSON Web Token) Token for Qr generation and to validate whether a user OTP (One Time Password) system is implemented. JSON Web Token creates a JSON object that is used to transfer information between a client and a server on the web. After generating a QR code we can scan with the help of any device that has a QR scanner as a medium. After scanning the user will get the information about the particular Users & will be able to download their basic documents in different formats. We have used NodeJS to develop the user interface that contains libraries to generate QR codes. This system guarantees the safety of documents as we used JWT and OTP two authentication methods. [1]

According to the Indian Ministry Education statistics, document verification is a complex domain that involves various challenging and tedious processes to authenticate. Due to the lack of an effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate a in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile, calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. In this research, the authors have identified the security themes required for document verification in the blockchain. This research also identifies the gaps and loopholes in the current blockchain-based educational certificate verification. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. [2]

The prolong growth of wired and wireless communication has spark off the revolution for the generation of new cryptographic algorithms. Hash functions are similar and important cryptographic fields, which are very complicate for data integrity assurance and data security services. This paper looks into optimization technique in new VLSI architecture for the SHA-256 hash functions are presented. This paper combines different techniques namely rescheduling of Carry Select Adder and Nonlinear Pseudo code random generator for improving the functions in an inner loop of hashing algorithm. The new system can minimize the critical path by rescheduling of inner part of the SHA architecture. The proposed system can be suitable to achieve less area utilization, improved security and fastest data throughput and higher performing frequency. The proposed architecture is developed using VerilogHDL and synthesized in Quartus V9.0 and Modelsim V6.4 on a common platform for achieving good results. [3]

III. METHODOLOGY

The document may be subjected to a process of verification by an authority by using a signature, and this process has proven to be time consuming and cumbersome. Later if there is a need for another verified copy of the same, the whole process has to be repeated, or a copy of the document has to be verified again by another party. In addition to these difficulties, sometimes the fraudulent activities that are followed by certain citizens lead to doubtfulness of the authenticity of the content of the documents. This is the problem that is addressed in this project, and a solution architecture and an execution model are proposed, which can be used to verify documents incorporating digital signatures and document correlation factors.

IV. OBJECTIVE OF SYSTEM

- **Tamper-proof Verification:** Utilizing blockchain immutable nature to create a record of the document authenticity, ensuring it hasn't been altered or tampered with since its creation.

- **Transparent Verification Process:** Providing a transparent verification process where anyone with access to the QR code can confirm the document validity by accessing the blockchain distributed ledger.

- **Enhanced Trust:** Increasing trust in digital documents by leveraging blockchain decentralized and secure ledger, reducing reliance on centralized authorities or intermediaries.

- **Efficiency and Accessibility:** Streamlining document verification processes by enabling quick and easy verification through QR codes, accessible via smartphones or specialized readers.

- **Traceability and Auditability:** Allowing for the traceability and auditability of document history, including timestamps and changes made over time, providing a comprehensive audit trail.

V. SYSTEM ARCHITECTURE
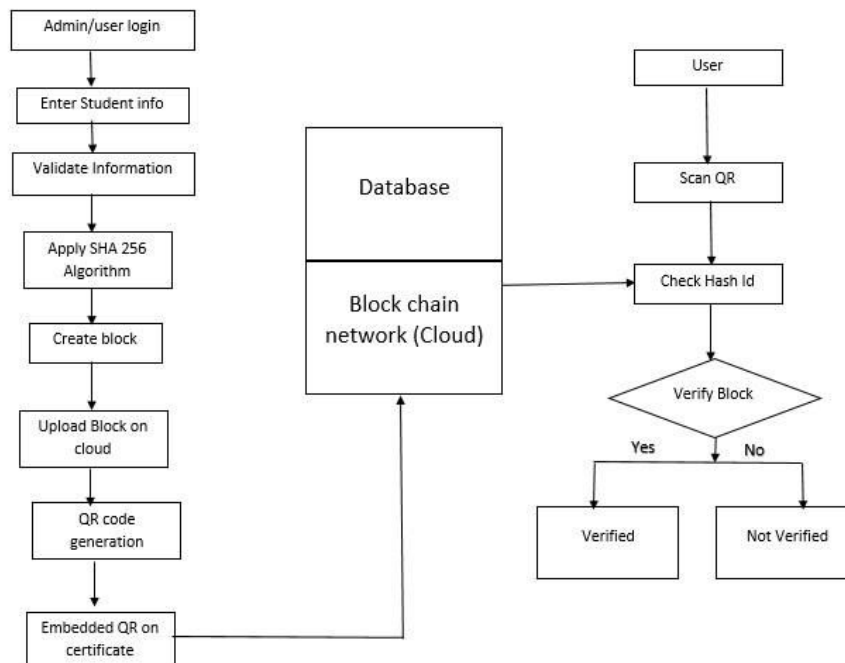
- **Admin/User Login:** The process starts with an admin or user logging into the system. This could be a university administrator or an employer who needs to verify a student's diploma or an employee's certification.

- **Enter Student Info and Validate Information:** The admin or user would then enter the student's information or the document holder's information into the system. This information could include the student's name, ID number, and the type of document being issued (e.g., Bonafide and Transfer Certificate). The system would then validate this information against a database to ensure accuracy.

- **Apply SHA-256 Algorithm:** Once the information is validated, a cryptographic hash is generated using the SHA-256 algorithm. A cryptographic hash is a unique alphanumeric string that is generated from a piece of data. Any change to the data will result in a completely different hash value.

- **Create Block and Upload Block on Cloud:** The document information, along with the cryptographic hash, is then bundled together into a block. This block is then uploaded to the blockchain network, which is essentially a distributed ledger technology that securely stores data across a network of computers.

- **Blockchain Network (Cloud) Checks Hash ID:** Once the block is uploaded to the blockchain network, the network checks the validity of the cryptographic hash. The blockchain network can perform this check because it has a copy of all the previous blocks in the chain, allowing it to verify the integrity of the data.

- **Verify Block:** If the cryptographic hash matches the hash generated from the document information, the block is considered valid. This means that the document is authentic and has not been tampered with.

- **QR Code Generation and Embed QR on Certificate:** If the block is verified, a QR code is generated that contains a unique identifier for the document. This QR code is then embedded into the digital certificate or document itself.

- **Scan QR and User:** The user, who may be a potential employer or someone verifying the authenticity of a document, can then scan the QR code using their smartphone or other device.

- **Verified/Not Verified:** If the re-computed hash matches the hash stored on the blockchain, the document is verified as authentic. If the hashes do not match, the document is not authentic and may have been tampered with.

VI. ALGORITHM AND SYSTEM REQUIREMENT

ALGORITHM

SHA-256 - SHA-256, part of the Secure Hash Algorithm (SHA) family, is a cryptographic hash function that generates a fixed-applications, including digital signatures, certificates, and blockchain technologies like Bitcoin. SHA-256 takes an input (message) of any length and produces a unique 256-bit hash value, making it highly resistant to collisions (two different inputs producing the same hash).

1. Minimum System Software Requirement
   - Visual Studio 2017 and Onwards
   - OS type: 32-bit Operating system

2. Minimum System Hardware Requirement
   - RAM 4 GB or Above
   - I3 Processor or above
   - 150GB Hard disk or above

VII. RESULT

1. **Login Page:** This is the opening window that show the option for login of Admin.
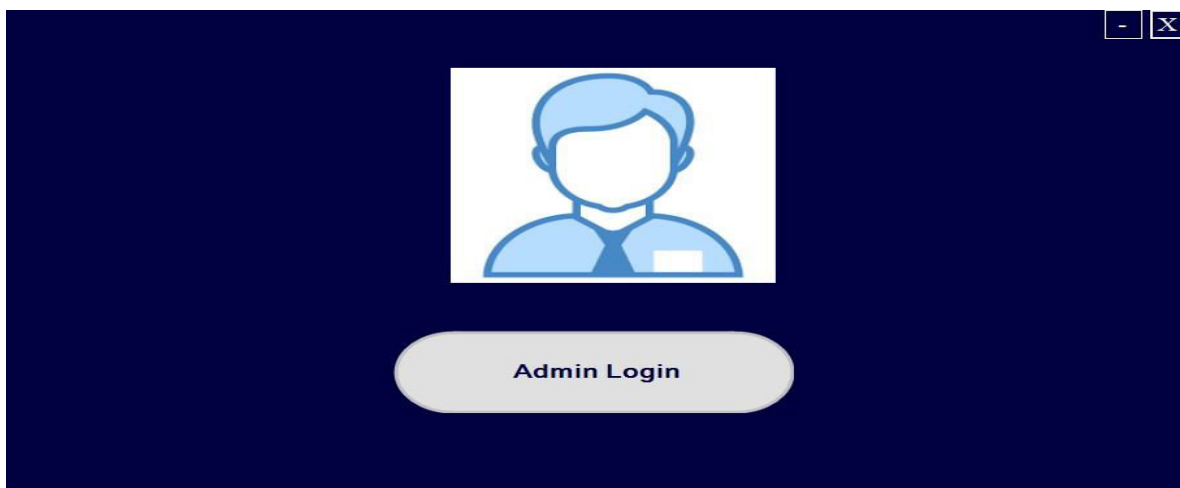

Fig. Login Options for Admin and User

2. **Admin Login:** In this page admin can login with the help of default Id and Password
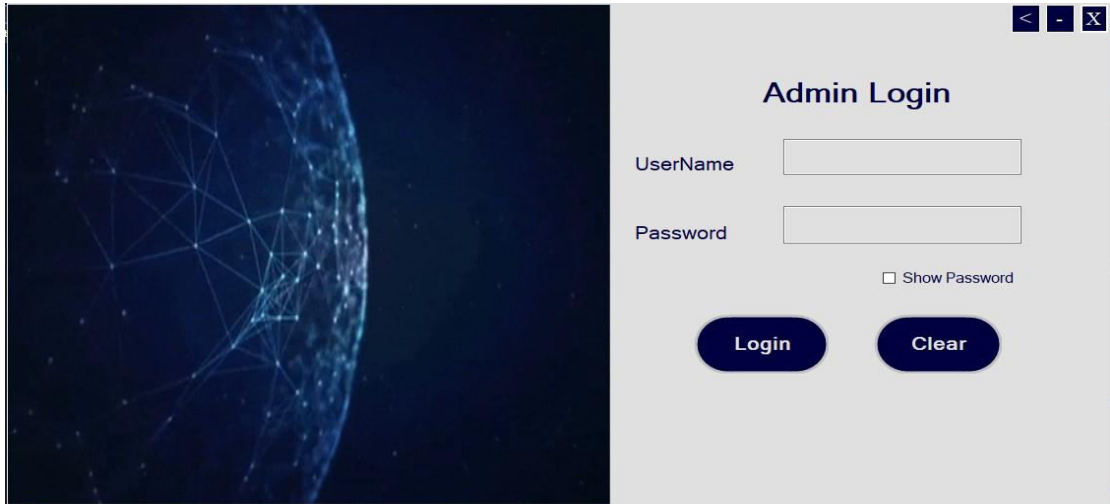

Fig: Admin Login

3. **User Registration:** After the login of admin, admin can set password for different user who can access software and create a certificate for user.
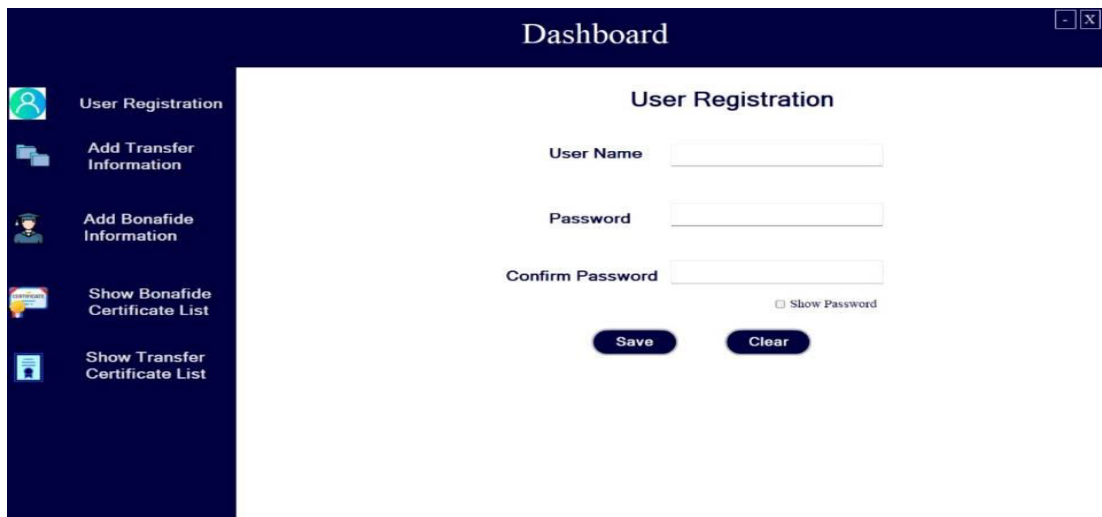

Fig: User Registration

4. **Generate Bonafide Certificate:** With the help of this slide or user and admin can create Bonafide certificate for Student

Fig: Generate Bonafide Certificate

5. **Generate Transfer Certificate**: With the help of this slide or user and admin can create Bonafide certificate for Students

Fig: Generate Transfer Certificate

6. **Show Transfer Certificate Information:** With the help of this module we can see the generated certificates information.
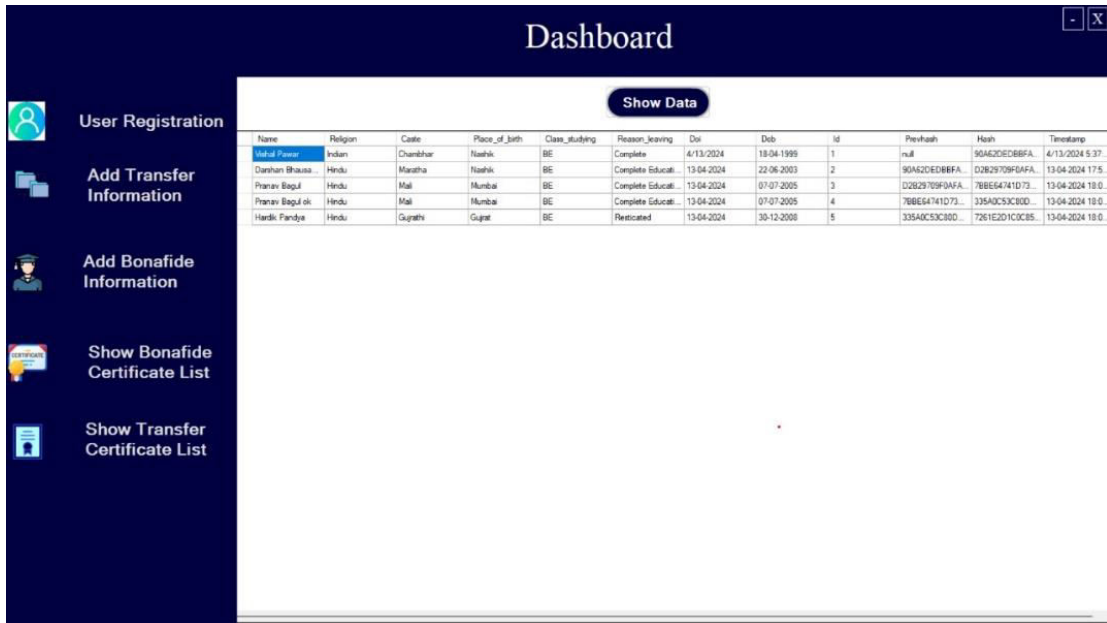

Fig: Show Transfer Certificate Information

7. **Show Bonafide Certificate Information:** With the help of this module we can see the generated certificates information.
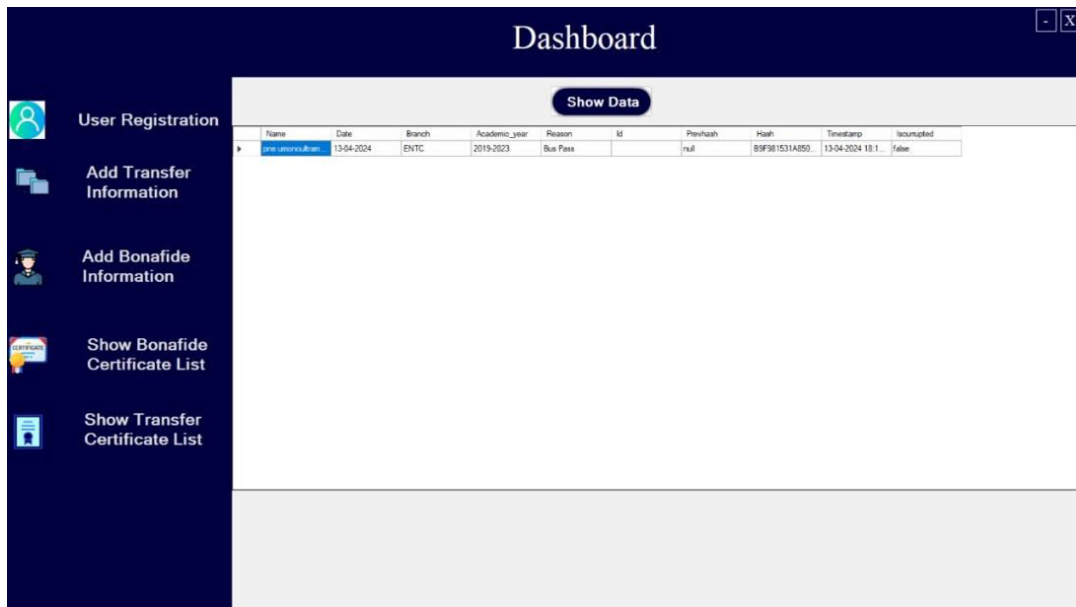

Fig: Show Bonafide Certificate Information.

VIII. CONCLUSION

In the ever-evolving landscape of information management and verification systems, the integration of blockchain, QR codes, and cloud computing has emerged as a transformative force. This comprehensive exploration into the amalgamation of these technologies for document creation and verification underscores their collective potential in establishing unparalleled levels of security, authenticity, and accessibility.The use of blockchain technology, with its decentralized and tamper-resistant ledger, ensures the immutability of documents through smart contracts and cryptographic hashing. This innovation not only mitigates the risks of fraud but also lays the foundation for a transparent and chronologically organized chain of information. The application of the SHA-256 algorithm as part of the blockchain process enhances the security of document encryption, providing a robust digital signature.

IX. FUTURE SCOPE

This digital document verification system using QR codes and blockchain offers a secure and efficient method. Documents are hashed, uploaded to a blockchain for immutability, and a QR code on the document itself links to the blockchain for verification. This system can be further enhanced to integrate with e-governance services, support self-sovereign identities, utilize zero-knowledge proofs, and leverage decentralized applications for broader adoption. Additionally, future advancements in blockchain interoperability and AI integration can broaden the scope to applications like supply chain management, creating a future of secure, transparent, and user-friendly document management.

REFERENCES

1. divya shree r, keerthana g, krisshneshri m, vasantha kumar v, "digital documents verification system" published in: 2022 international conference on computer, power and communications (iccpc).
2. rasha m. abd el-aziz, anis ben, aissa ahmed i, taloba islam abdalla mohamed , "experimental analysis of document verification scheme using blockchain logics over secured cloud environment" article in international journal of advanced research in engineering & amp; technology · september 2020
3. vinayak patil, chinmay katkar, rohan rahate, sanjay waykar qr code document authentication and retrieval international journal of advanced research in engineering & technology 2022.
4. pankaj chougale, vaibhav yadav, dr. anil gaikwad ,Pankaj chougale, vaibhav yadav, dr. anil gaikwad firebase - overview and use international journal of advanced research in engineering technology 2021.
5. fariha jahan, mayel mostafa, shahrin chowdhury sha-256 in parallel blockchain technology: storing land related documents international journal of advanced research in engineering & technology 2020.
6. rohan hargude, ghule ashutosh, abhijit nawale, sharad adsure verification and validation of certificate using blockchain international journal of advanced research in engineering technology 2021.2004. 26th annual international conference of the ieee, ieee, pp 1513–1516.
7. binh nd, ejima t (2005) hand gesture recognition using fuzzy neural network. in: proc. icgst conf. graphics, vision and image process, cairo. pp 1–6
8. shinj-h, lee js, kil sk, shen df, ryu jg, lee eh, min hk, hong sh (2006) hand region extraction and gesture recognition using entropy analysis. ijcsns int j comput sci netw secur 6:216– 222
9. bayh, tuytelaars t, van gool l (2006) surf: speeded up robust features. in: european conference on computer vision. springer, pp 404–417

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

ISSN

INNO SPACE
SJIF Scientific Journal Impact Factor

doi
cross ref

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL
OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 **9940 572 462** 🟢 **6381 907 438** ✉ **ijircce@gmail.com**

Scan to save the contact details