iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56705

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 XI Nov 2023- Available at www.ijraset.com

Certificate Verification and Counterfeit Detection using Blockchain

Sahil Wadhwani
Department of Computer Engineering, All India Shree Shivaji Memorial Society College of Engineering, Pune, India

Abstract: ***Certificates help students not only to prove their achieved goals and milestones but also ensure that he/she maintains a high level of knowledge in that particular field. An estimated total of 25.57 crore Indian students have been enrolled for primary to higher education in 2020–21 and nearly 65 lakhs of them graduate each year. Throughout this journey, a student generates a myriad number of certificates that may include results, transcripts, degrees, diplomas, etc. A student has to submit these certificates to apply for a job or seek higher admission in any particular organization. A major problem today is manually verifying and authenticating these certificates. Many hardworking people with genuine certificates get rejected and suffer because of the lack of a system that can differentiate original certificates from fake ones. With easy access to cheap and advanced software, document forgery has become a matter of concern nowadays. This scenario demands an updated system that could not only store documents safely but also help verify and authenticate them, their issuers, and holders in a way that is much simpler, effective, and secure. Blockchain technology comes up as a solution to all these problems. Blockchain has recently emerged as a potential means for the document-authentication process and can be easily used to tackle document forgery and counterfeiting as it follows a decentralized approach. Our proposed model includes several methods such as unique hash generation, key cryptography, digital ledgers, proof of work, digital signatures, and distributed storage which has made the document-verification process easier and more secure for both the certificate-generating organization and the holder of the certificate. The SHA-256 algorithm has been used to assign a unique hash to each uploaded document which can be used to validate its authenticity. Thus, this system meets up all the criteria for a document verification system by overcoming the drawbacks and difficulties currently faced in the traditional methods of document verification.***
Keywords: Certificate Verification, Hashing, Blockchain, Cryptography, SHA-256.

I. INTRODUCTION

The basic structure of a student's education flows as follows: kindergarten, primary school, secondary school, junior college, and seeking admission for undergrad. After this, some students also plan to pursue higher studies either in their own country or in other foreign countries. Throughout this journey, a student earns many certificates that help him/her prove his/her knowledge in that particular domain. To climb this educational ladder, a student has to verify his hard-earned certificates at every stage. A majority of these certificates are in the form of paper, and electronic documents cannot effectively replace these traditional physical certificates. However, with the advancements in IT and easy access to cheap and advanced equipment, document forgery, i.e., counterfeiting has become quite easy. This has a negative impact not only on the holders of the certificates but also on the organization or boards that issued them. Thus, making document verification and authentication a complex and difficult process. There are a lot of hidden agencies and even individuals in our country who secretly run this document tampering business behind everyone's back. Differentiating fake certificates from genuine ones would be a time-consuming process that requires careful attention. Many hours will be spent simply contacting the organizations to get the certificate approved or requesting a statement guaranteeing the authenticity of the same. Therefore, there arises a need for a mechanism that could verify and authenticate certificates at a much lower cost (time and money).

Blockchain technology has recently emerged and has the potential to turn the disadvantages of the current document verification process into its advantages. With the help of blockchain, we can easily validate certificates, which would in turn reduce document fraud and misuse. Blockchain simply refers to a distributed database that stores multiple blocks linked together in such a way that makes it difficult or nearly impossible to change, hack, or cheat the system. To give a more technical definition of the blockchain: It is a digital ledger of transactions that are distributed across an entire network of nodes on the blockchain. Each block in the blockchain contains several transactions, a hash that uniquely identifies that particular block, and a link to the previous block, i.e., the hash value of its last counterpart in the connection. Each time a new transaction takes place in the blockchain, a record of that specific transaction is added to every participant's ledger. A ledger is a distributed database that is individually managed by each

participant. Different hash algorithms are available that can be used to generate unique hashes for these blocks. In our proposed system, we have used the SHA-256 hashing algorithm for this purpose. This hash acts as a cryptographic signature of that block and it cannot be changed. This means that even if one block in the chain is tampered with, all blocks succeeding that block will automatically carry an incorrect hash value. Any modifications made to the system can be readily verified. If an individual attempts to manipulate data stored within, he/she will have to change each and every block in the chain, across all the distributed versions. Owing to this purely reliable, transparent, and decentralized method of storing and validating certificates, we are motivated to use blockchain technology in our proposed model.

II. LITERATURE REVIEW

Imam, et al. [1] have proposed a model using the Ethereum blockchain that can be used to authenticate digital documents. The solidity programming language has been used for implementing smart contracts. A hash value for each certificate is generated using the SHA-256 algorithm. Their developed system consists of two sections (Admin and User). The admin is certificate generating organization that can perform all three tasks (upload, verify and download). Any user/verifier can verify the document or even download it using the IPFS hash. The IPFS hash has not been stored in the smart contract for enhanced security.

A. Gayathiri, et al. [2] using blockchain technology have developed an application for the validation of digital certificates. By using the analogue to digital image conversion, the values 0s and 1s are created for each certificate. Further, sampling and quantization techniques are used to convert paper certificates into digital ones. The chaotic algorithm is used to generate the hash value for the certificate. The admin can log in into the application using his login-id and password to either upload or verify a certificate. Validation is done by matching the hash values.

In paper [3], Satoshi Nakamoto proposes concepts related to Blockchain Technology. Blockchain is a ledger that allows the storage and transfer of records in a decentralized and transparent manner. It is a growing list of nodes that are linked to each other via cryptographic hashes. The first block which does not hold any previous hash is known as the Genesis Block. Timestamps are used to prove the creation of a particular block. Blockchains are managed by peer-to-peer networks, where nodes collectively adhere to the consensus algorithm protocol, which makes the blockchain records unalterable. Thus, making the entire process hassle-free and providing enhanced security to the public.

Jiin-Chiou, et al. [4] developed an application using the Ethereum blockchain to avoid the counterfeiting of certificates. Events that cause the certificates to be forged often get noticed, this is all due to the lack of an effective anti-forge mechanism. First, the paper certificates are converted into digital ones and a unique hash value for each is generated. This hash value is been stored in the blockchain. The system then creates a related QR code and inquiry string code to affix to the paper certificate. This system prevents document forgery and also cuts down on the use of paper. But a separate smartphone is required to scan the QR codes.

In paper [5] published by Omar S. Saleh, et al., the goal of this study was to fill up gaps in the current certificate verification system. The study majorly focuses on the five principles of security i.e., Authentication, Authorization, Confidentiality, Ownership and Privacy. The proposed system is built on the Hyper Ledger Fabric framework. Hyperledger comes up with an added advantage as it is not coin (token) based and is developed in an environment that is comparatively less complex.

According to the report in paper [6], a platform keeping into account the characteristics of blockchain technology like immutability, decentralized, distributed ledgers, and consensus has been developed to issue and verify documents in a public blockchain called SPROOF. Keys are being used for the transfer of data. The public key (which is accessible to all) is used to upload the documents to the platform. The private key is then used to prove the ownership of the verifier. The Key Derivation Function is used to derive the private key from the master key. A digital wallet called the hierarchical deterministic (HD) wallet is used to store the digital keys. Each user contains a key ring with other peoples' public keys which helps in the process of encryption and decryption.

Macro Baldi, et al. [7] have proposed a system that overcomes one of the main point of failures (POF) of the modern public key infrastructures (PKI) concerning the security and reliability of certificate revocation lists (CRLs). Private blockchain has been used to distribute the CRLs for a given set of certificates which is maintained by the same Certificate Authority (CA) that issued the certificate. Thus, CAs have the absolute responsibility to issue correct certificates. However, the CAs can be compromised and fake but genuine certificates can be issued due to the lack of security practices. This makes the CA ecosystem prone to counterfeiting and vulnerable.

They proposed a blockchain based system in paper [8] that employs a digital signature scheme and timestamps to detect education degree fraud and verify student certificates. According to this paper, the current tools and techniques used to mitigate forgery threats are insufficient and come with a myriad number of limitations. Academic credential fraud comes up through counterfeiting, as well as the involvement of in-house authorities. Thus, the digital signature with timestamps is used to prove that a certificate was issued

at that specific time. With this proposed platform, a student benefits from a single and transparent view of his/her completed courses and at the same time has access to up-to-date data.

III. PROPOSED METHODOLOGY

A. *Modules*

1) *Blockchain:* Blockchain, an advanced and more secure technology, has been laid as the backbone of this proposed system. Blockchain is a decentralized ledger tracking one or more digital assets on a peer-to-peer network. It is a transaction-based database where data can be stored in a decentralized manner by creating a distributed network.
2) *P2P Network:* The peer-to-peer network is a decentralized ledger that consists of a group of nodes, maintained by a distributed network of users, where each node acts as a server as well a client. The security of the underlying consensus algorithm makes the P2P network a crucial component of blockchains.
3) *Ethereum:* Ethereum is a global, distributed, and decentralized blockchain-based network that offers smart contract functionality. It is an open-source platform similar to Android for building apps, organizations, transacting, communicating and is most widely used in the cryptocurrency system.
4) *Smart Contract:* A Smart Contract is a programming code that is deployed on a blockchain when an event with some predetermined conditions takes place. Smart contracts that are deployed in blockchains are copied to each node to prevent contract tampering. This ensures transparency and secured facilitation of the contractual terms.
5) *SHA -256 Hashing Function:* A Hash function is a cryptographic algorithm that works on a message of arbitrary length and produces a message digest of a fixed length. The MD-5 (Message Digest) divides the message into blocks of 512 bytes and converts each block into a 128-bit message digest, but this 128-bit message digest proves to be too small to prevent attacks. Therefore, the Secure Hash Algorithm (SHA) was invented. In our proposed system, we give the size of the certificate file as input to this algorithm and it generates an almost unique 256-bit (32-byte) signature for the same.
6) *IPFS:* With decentralized storage, data is encrypted and stored across multiple locations, or nodes. Only the owner of the data holds the private encryption key. The Inter-Planetary File System is a file storage system that allows one to store and share files over a distributed network. This file system interacts directly through a global P2P network. With other decentralized data storage systems like Arweave, BitTorrent (BTFS), Filecoin, Sia, Storj, and Tardigrade, etc. in the market, IPFS proves to be advantageous as it becomes exponentially more stable and secure.
7) *Solidity:* Solidity is a statically-typed object-oriented programming language just like Python, C++, etc. created by Ethereum for implementing smart contracts. It supports complex user-defined programming libraries and is used as the primary language for blockchain running platforms. Solidity targets the Ethereum Virtual Machine (EVM) and is used to embed logic in smart contracts.

B. *Decentralized*

Blockchain is that internet platform that allows a decentralized and transparent transfer of data. Decentralization refers to the transfer of decision-making and supervision from a centralized organization (individual, corporation) to a distributed network. The data elements are transparent to all members who share their data components in that distributed network and sets no constraints on who may see it.

Each member has a copy of the same data in the form of a distributed ledger. This facilitates a trust less setting where no one has to know to or trust anyone else. If any ledger is corrupted or altered in any way, it will be rejected by the majority as each party has a timely and shared impression of the data. This improves the data recovery process.

C. *Enhanced Security*

Blockchains are encrypted end to end to provide an extra layer of security. Cryptography plays a vital role to sign messages and encrypt data with the help of a public-private key mechanism. Each document uploaded is assigned a unique hash to give it a distinctive identification. The three major principles of security i.e., Confidentiality, Integrity and Availability (CIA) are highly regarded. However, blockchain implementation does not enforce confidentiality aspects as strongly as it enforces integrity and availability of information. The data elements are transparent to all individuals in a single blockchain, owing to its decentralized nature.

D. Proof of Work and Transparency

Proof of work is a software algorithm, a consensus mechanism to choose which network participants are allowed to handle the verification of new data. A consensus algorithm is a process to achieve agreement on the present data set of the ledger among distributed processes and systems. All network participants with permission access same information at the same time, providing full transparency and ensuring openness. All activities are time-stamped and recorded in multiple locations.

E. Immutability

Immutable ledger in the blockchain refers to the ability to remain unchanged, unalterable and indelible. Every participant in the system has a copy of the digital ledger and if any member wishes to make changes to the document, the others validate its authenticity, and changes are allowed only if a majority votes for the same. This makes the entire process much more secure and enhances user trust.

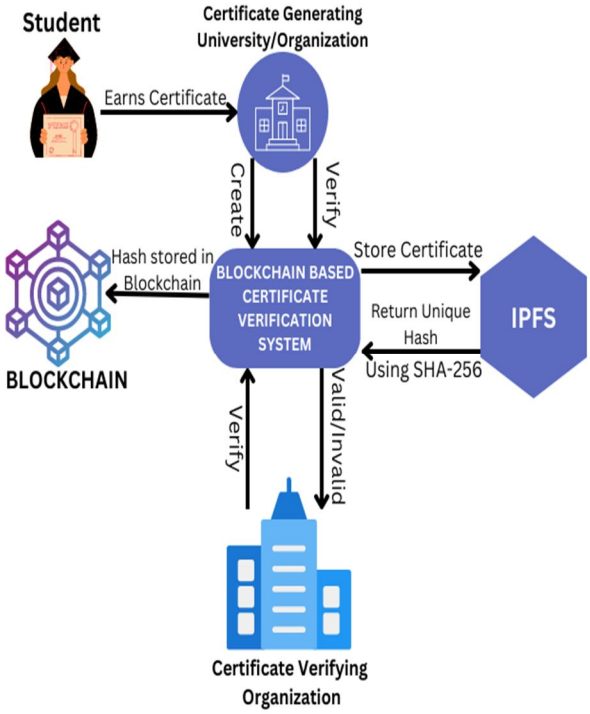


Fig. 1 Proposed System Workflow

IV. IMPLEMENTATION

We have developed this system in order to overcome the loopholes and drawbacks of the current certificate verification process. The certificate generated at the organization is first uploaded to our blockchain-based certificate verification system. The further steps are explained in the subsequent sections. A very well know hash generating algorithm SHA-256 has been used to assign unique hash values to each certificate. With other popular hashing algorithms available in the market, we have chosen the SHA-256 algorithm as it strongly follows the Avalanche effect and is considered more secure than the others as it does not have any known vulnerabilities to date.

A. Roles

1) *Certificate Generating Organization:* This entity can be any school, college, university, or organization that issues one or more certificates for its candidates. They have the right to both generate and verify certificates.
2) *Student:* Students graduating from universities can view and download their certificates from this web-based application.
3) *Certificate Verifying Company:* This entity is the most concerned regarding the integrity and authenticity of the certificate. The company verifies the certificate based on the unique hash and determines whether the certificate is genuine or not.

B. Certificate Upload / Creation by University

The admin can log in to the application using the university credentials. After logging in, the next page shows an option to add certificate or verify certificate. As the admin taps on the add certificate, he/she has to fill in the details required to generate a new certificate and is allowed to upload the new certificate. Furthermore, OpenCV and image processing techniques are employed to generate distinct and easily recognizable digital certificates. The certificate verification process will be the same for the user as well as the issuer, which has been discussed in further sections.

C. Storing Certificate in IPFS and Generation of unique hash

The digital certificate is then stored in the IPFS (Inter Planetary File System). Before storing the actual certificate in the IPFS, the document data is gathered and appended in a bit array. Now, IPFS is provided with this data and the certificate. Thereafter, the hash generation process begins. The SHA-256 algorithm takes input in different sizes and produces a unique 256 bits (32 bytes) hash, which is further encoded as 64 alphanumeric characters in hexadecimal. The probability of two hashes colliding is extremely low, P ≈1/2(n/2^128) ^2 where n is the length of the hash which is 256 length. Compared to the other hashing algorithms available in the market, SHA-256 does not have any know vulnerabilities to date.

D. Certificate Verification

Further, this data is passed to the Blockchain. Now, this unique hash stored in the blockchain cannot be changed, and if anyone tries to tamper with the data, as the fundamental properties of the blockchain explain, it can be easily tracked when and where the data has been changed. Certificates are verified using the unique hash value assigned to each certificate. If the certificate is legitimate, the output results as success, and if not, the output prompts Modified Certificate.

E. Working of Application

In our web-based application, there are two sections, viz., Issuer and Verifier. Only the issuer, i.e., the certificate-generating organization has all the privileges, that is to upload, verify and download the certificate. The issuer can log in to the system using admin credentials.

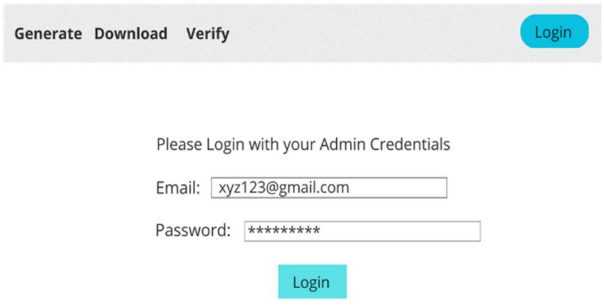


Fig. 2 Admin Login Page

After a successful login, the issuer can now upload certificates. A unique hash is generated for each uploaded certificate. Further, this hash is stored in the Blockchain memory. This hash is also used to verify the certificate.

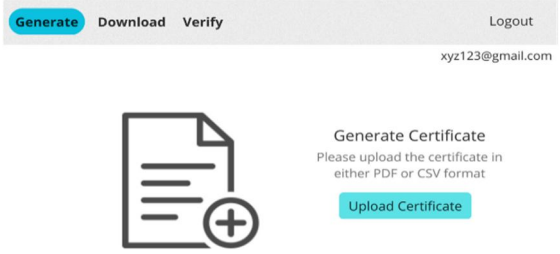


Fig. 3 Certificate Generation/Uploading

The Verifier is the organization or company that validates the authenticity of the certificate.

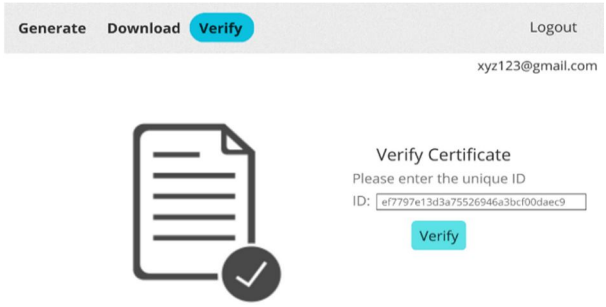


Fig. 4 Verification using ID

If the certificate is legitimate, the result will be Valid Certificate else Invalid.

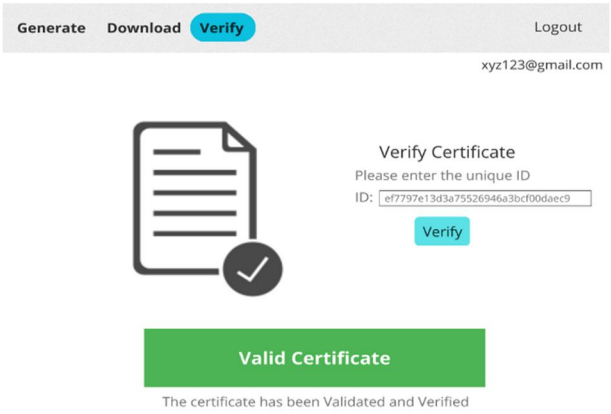


Fig. 5 Valid Certificate

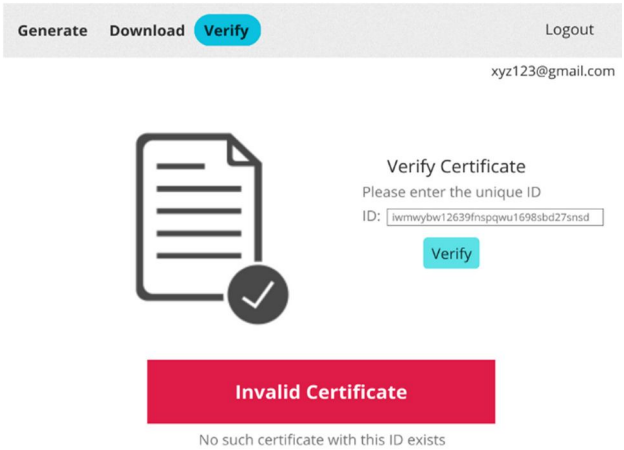


Fig. 6 Invalid Certificate

V. CONCLUSION

In this paper, we proposed a decentralized system using blockchain that not only stores certificates but also validates the authenticity. Compared to the traditional cloud-based storage system, our proposed system is more secure and efficient. Blockchain being a shared, immutable ledger that also facilitates the process of recording transactions, counterfeiting and forgery of certificates can be reduced greatly. With our web-based application, the specified user can generate, verify and download certificates with great ease. Thus, the system guarantees data privacy and transparency.

REFERENCES

[1] Imam, I. T., Arafat, Y., Alam, K. S., & Shahriyar, S. A. (2021, February). DOC-BLOCK: A blockchain based authentication system for digital documents. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1262-1267). IEEE.

[2] Gayathiri, A., Jayachitra, J., & Matilda, S. (2020, July). Certificate validation using blockchain. In 2020 7th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-4). IEEE.

[3] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin. –URL: https://bitcoin. org/bitcoin. pdf, 4(2).

[4] Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In 2018 IEEE international conference on applied system invention (ICASI) (pp. 1046-1051). IEEE.

[5] Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. Journal of critical reviews, 7(3), 79-84.

[6] Brunner, C., Knirsch, F., & Engel, D. (2019). SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain. In ICISSP (pp. 15-25).

[7] Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni, D., & Spalazzi, L. (2017, January). Certificate Validation Through Public Ledgers and Blockchains. In ITASEC (pp. 156-165).

[8] Dongre, J. G., Tikam, S. M., & Gharat, V. B. (2020). Education degree fraud detection and student certificate verification using blockchain. Int. J. Eng. Res. Technol, 9, 300-303.

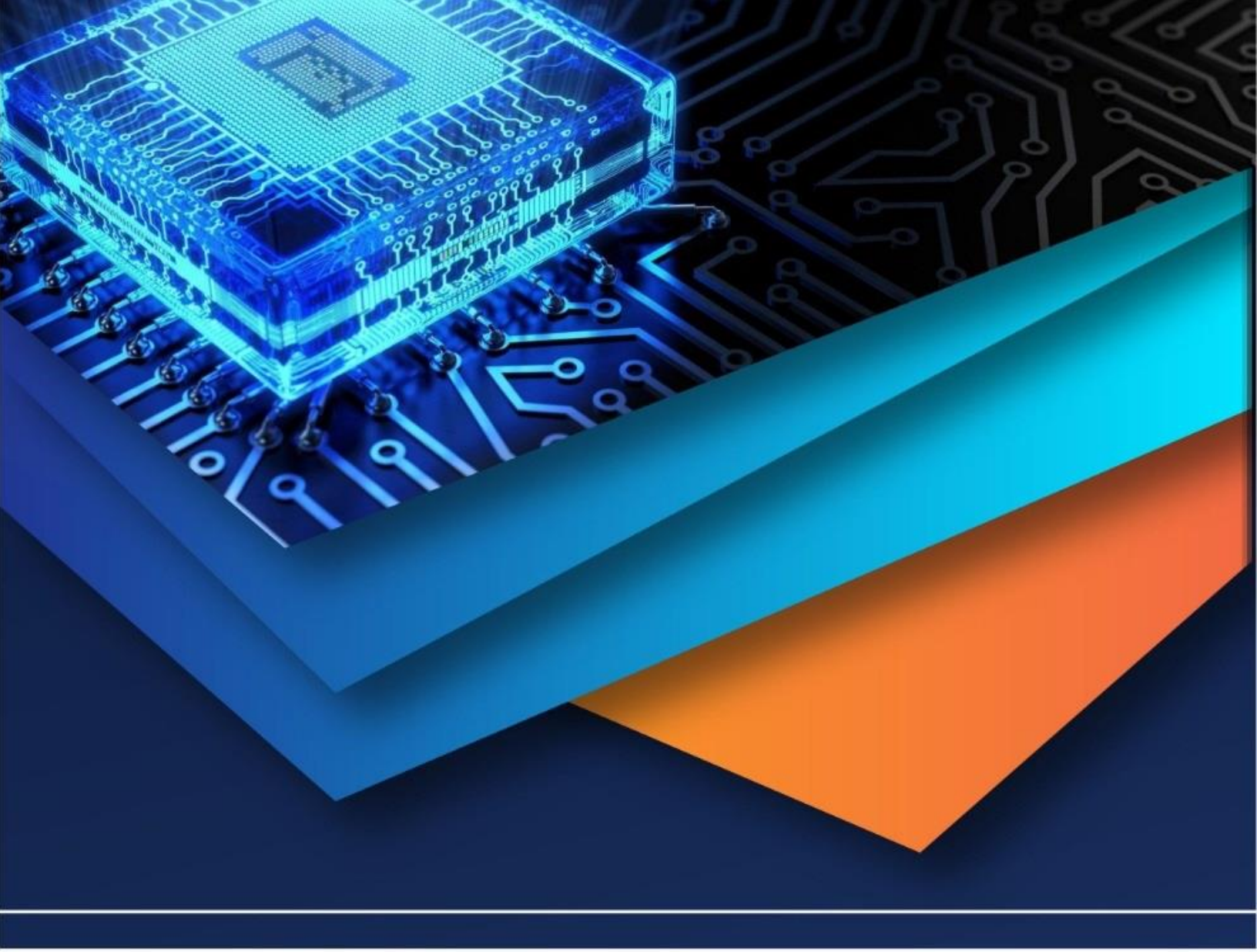
[9] Jadhav, P., Godambe, A., Gaikwad, R., & Deshpande, K. (2022). Online Certificate Generation and Verification Using Blockchain Framework. In Soft Computing for Security Applications: Proceedings of ICSCS 2021 (pp. 217-225). Springer Singapore.

[10] Shilpashree B N , Rohini Krishna Mohite , Sahana S , Rajesha, Rakesh K R, 2021, Counterfeit Detection of Documents using Blockchain, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 07 (July 2021)

[11] Lamkoti, R. S., Maji, D., Gondhalekar, A. B., & Shetty, H. (2021). Certificate verification using blockchain and generation of transcript. Int. J. Eng. Res. Technol, 10(3).

[12] Priya, S. R., & Swetha, N. (2019). Online Certificate Validation Using Blockchain. International Journal of Advanced Networking and Applications, 132-135.

[13] Mara, P., & Motupalli, R. K. Blockchain-based model to track and verify official certificates. International Journal of Engineering Technology and Management Sciences, 6(1).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY