Decentralized Smart Contract Certificate System Using Ethereum Blockchain Technology

K. V Raghavender(✉), S. Alankruthi, A. Akhila, T. Preethi, and M. Ashritha

Department of Computer Science, G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, Telangana, India
kvraghu2011phd@gmail.com

Abstract. Traditional paper certificates and electronic certificates are difficult to handle and preserve, may need third parties to authenticate the certificate, take a lot of time, and have a potential of being tampered with. People routinely fabricate certificates to represent their credentials and degrees. A false certificate created by a skilled con artist is never easy to spot and address as the real one. As a result, it is imperative to enhance the certification and verification procedure. So, to avoid such issues, we want to develop a project where we can use blockchain technology for verification of certificates. Initially University will enter the students roll number and upload their college certificate and it will be stored on Interplanetary File System (IPFS) by generating a hash which uniquely identifies that block. Now any person like the student or recruiter or an administrator can fetch and verify the college certificate by providing a unique hash value and roll number of the student. And we can also validate the certificate by providing the certificate and roll number of the student in case we forget the generated hash value. This can result in increased security, lower costs, and a quicker platform for verifying educational certificates.

Keywords: Ethereum · IPFS · Smart Contracts · MetaMask

1 Introduction

The fundamental pattern of a student's education in India is to enroll in kindergarten, then transferring to a different school for elementary, middle, and high school courses. After graduating from secondary school, pupils must now apply for admission to junior college. For students, this is the basic cycle of the academic year. This cycle has the drawback of requiring a student to submit all the certifications for approval at each stage. This could result in the certificate being broken or lost. Also, the validator finds it time-consuming to authenticate each certificate. It is quite difficult to maintain track of and certify such a large number of records due to the country's massive population. Certificate manipulation and the creation of false certificates consequently turn into negative occurrences. As technology advances, it becomes easier to create fake certifications. It will need a lot of focus to distinguish between a real certificate and a phoney one, which will waste time. Finding a clear solution necessitates a major investment of time, money, and resources.

B. Raj et al. (Eds.): ICETE 2023, AER 223, pp. 452–461, 2023.
https://doi.org/10.2991/978-94-6463-252-1_48

Blockchain technology holds the promise of eradicating this flaw. Why then utilize Blockchain? because it is impossible to change data in a blockchain under normal circumstances. Even when data is altered, it only takes a little period of time for us to notice the difference. The system would always be trustworthy and authorized. The problem of tampering is now resolved. The time required for validation is the next problem that is raised. The system we design will store certificates in addition to validating them. Because everything is automated, validating the paper simply needs a few seconds. The certification process will retain everything digitally, so a student won't have to be concerned about the certificate becoming lost or damaged.

1.1 Problem Background

The problem arises with the student certificates in each stage of student's life for validation. As the data is huge, sometimes the data may be lost or tampered. The validator finds it challenging to authenticate each certificate. The production of false certifications is getting simpler as technology develops. Differentiating between authentic and fraudulent certifications takes a lot of labor, which takes time. Because of centralization and digitization, the issue of fraudulent credentials has become a headache for both colleges and recruitment firms. Innocent people's lives might be lost as a result of false buildings planned by false engineers and false medical care provided by false physicians. At the very least, it is necessary to properly validate the certificates before allowing someone to join the organization.

1.2 Problem Definition

Every person's identity document must be issued and verified in a rapid, dependable, and secure manner. The mechanisms already in place are operational, but because the procedure often takes several weeks, the efficiency and security need to be increased. This is not just a hassle and a waste of time, but it's also costly financially and environmentally. The solution for this problem is to detect fake certificates, store certificates and make organizations certificate verification easier without the help of third party. Creating a website using Ethereum blockchain technology that doesn't allow data tampering and which makes storage and validation of certificates easier is a way to create a system that facilitates all the requirements and makes the process of verification and storage simpler.

1.3 Contribution

The following are the main contributions to the research work: In order to verify certificates without use of third party or central authority, we had developed a website which uses SHA-256 algorithm to generate hash for the certificate which is stored in blockchain. This hash is unique and irreversible. It minimizes manual work required for their verification and ensures security.

The remaining part of the paper follows the same format. By describing current methodologies and systems, Sect. 2 illustrates the relevant research on existing certificate verification systems. Section 3 presents the suggested approach for verification

of certificates using Ethereum Blockchain Technology. Section 4 of the proposal finishes with a presentation of the results together with any limitations and any future recommendations.

2 Related Work

To recognize false documents and certifications, both in paper form and digital form, research has been ongoing. The project focuses on developing a mechanism for both storing immutable certificates and validating them. The following techniques have been suggested to reduce the use of fraudulent documents and publications. Blockchain technology and digital certificate validations were the main topics of the survey. An Enhanced Web Base Certificate Verification System [5] was the title of our first paper. It used the object-oriented and design methodology (OOADM), with HTML5, CSS3, Bootstrap, and PHP5 as the frontend and backend programming languages, respectively. The fact that it is centralized, requires a third party, and involves manual verification is a major drawback. The second publication, An Overview of Blockchain Technology [15], gave further information about Blockchain. It defined a number of words related to this technology, including the most crucial idea known as a smart contract. The Blockchain generates a long chain of nodes and stores the data's hash in the block before it. When data is changed, its hash will modify and cease to correspond to the value recorded in the preceding block, alerting us to the change. Blockchain and Smart Contract for Digital Certificate was the title of the third paper [8]. There were 3 actors in their design. Institutions came first, followed by students, and then service providers. Their strategy had the drawback of using "one hash as a key," making it available to anyone with the hash. Next up is our tamper-proof birth certificate [11] document. With the exception of using the AES technique and IPFS to store the data, their concept was essentially identical to that of the second paper. They specifically designed their system for birth certificates. The problem was that neither the original document nor the capability to create certificates online were ever stored anywhere. We investigated a distinct paper with the title BlockIPFS (Blockchain enabled Interplanetary File System for Forensic and Trusted Data Traceability) [3] to address the issue of document storage. We learned about IPFS and how to combine it with blockchain in this paper. The results showed that BlockIPFS prevailed in the majority of areas, including upload transaction, read transaction, and download transaction, when they contrasted conventional IPFS with Blockchain and IPFS. The final paper put out a trustworthy approach for using blockchain to secure and validate graduate credentials [14]. In their strategy, the document will be produced by an issuing authority, and a hashing method will be used to encrypt it, and storing of the document's value, just like the methods used in the second and third publications. Numerous studies have already embraced the object-oriented and design methodology (OOADM), with HTML5, CSS3, Bootstrap, and PHP5 being utilized for the frontend and backend, respectively, to store university certificates. Companies are asked to send a copy of the certificate after receiving the originals from the students. Then they hire a private firm to do the inquiry. Following manual certificate verification, they transmit reports to the business conducting background checks. Additionally, no effort was made

to persuade educational institutions to use this model for the easy exchange of educational credentials with other institutions in order to facilitate the process of exchanging certificates.

3 Methodology

The proposed system offers a framework for storing and using blockchain tovalidate student credentials. It makes use of the Ethereum blockchain technology to conduct the standard verification process faster, more securely, and with simply one click,thereby saving time (Fig. 1).

Every blockchain project's foundation is a contract, a piece of code that executes on an Ethereum node. Participants who engage with our smart contract include the following:

3.1 University Admin

College has the authority to issue one or more certificates within the framework. They upload certificates into a distributed file storage system called IPFS (Inter Planetary File System). IPFS connects all computers worldwide by using a content-based addressing scheme to identify each file separately. For the benefit of other network users, any kind of material may be housed here, and users may also access content from any node that holds the particular kind of content they are looking for. Some users carry a portion of the entire quantity of data, allowing for a flexible file distribution and storage mechanism.

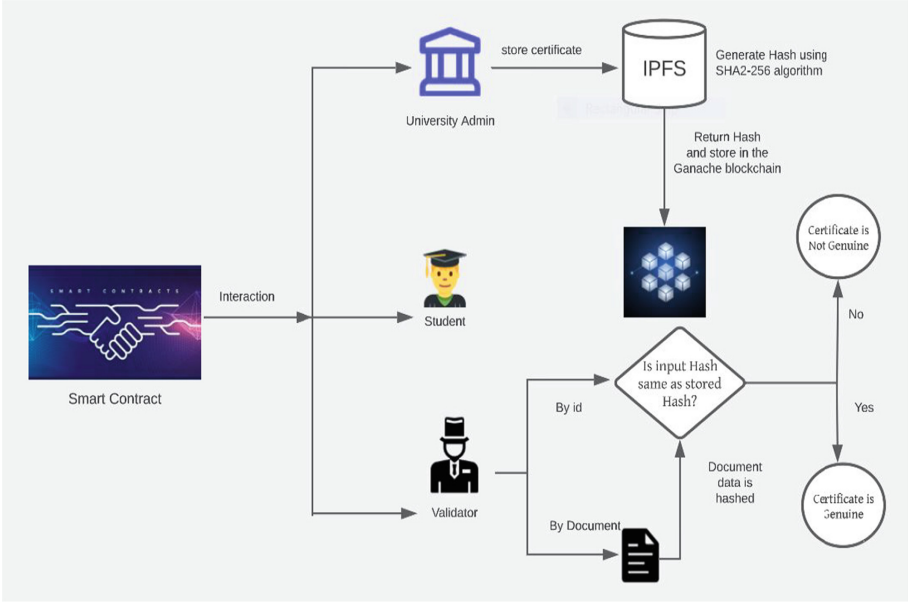

Fig. 1. Architecture of the Proposed System

When IPFS receives this data, it uses its SHA2–256 hashing algorithm to process it. SHA-256 may transform large input data into a fixed-size hash code of 256 bits (32 bytes). Hashing is always a one-way process. As a result, finding a hash function's input is computationally impossible based on the hash output. Large amounts of storage space are needed to store the original files in the database. Therefore, a method is required to identify documents in a way that are lesser than their actual size. To complete this task, a hashing method must be employed. Along with the original Document, this generated hash is kept in the IPFS and it needs to be stored in the Blockchain. For this, some generation charges in MetaMask must be approved by the issuer. This hash is then saved in the Blockchain and cannot be normally modified after that. Even in the unlikely event that the data is altered, the Blockchain's other nodes will alert you. It only takes a few seconds for us to be informed if data is changed. A specific certificate ID is assigned to each certificate that serves as the distinctive ID required for verification.

For this process, we need MetaMask extension in the browser, ganache and truffle framework using NPM and also local ipfs needs to be installed through command line. Here truffle will be used to set up the ReactJS application using "truffle unbox react" command. Then smart contracts need to be created using solidity language inside contracts folder (Fig. 2).

StoreHash.sol consists of two state variables: ipfsHash and a mapping "doc" where id [Roll number] is the key and ipfsHash is the value. It consists of two methods: send Hash takes id and ipfsHash and assigns ipfsHash to id through mapping. Verify Document takes id and hash as parameters to check the certificate's legitimacy by comparing the hashes after applying Keccak256 hash function after encoding the string into bytes. Then, truffle-config.js file should be created and network should be mapped to Ganache with network ID 7545. Now, to compile and deploy this contract launch ganache, add truffle-config.js file and save the workspace then to deploy this contract run the command "truffle migrate". The deployed smart contracts in the ganache network are as shown in Fig. 2. In ganache, there are 10 accounts with 100 dummy ethers in it and the first account is the active account which we are using during the process. The account through which transaction occurs should be imported into MetaMask to make ganache and MetaMask in sync. When the certificate is uploaded in the main page, it is transformed into a buffer and uploaded to IPFS. Then this ipfs hash and entered id is sent to send-hash method in

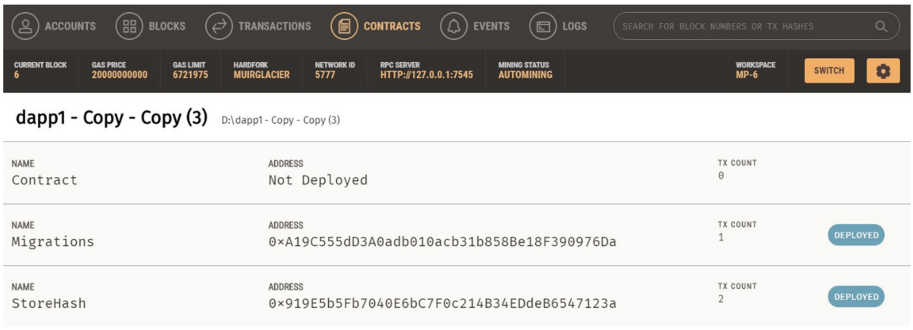

Fig. 2. Deployed Smart Contracts in Ganache

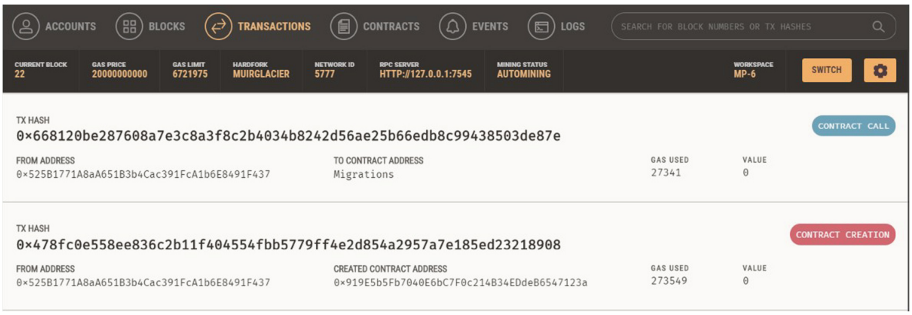

Fig. 3. Transactions in Ganache

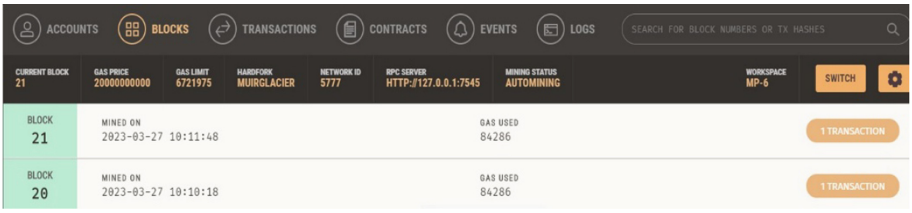

Fig. 4. Generated blocks in the ganache

store Hash contract to map hash and id. Here IPFS will be used to store content, and the blockchain will keep the created hash. When the interaction with the ganache blockchain occurs, different transactions take place for contract creation and contract call which are shown in Fig. 3.

As a result of transaction that occurs after interacting with smart contract new blocks are generated as shown in Fig. 4.

3.2 Student

Following the successful storage of the certificate in IPFS and hash in Ganache blockchain, student receives a message regarding certificate details like unique hash which is generated by IPFS and stored in blockchain and also the certificate itself.

3.3 Validator

Validator can be anyone be it university Admin, Student or any company organization. They verify the originality of the document. Verification is done by verify Document method in store Hash smart contract. They have two options for validating the document.

Validating using distinct ID:

The validator can type the specific ID of the document he wishes to validate. The validity of the certificate is determined by comparing this ID to the ID contained in the blockchain. A warning arises if a fraudulent ID is presented.

Validating using document:

The document could also be uploaded directly to the system by the validator. Data from the document is hashed and compared to the hash saved in IPFS/blockchain. If it matches, it is successfully verified else it is invalid.

4 Results and Discussion

Some of the outcomes of our implementation are listed in (Fig. 5).

4.1 Certificate Upload

Here only college admin has access to upload the certificate. Admin has to upload the certificate and student roll number and when he clicks on submit button then certificate is uploaded to local IPFS and it runs its SHA-256 hashing algorithm to get IPFS Hash and it will be stored. The identical hash will be transmitted to the Blockchain Node, where the administrator must first accept the charges in MetaMask before they can be stored to the Blockchain. After MetaMask approval, some gas fee is utilized to store IPFS Hash into the local blockchain ganache. Then a transaction hash is generated after interacting with the contract and then a new block is created in the blockchain (Fig. 6).

4.2 Certificate Verification

Using IPFS Hash

The representative of the authority may provide the specific ID of the document he wishes to validate (IPFS Hash). When the ID is equal to the ID that is recorded in the blockchain, certificate verification takes place. A problem arises if a fraudulent ID is presented (Fig. 7).

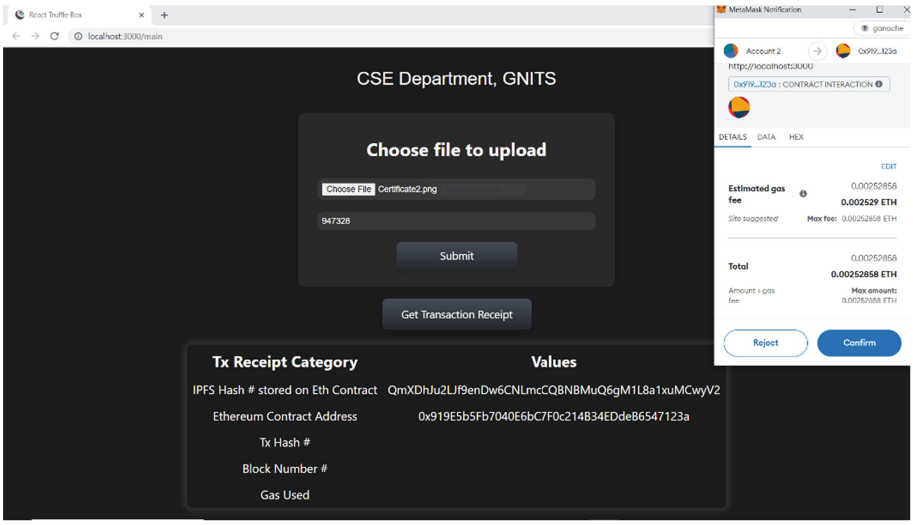

Fig. 5. Certificate Upload to IPFS

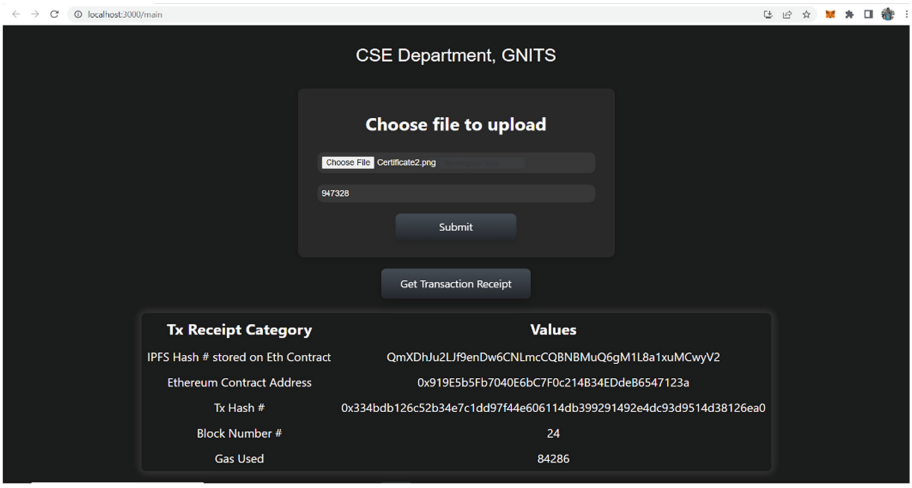

Fig. 6. Transaction occurs and new block is generated

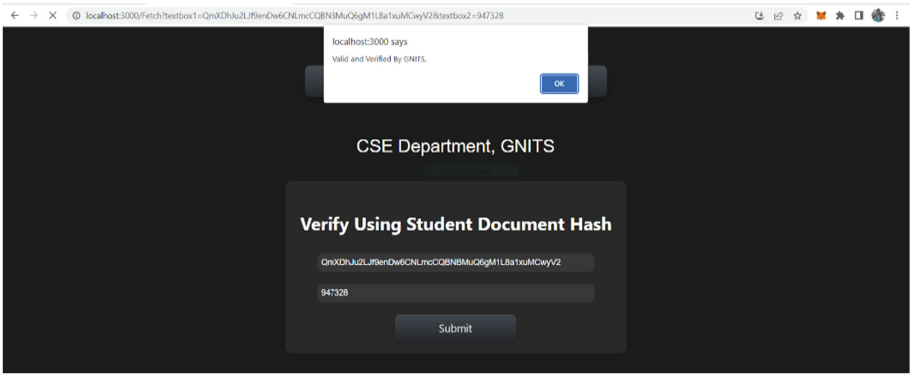

Fig. 7. Verification using Hash

Using Certificate itself

The validator also has the option of directly submitting the document. Here the information in the document is hashed and compared to the hash kept in IPFS. Based on the comparison's outcome, the output is either passed as verified or not verified (Fig. 8).

5 Conclusion and Future Scope

The proposed solution entails creating a federated blockchain amongst businesses, academic institutions, and students. Universities typically add student certificates first, and then businesses or other verifiers can check the credentials using the certificate. No one will be able to alter the data contained in a blockchain or incorporate fresh transactions that are backdated. All universities and colleges are able to use this system to add

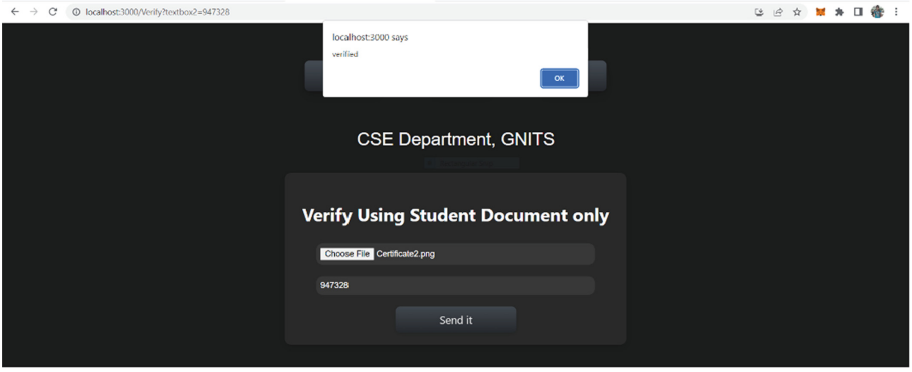

Fig. 8. Verification using certificate itself

additional protection to the certificates and student data. The System makes it easier to submit certificates while reducing the quantity of manual effort needed to verify them. And students also have a relatively low risk of losing their credentials. By using the SHA2–256 hashing algorithm, we minimize the quantity of data that has been changed. The Inter Planetary File System will hold the actual document, while the blockchain will retain the certificate's hash. This allows us to maintain data and ensure transparency.

The following are some potential future directions for the work: (i) Development of a terminal-based document authentication system that allows for multiple file uploads and incorporates additional usability elements. (ii) This can be extended to ensure the integrity of all kinds of documents, not just in education field, but in government sectors where digital time stamping of documents is necessary. (iii) To develop a feature that gets rid of the fraudulent certificates that are already present in society.

References

1. A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar and P. C. K. Hung, "A Permissioned Blockchain-Based System for Verification of Academic Records," 10th IFIP International
2. Conference on New Technologies, Mobility and Security (NTMS), CANARY ISLANDS, Spain, 2019, pp. 1–5.
3. Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.
4. Emmanuel Nyaletey, Reza M. Parizi, Kim-Kwang Raymond Choo, "BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability", Published on IEEE International Conference on Blockchain, 2019.
5. Gunit Malik, Sai Prasanth Reddy, Dr. Seema Shah, "Blockchain Based Identity Verification Model", International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019.
6. Izuchukwu Chijioke Emele, Stanley Ikechukwu Oguoma, Kanayo Kizito Uka, Emeka Christian Nwaoha "An Enhanced Web Base Certificate Verification System".

7. Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam and Shaikh Akib Shahriya,"DOC BLOCK: A Blockchain Based Authentication System for Digital Documents" Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021) , Volume-7, Issue-03, March 2021.
8. J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," IEEE ICASI, Chiba, 2018, pp. 1046–1051.
9. Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," IEEE International Conference on Applied System Innovation 2018.
10. Meerja vali Shaik, Ch. Rupa, M N S Koundinya, Rohith Gadde, Harish Donepudi, "Blockchain based Certificate Issuing System using Smart Contracts" IJITEE, Volume-9, Issue-7, May 2020
11. M. HamithaNasrin, S. Hemalakshmi, and Prof G. Ramsundar, "A Review on Implementation Techniques of Blockchain enabled Smart Contract for Document Verification," IRJET, Volume 6, Issue 2, 81, February 2019.
12. M. Shah and Dr. Priyanka Kumar, "Tamper Proof Birth Certificate using Blockchain Technology" IJRTE, Volume 7, Issue 5S3, pp. 95–98, February 2019.
13. Maykin Warasart and Pramote Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," 2012.
14. Ravi Singh Lamkoti, Devdoot Maji, Prof. Bharati Gondhalekar, "Certificate Verification using Blockchain and Generation of Transcript" IJERT Vol. 10 Issue 03, March-2021
15. T. Rama Reddy, Rayudu Srinivas, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain", Published on Springer in June 2021.
16. Zibin Zheng, Shaoan Xie," An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", Published on IEEE in 2017.
17. Shitharth Selvarajan, Gautam Srivastava, Alaa O. Khadidos, Adil O. Khadidos, Mohamed Baza, Ali Alshehri and Jerry Chun-Wei Lin, "An artifcial intelligence lightweight blockchain security model for security and privacy in IIoT systems", Published on Journal of Cloud Computing in 16 march 2023.
18. B.C. Gajarla , A.V. Rebba , K.S. Kakathota ,M. Kummari , S. Shitharth , "Handling tactful data in cloud using PKG encryption technique", conference on 4th Smart Cities Symposium (SCS 2021)
19. Mohamed Sirajudeen Yoosuf, Muralidharan,S. Shitharth, Mohammed A ghamdi,Mohammed Maray, and Osama Bassam J. Rabie, "FogDedupe: A Fog-Centric Deduplication Approach Using Multi-Key Homomorphic Encryption Technique", published on 25 Aug 2022