iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41182

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 10 Issue IV Apr 2022- Available at www.ijraset.com

Docverifer

Jashuva Peyyala
Jain University

***Abstract:** In this digital world, everything is digitalized but still, some practices are a bit unvarying, one of those is the certificate verification process. The foremost important documents are certificates for graduates from universities and other educational institutions. However, it is costly and time-consuming to check certificates using traditional methods. This paper aims to introduce a theoretical model, which can give the possible infusion for the issue and verification process of any type of document. We need to consider strong points on blockchain apart from finance, those are tracking, supply chain, etc. In this model, we are using blockchain and distributed storage. There are many functions such as hash, public and private key cryptography, digital signatures, peer-to-peer networks and work evidence in blockchain technology. In This model, we are using IPFS for distributed storage (peer-to-peer) everything in ipfs is globally available with the appropriate hash generated by ipfs, for this reason, we added multi-layer security at the Client-side, as an encryption mechanism. To Protect the documents uploaded by the issuer, we enabled an encryption mechanism at the client This Dapp (decentralize) has been divided into two parts one is the document issuer and the other one is the verifier.*

I. INTRODUCTION

In India, the educational certificate verification process is strict than promoting work in multinational corporations. From a university to another university from another university or the cycle continues, it will take a few months to handle the cycle. To interfere with this barrier, we provide this model of the online certificate verification process. We all know that everything on the internet is vulnerable at some point. The centralized network is always vulnerable to creating networks in relation to confidential data. Always dangerous. To overcome these security issues, we use distributed storage for document load and integrity of distributed networks (Ethereum). Decrypted Storage the IPFS used by this model has many distributed storage applications, but it prefers IPF because free and IPFS have no single failure point. The node should not trust each other. Distributed storage is always safe because it does not depend on all the property. One of the reasons for Industries is not interested in IPF is because the IPF is data and all people are available publicly. Do not enter confidential data for confidential data. However, this model adds security levels (client encryption) to this model and overcomes this security issue through the development of this DAPP (distributed application). The encryption algorithm used in this model is a symmetric-key method like one password will be used vice versa, using the same keys, using the same keys, and is symmetric-key encryption. One of the major significant benefits of a distributed network is often that there is no real single point, but it seems that the individual user's computer no need to rely on one central server to handle all processes. Distributed networks are expanded to add more computing power to the network by adding additional machines to the network.

II. PROBLEM STATEMENT

A. Why Blockchain?

Unfortunately, counterfeit documents are rampant in today's world, and as most of you know, it is not difficult to obtain counterfeit documents. Because counterfeit documents look exactly like the originals, it is difficult for non-professionals to distinguish real documents from replicas. Service providers have to spend millions of dollars to verify candidates' documents. However, blockchain is also used in the document verification process. In the underhood of blockchain technology, digital certificates can solve the above problems. Let's see how detailed it is in this article.

1) Verification of documents using blockchain technology limits the cost of transactions on the network by excluding third parties. This greatly saves money.

2) Certificates are stored on a distributed log allowing people to access information anytime, anywhere. On the blockchain, documents are hosted securely and only authorized individuals can access documents with their private keys.

3) Blockchain technology stores data in an immutable form through encryption, which uses a hash function to encrypt the data. Therefore, the data cannot be changed. Hacking is almost impossible.

4) No more scalability issues as transaction times can be as short as a few seconds. Therefore, documents verified on the blockchain enable rapid service provision. Checking the document is a common phenomenon because it is related to people who are far away. Regardless of whether new births, marriage, trials, employment, or vitality are new, you should check the document for each lifetime. It can be effectively made through blockchain technology.

©IJRASET: All Rights are Reserved

The identification of the document today is not only intense as well as defective ideas through blockchain technology. In Blockchain technology, documents that need to be calm are installed in a distributed book. This is not a digital replica or not a copy of the encryption stored on the blockchain network.

III. LITERATURE REVIEW

1) Review 1

On the modern web, HTTP is the preferred protocol for transferring files. Effective for moving small files. However, HTTP cannot implement any other more efficient file distribution method. The IPFS is a wide-ranging p2p file system that addresses issues related to data reliability, fault tolerance, consistency, and non-repudiation of current systems. In this model, we have proposed an innovative and efficient way to store and retrieve files on the Internet using IPFS. uploading files is simplified and high data security is ensured. Although there are so many effective approaches in which files are stored in distributed systems, approaches using distributed storage protocols are deprecated and provide a new dimension to applications. [A. Manoj Athreya, Ashwin A. Kumar, S. M. Nagarajath, H. L. Gururaj,V. Ravi Kumar, D. N. Sachin, and K. R. Rakesh]

2) Review 3

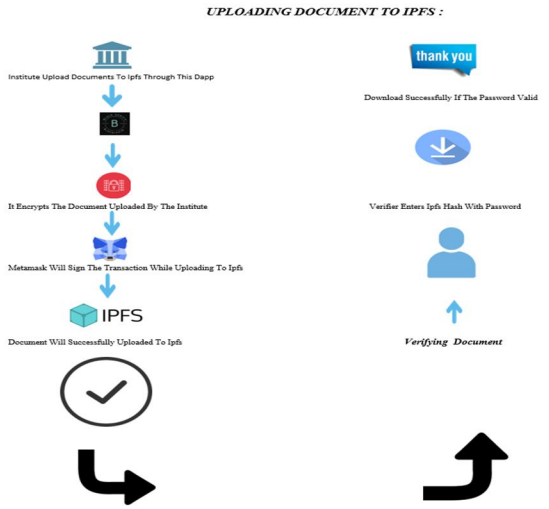
Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data:

The encryption algorithm used in this model is Advanced Encryption Standard is an encryption algorithm that uses a symmetric key approach cryptographic developers use this model widely. The functionalities of This algorithm have their own structure to encrypt and decrypt file content in their own way. It is difficult for malicious users to get the original data when encrypting by the AES algorithm. No way to crack this algorithm so far. There are countless beautiful features we have found in this research when compared to other algorithms in the cryptographic world DES, 3DES, Blowfish, etc. this is the main reason we have picked this algorithm for this model.

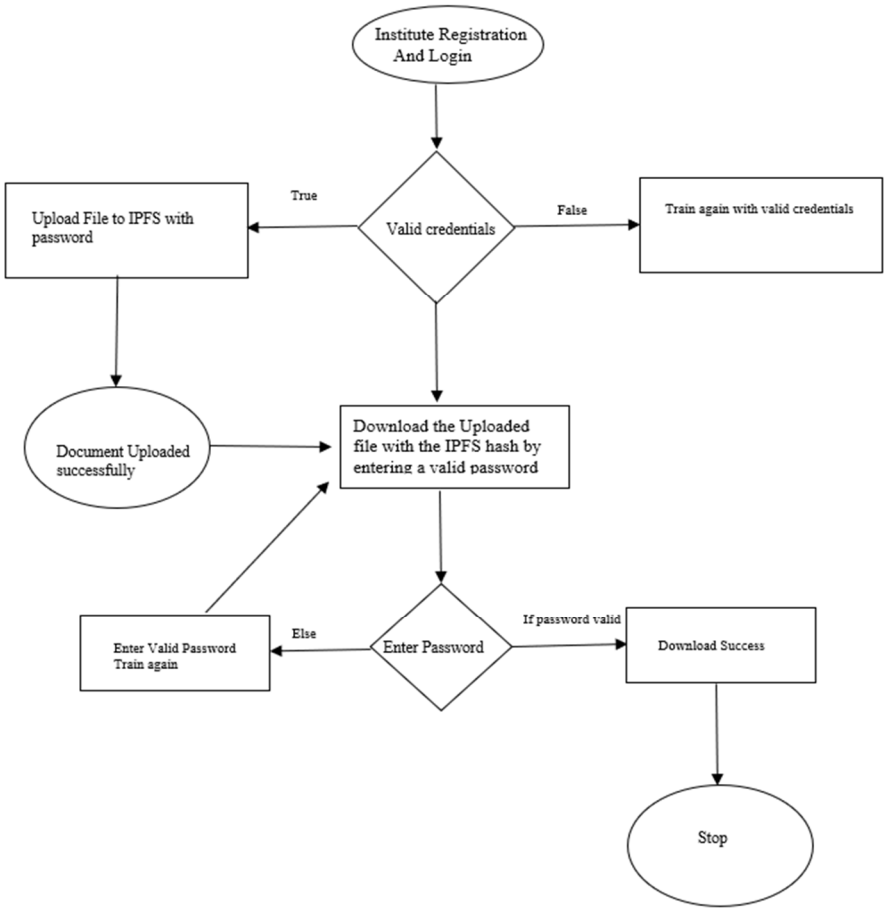
IV. DESIGN AND IMPLEMENTATION

The Dapp (decentralized application) purely built on reactJS, is a framework that was built on JavaScript programming language. In this model, we are using web3 functionalities and a blockchain network called Ethereum and truffle is a development environment, testing framework, and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM). This truffle will help our app to interact with solidity contracts we are written. This model will be an advantage to the institute and organizations that are using background verification in the traditional way like physical thorough verification. We have built this model in a secure manner so that the document data will not spill out of the app at any cost because we are encryption the document at the client-side using the AES encryption model and on transmission, the ipfs network will encrypt the traffic if any case you are network is vulnerable the data will be in safe and secure hands.

A. Dapp Design



B. DAPP ER-Diagram



Implementation: The implementation of the model is followed by two steps as Document issuer and document verifier.

C. Functionalities of Document Issuer

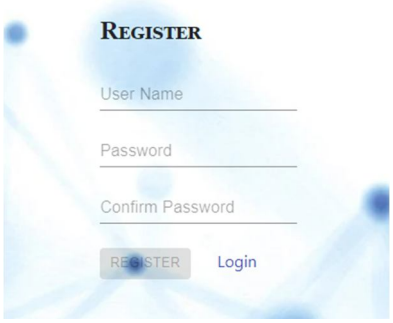
1) The document issuer will create an account on the application after successful validation, he will log in to our application.
2) Foremost important thing is the issuer must have a meta-mask wallet installed on their web browsers
3) Next step involved uploading the document to ipfs through our application.
4) While uploading a document we will prompt a password field to encrypt the document after password completion the issuer will click the submit button.
5) On Clicking the submit button the meta-mask will arrive and ask for some fee to upload the document to the blockchain main network usually call it eth gas fee approx. 2-3$ for the document.
6) After successful pay the gas fee the ipfs hash will be updated on the blockchain and our application will give the ipfs hash for more forth usage like downloading the document or verifying of the document.

D. Functionalities of Verifier

1) The issuer does not need to register to our app to download the document.
2) The issuer will enter the ipfs hash along with a valid password provided by the issuer.
3) On clicking the submit button our app will fetch the document from ipfs and decrypt the document on the client-side and download it to the local file system.
4) The verifier can able verifier who uploads the document to the ipfs with transaction id and issuer metamask Ethereum address since will build on the Ethereum network
5) This way the verifier can ensure the document is uploaded by the authorized institute.

E. Application Model

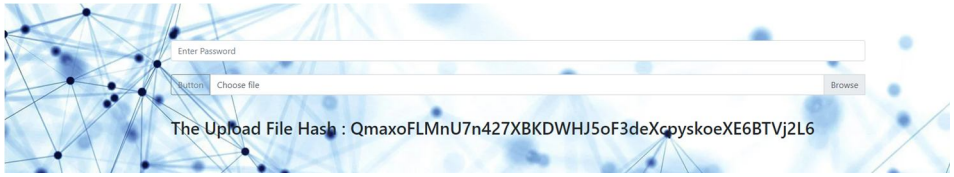
Registration Page



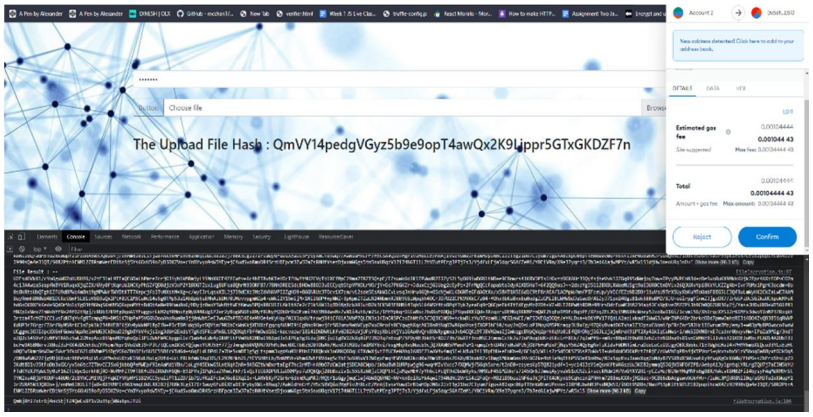
Verifier Page



File Uplaod Page



The Encrypted file format: [Development mode]



Modules in this Project: there are so many modules we are used in this module but the major modules are:

1) CryptoJS
2) Web3
3) IPFS-API

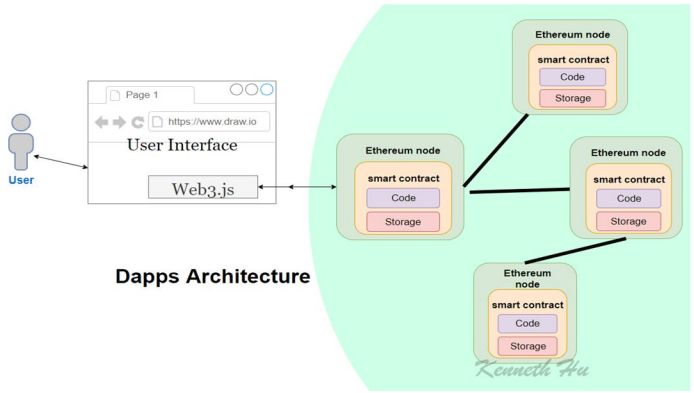
F. Brief Explanation of These Modules

CryptoJs: CryptoJS is a growing collection of standard and secure cryptographic algorithms implemented in JavaScript using best practices and patterns. They are fast, and they have a consistent and simple interface.

Crypto is a module in Node.js that deals with an algorithm that performs data encryption and decryption. This is used for security purposes like user authentication were storing the password in the Database in the encrypted form.

The Crypto module provides a set of classes like hash, HMAC, cipher, decipher, sign, and verify. The instance of that class is used to create Encryption and Decryption. Node.js cannot create a class object using the new keyword.

Web3: Web3 .js Ethereum JavaScript API, web3.js is a collection of libraries that allow you to interact with a local or remote Ethereum node, using an HTTP or IPC connection. The web3 JavaScript library interacts with the Ethereum blockchain. It can retrieve user accounts, send transactions, interact with smart contracts, and more.



IPFS-API: ipfs-API is a client library for the IPFS HTTP API, implemented in JavaScript. This client library implements the interface-ipfs-core enabling applications to change between an embedded js-ipfs node and any remote IPFS node without having to change the code. In addition, this client library implements a set of utility functions.

1) Test Case 1: We have tested our web application by uploading various types of files

2) Test Case 2: Uploading an image file and returning the file encryption on the chrome console

a) The has been encrypted with AES CBC encryption method

b) The cryptoJS not only encrypt the file itself and also encode the password with the latin1 encoding.

c) After successful submission of the file, we will get the ipfs hash that has been returned on the web browser.

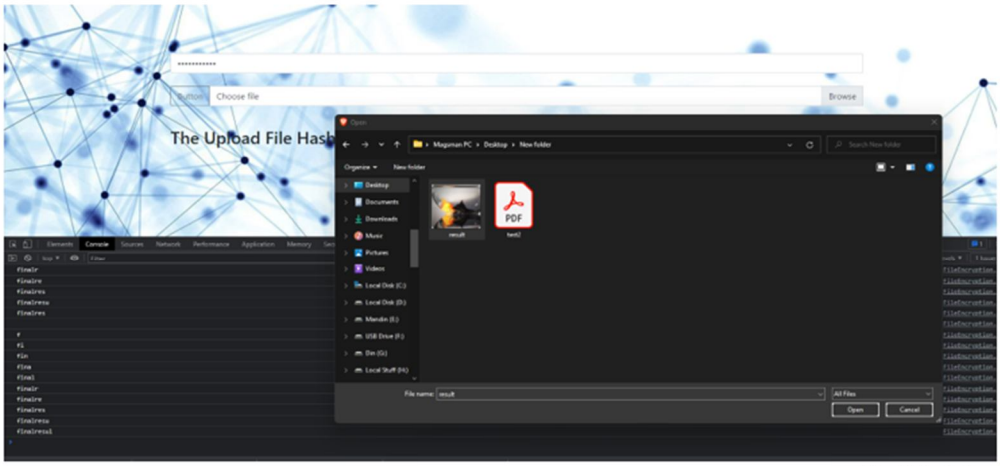


Fig 9.4 -9.6

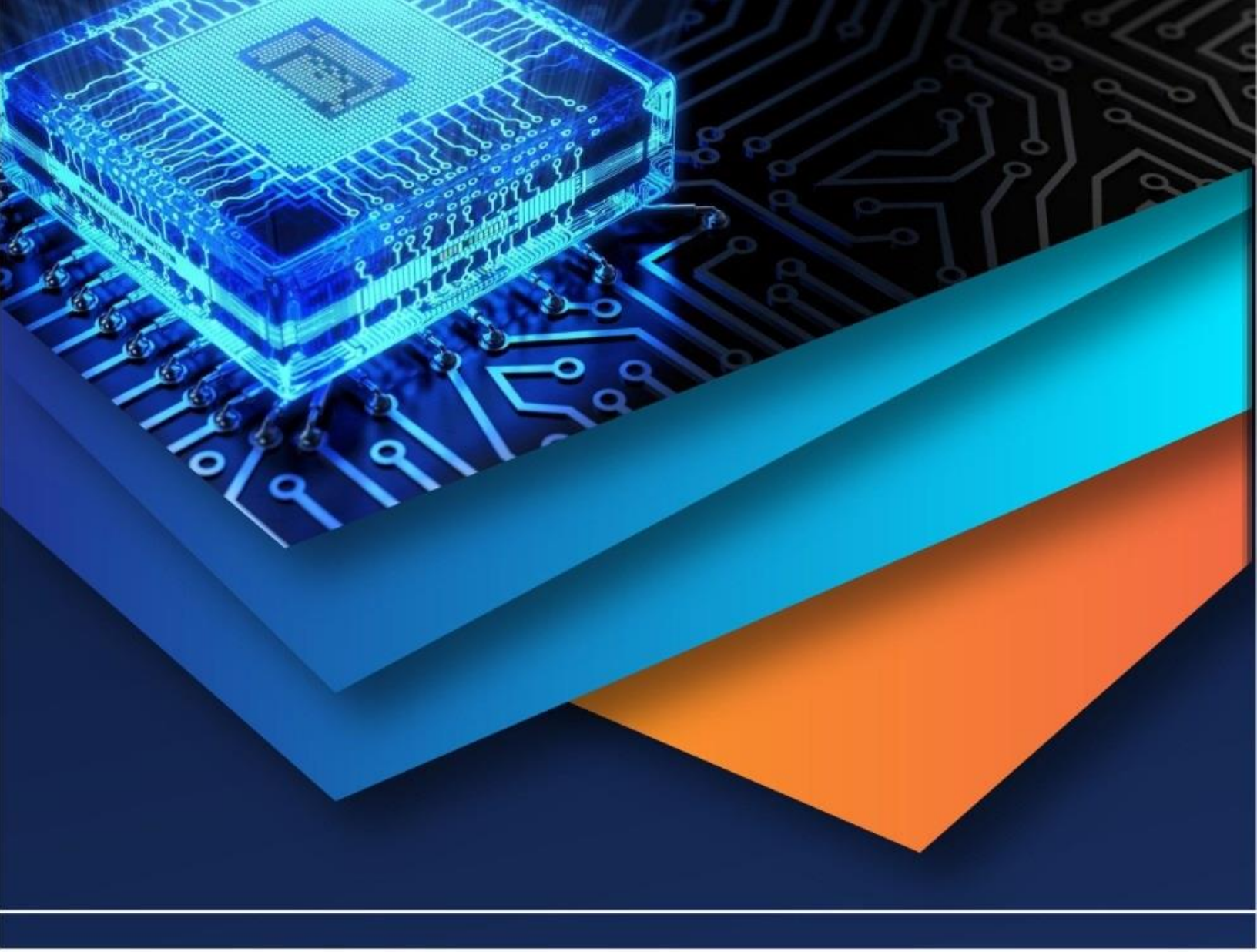


V. CONCLUSION

Despite many restrictions on data security and confidentiality, various techniques have been discussed to reduce certificate counterfeiting and ensure the security, validity, and confidentiality of graduation certificates. A new blockchain-based system reduces the possibility of certificate forgery. The automatic issuance of certificates is open and transparent in the system. Thus, a company or organization can request information about any certificate from the system. The proposed system Lower management expenses and forbid document forgery, and provides accurate and reliable information about digital certificates. Despite many security and data privacy restrictions, various techniques have been discussed to reduce certificate counterfeiting and ensure the security, validity, and confidentiality of graduation certificates. A new blockchain-based system reduces the possibility of certificate forgery. The automatic issuance of certificates is open and transparent in the system. Thus, a company or organization can request information about any certificate from the system. In this way, the verifier can lower the organization's cost while doing the background verification.

REFERENCES

[1] Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate" Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)
[2] Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, Wenlin Han "Security Applications and Challenges in Blockchain" Published in IEEE International Conference on Consumer Electronics (ICCE) 2019
[3] 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 (ITASEC17) 2017
[4] Neethu Gopal, Vani V Prakash "Survey on Blockchain Based Digital Certificate System" International Research Journal of Engineering and Technology (IRJET) Nov 2018
[5] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2018.
[6] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)