iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.51019

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 IV Apr 2023- Available at www.ijraset.com

Secure Storage and Certificate Verification System Using BlockChain

Mrs. M. Anitha[1], O. Tulasi[2], P. Maneesha[3], R. Jyothika Reddy[4], N. Lahari[5], M. Sagari[6]
[1]*M. Tech, Asst Professor, Department of CSE, BWEC, Bapatla, Andhra Pradesh, India*

Abstract: ***Over the years there has been a great need for quick and easy ways to verify your score/certificate to reduce certificate level or forgery and relieve stress as well as save time on certificate verification which today is done manually what for Your employer or whoever applies need to come or send a delegate to the school to verify a specific certificate, some employers have never done this and it has resulted in the acceptance of a fake The system can be implemented as a standalone website (recommended) or integrated into an existing official institution website. The aim of this study is to design an online certificate examination system based on the university's performance examination procedure.***
Keywords: blockchain, digital certificates, confidentiality, reliability, availability

I. INTRODUCTION

The Internet is one of the most commonly used means of exchanging information between people. Electronic data transmission breaks the barrier of distance. Steve Lawrence, Lee C. Giles, Kurt Bollacker (1999) The rapid development of the scientific literature has resulted in researchers constantly struggling with information overload in their quest for knowledge. Also, everyone should be able to browse the same websites and have the same user experience online.In other words, the Internet must be accessible to everyone. The online certificate verification system paves the way for the future development of certificate authentication. The promotion of the online certificate review system will bring tremendous benefits to society and business. The online certificate verification system improves the speed and quality of certificate authentication services, promotes market globalization and reduces costs. The system is aimed at employers and universities. This document emphasizes the need to implement an automated online verification system to avoid overwhelming a manual verification method. This will allow anyone or the employer to check the school report online without having to visit the school for this purpose. The employer just needs to access the verification link provided which is a link to the university portal and enter the number of the certificate they wish to verify, then the original of that certificate will appear on the screen with the following message (assuming the certificate holder is name “NjoeteniOrikeze”), “NjoeteniOrikeze graduated from the Faculty of Computer Engineering at Michael Okpar Agricultural University in Umudike in 2015. Carefully compare the certificate you have there with the one on the screen, any change will invalidate it, however if the certificate number is invalid (eg.and fake certificate number), the screen shows the message "Invalid certificate, we do not have this person's details in our registry, or you forgot to enter the certificate number, or the owner has not passed this authority.

A. Motivation

Conception of an online certificate examination system based on the university performance examination procedure.

1) The outdated paper/manual method has been removed, although the documents are still kept securely in the schools for future use.
2) Facilitate access to the certificate
3) Save time and resources
4) Avoid risks during transport when verifying results etc.

B. Objective

1) *Efficiency:* Consider the accuracy, speed and completeness of the system results.
2) *Flexibility:* It is the ability of the system to adapt to the changing needs of users. This is also related to the portability of the system.
3) *Practicality:* It is the ability of the system to withstand long periods of use by the user. • Security: Apply security measures to protect data, including hardware reliability. The system scan must have a working security platform to protect the system from unlawful damage and unauthorized users

© IJRASET: All Rights are Reserved |

C. Existing System

Currently, the usual method of verifying a certificate is a manual process where the institution/organization wishing to verify the result should visit the university or send a written request for verification of the result. The request then goes to academic questions related to the library or secure files for finding duplicate certificates, this can be time consuming, also sometimes files are lost moving from one office to another and in some cases the number absent or difficult to locate.

D. Proposed System

The online certificate examination (OCV) was implemented via a web server. The software components of the graphical user interface (GUI) screens act as the user interface. The database is implemented in my structured query language MYSQL. The system comes with a certificate associated with the object (eg.MOTHER). This certificate verification system will follow the same process in your institution, but this time it will be online and automated. The system will be adjusted so that each certificate number is linked to student data. Any person or organization wishing to verify the certificate must have a certificate number and enter it in the Enter Certificate Number field. A poll was conducted with an interview question on “Public Opinion on a Certain Issue”. interviews were conducted in different places such as schools, companies and public places. Questions asked during the interview ranged from; The ease of use, the feeling of anonymity, the security and the look of the user interface, as well as the information collected were very satisfactory. The first approach will be to configure the system via the existing university portal. The disadvantage of this approach is the ambiguity of the data tables of the science portal and the so-called individual entries. In the certificate table, the same field can contain multiple values.These multiple values can be "combined"; to values in other domains and how that relationship is captured and used. However, information about these relationships will not be publicly available.

II. LITERATURE REVIEW

The academic subject is usually responsible for coursework and the timeliness of honors awarded to each student. It has a set of sources, resources and services and a structure in which it is hosted. Undoubtedly, many certifications in this area speculate on the future role of security measures (mini-libraries), none of which is particularly clear. Since (1995) or what Tenopir calls the "post-networking world" (2003), libraries have been seen as threatened by the " replacement". leads to questioning the value of libraries and their collections. This review will not speculate about these future roles, but will focus on the certainty of evolving technologies, increasingly digital information resources, and societal changes that have changed user expectations of an online certificate verification system. Digital libraries are in unique environments, so environmental factors were also examined for their impact on users' awareness, acceptance and habits. Often the social contexts or domains surrounding the online certificate review system are very different, for example they vary from institution to institution. Adams and Blandford (2004) show why it is important in academia to promote the digital library as a source of knowledge, but to show users in the clinical setting (eg. information-based medicine) who is 'more important' when making decisions. In this article we present the basic elements of the manifesto and present the main aspects of the digital library structure.

A. An Enhanced Web Base Certificate Verification System

Izuchukwu Chijioke Emele, Stanley Ikechukwu Oguma, Kanayo Kizito Uka, Emeka Christian Nouha; Emele, Izuchukwu-Chijioke; Emele Chijioke; Emele, Izuchukwu Chijioke (2021) in [1].

The goal of this work is to design and implement an improved marriage certificate verification system that will help partner schools and organizations to certify the authenticity of a student document by showing the details and format of the certificate with the photo of the owner. This work was motivated by Fake certificate, waste of time and stress of manual processing. The result of the project was an improved online certificate verification system that can verify and authenticate student certificates and display the certificate image after the verification process, which can reduce the high fraud rate of uncertified certificates only in the education system. but also in other cooperating organizations.

B. Blockchain Based Certificate Transparency and Revocation Transparency System.

Ze Wang et al [2] has developed a blockchain-based certificate revocation and transparency system. In this system, the certificate authority (CA) signs the certificate and the entity (certificate authority) publishes information about the revocation status of respected certificates. Public logs are used to monitor the performance of certificate authorities. This system was implemented in the Firefox and Noix browsers. This system provides trust, but certificate validation is delayed and gives a false sense of security.

© IJRASET: All Rights are Reserved |

C. Decentralized application was designed based on Ethereum blockchain technology.

Jin-chiou et al [3] have developed anti-counterfeiting software. Due to the lack of tamper protection, the diploma requires tampering. Therefore, the decentralized application was designed based on Ethereum blockchain technology. First it generates a digital certificate for the paper certificate, then the hash created for the certificate is stored in the blockchain system. Another scanning program was also required to scan the certificate during the verification of the authenticity of the certificate. The system saves paper and prevents forgery of documents. However, the QR code must be scanned with a smartphone and an internet connection is required.

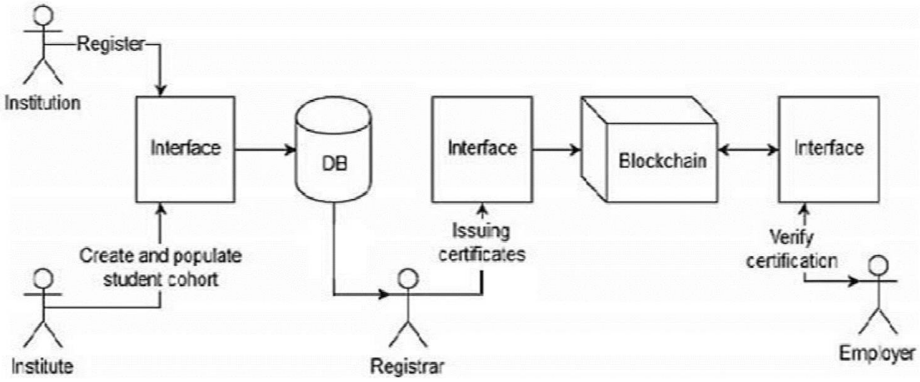
D. Certificate Validation through Public Ledgers and Blockchain.

Macro baldie et al. [4] have developed a system of so-called validation of certificates through public registers and blockchain. In this system, CRLs (Certificate Revocation Lists) were distributed on a private blockchain and made available by certificate authorities. CAs are responsible for issuing certificates to subjects that comply with the requirements and maintain the CRLs. The certificate revocation list was available and certificate authentication was still available. The certificate revocation list for the certificate set was maintained by the same certificate authority that issued the certificates. The CA ecosystem is fragile and prone to compromise.

E. System based on syndicated blockchain technology.

Aisong Zhang et al. [5] has developed a system based on syndicated blockchain technology. They used a secret identification system. It can verify the digital certificate to protect the user's information and property. Revocation lists for digital certificates in cooperation with certification authorities.

III. SYSTEM ARCHITECTURE



A. Modules Description

1) Authentication Request (AR), when a request from a user for a document verification question arrives, the proposed model validates and verifies the user's authenticity by connecting to the user's authentication server.

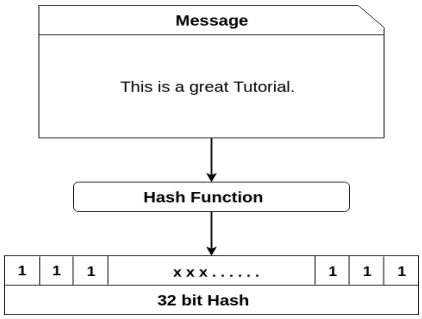
2) Verification Server (VS), After completing the user authentication, the request is forwarded to the service provider to obtain the requested service from the list of available services, then the user enters the candidate's name and matriculation number, and the server compares the result with the university database and from that generate result.

3) Service Provider Management (SPM) The service certified and depicted above must then be managed to achieve user or end-user satisfaction. Essentially, the model monitors the mapped service for profitability, service delivery time, and quality. The model would also be responsible for the secure service by uploading and delivering the service through a secure transmission channel that ensures user satisfaction. Figure I. shows that when the user requests document verification, the service provider first authenticates the user with a username and password and provides a list of services for that user, then the user provides the name and candidate identification number for verification. Document Review Server. The server then checks the document from the university database and generates a result for the user. This cloud-based document verification architecture offers solutions to overcome the shortcomings of your existing document verification system.

© IJRASET: All Rights are Reserved |

B. Algorithms And Techniques

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic byproduct of a hash algorithm. We can understand it from the following diagram.



The hash algorithm has unique properties:

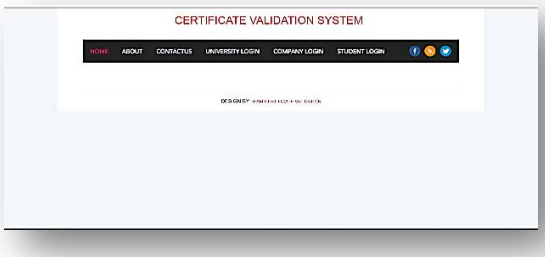
It produces a unique output (or hash). It is a one-way function. In the context of cryptocurrencies like Bitcoin, the blockchain uses this cryptographic hash function's properties in its consensus mechanism. A cryptographic hash is a digest or digital fingerprints of a certain amount of data. In cryptographic hash functions, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed size.

IV. RESULTS AND ANALYSIS

Here, in the process of certificate verification. There are two cases to be find out. They are:

1) Whether student details found in the database or not.
2) We will also check the uploaded certificate is tampered or not.

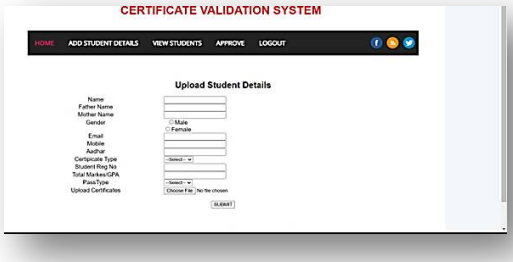
A. Initial Home Page will Look like This



B. Whether student details found in the database or not

1) At University side

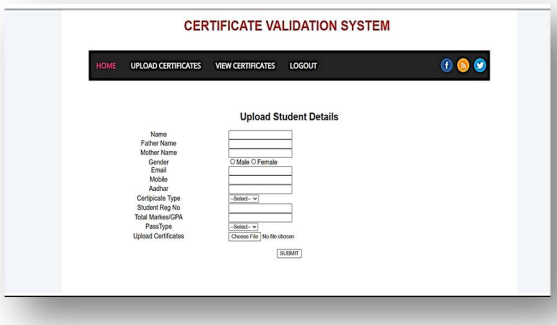
- First, University has to create an account and then after login to that site, it has to upload their student details to the database.



© IJRASET: All Rights are Reserved |

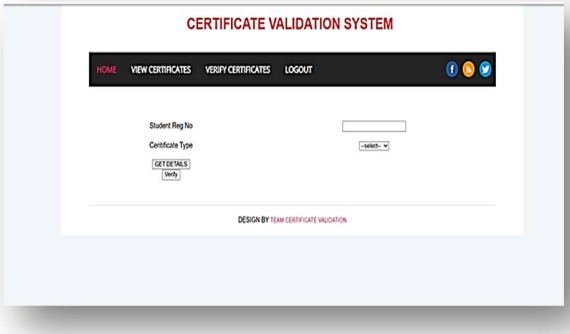
2) At Student side

- The candidate who wants to apply for a job also has to register in the company site, after creating account he/she should upload their details along with the certificate to the company.

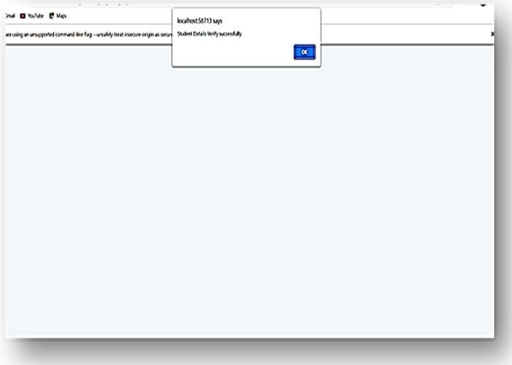


3) At Company side

- Company also should have their own website
- Here, company will check whether candidate details and certificate are original or fake by comparing with details of the database of that particular university which that candidate specified while uploading to company.

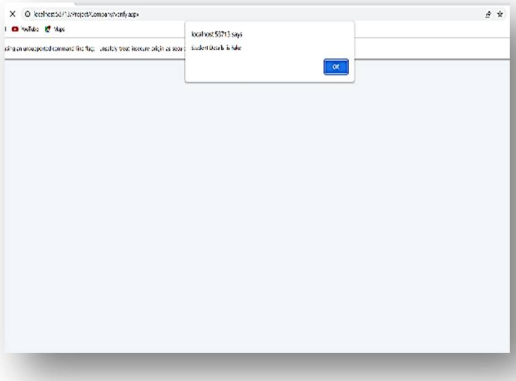


a) Case-1: If student details match with the details present in the university database



If the candidate details found in the database then we observe verify successfully prompt will display.

b) Case-2: If student details doesn't match with the details present in the university database



If the candidate details didn't found in the database then we observe student details is fake prompt will display.

C. Certificate is tampered or not is to be checked

Here, the same process taken place. If certificate is tampered then student details is fake prompt will display or else student details verified successfully prompt will display

V. CONCLUSION

We launched an online certificate review system that uses cloud computing to review academic documents online. The online certificate verification system provides an easy to verify and manage solution to bring the cloud computing paradigm into the online certificate verification system for different types of users with a single click. Providing data verification over a secure channel using the cloud concept. In addition, this can be extended to other types of data verification systems according to the needs of the system.

VI. FUTURE WORK

In the future, the proposed approach will be extended by developing robust security measures to prevent unauthorized access and ensure data privacy.

Some potential future applications of certificate validation include:

1) *Digital Identity:* The use of digital identity for certificate validation can provide a secure and reliable way to verify identities online.
2) *Supply Chain Management:* Blockchain technology can be used to validate certificates such as product quality, safety, and sustainability.

Overall, the future scope of certificate validation is vast and we can expect to see more applications of technology in various sectors in the coming years.

REFERENCES

[1] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi and Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate", *IEEE International Conference on Applied System Invention (ICASI)*, 2018.
[2] Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, D. Zha et al., "Blockchain-Based Certificate Transparency and Revocation Transparency" in Financial Cryptography and Data Security. FC 2018, Berlin, Heidelberg: Springer, vol. 10958, 2019.
[3] D. S. V. Madala, M. P. Jhanwar and A. Chattopadhyay, "Certificate Transparency Using Blockchain", *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 71-80, 2018.
[4] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Bas Blockchain", *Journal of Physics: Conference Series*, vol. 1069.
[5] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi, "Certificate Validation through Public Ledgers and Blockchains", Proceedings of the First Italian Conference on Cybersecurity.

BIOGRAPHIES



Ogiboyina Tulasi [B. Tech]
Student, Dept of Computer Science and Engineering, BWEC, Andhra Pradesh, India.



Palikithala Maneesha [B. Tech]
Student, Dept of Computer Science and Engineering, BWEC,
Andhra Pradesh, India.



Reddy bathulaJyothika Reddy [B. Tech]
Student, Dept of Computer Science and Engineering, BWEC, Andhra Pradesh, India.



Narravula Lahari [B. Tech]
Student, Dept of Computer Science and Engineering, BWEC, Andhra Pradesh, India.

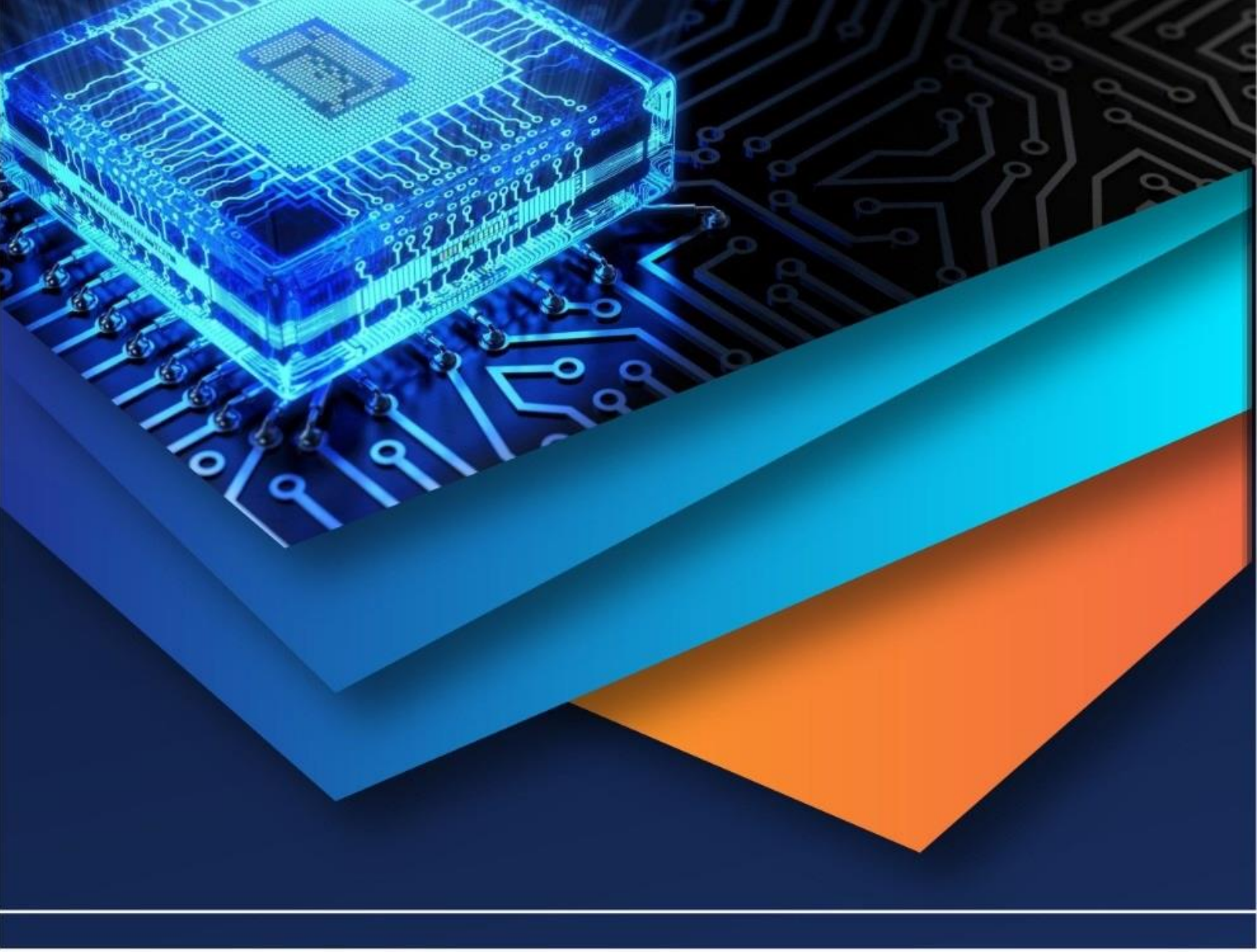


Mandapati Sagari [B. Tech]
Student, Dept of Computer Science and Engineering, BWEC, Andhra Pradesh, India.



M. Anitha, M. Tech, Asst Professor,
Dept of Computer Science and Engineering, BWEC, Andhra Pradesh, India.

© IJRASET: All Rights are Reserved |



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)