iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59238

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 12 Issue III Mar 2024- Available at www.ijraset.com

Digital Evidence Protection System Using Blockchain Technology

Reddyvari Venkateswara Reddy[1], Mrs. K. Nishi[2], Velishala Vyshnavi[3], Muthineni Anusha[4], Gunda Manikanta[5]
[1] *Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering and Technology, Hyderabad, India*
[2]*Assistant Professor, Department of CSE-Cybersecurity, CMR College of Engineering and Technology, Hyderabad, India*
[3, 4, 5] *Student, Department of CSE (Cyber Security), CMR College of Engineering and Technology, Hyderabad, India*

Abstract: Evidence may be stored and accessed in a safe, unhackable manner with the help of a blockchain-based evidence protection system, guaranteeing the evidence's integrity and authenticity. It can stop illegal access and tampering while facilitating effective and trustworthy access to evidence. In order to handle numerous users and substantial amounts of evidence, the system can be both scalable and reasonably priced. It can also satisfy legal and regulatory standards for the preservation and protection of evidence, offering a safe and impenetrable record of evidence. When evidentiary integrity is critical, such a system can be helpful in court cases, criminal investigations, and insurance claims. All things considered, the mechanism for protecting evidence can guarantee that justice is done and that the integrity of the evidence is preserved.

I. INTRODUCTION

The protection and preservation of evidence hold immense significance in various domains, including law enforcement, legal proceedings, and forensic investigations. The integrity and authenticity of evidence play a pivotal role in establishing trust, upholding justice, and making informed decisions. However, traditional methods of evidence storage and management often encounter challenges such as data tampering, loss, or unauthorized access. These limitations necessitate the exploration of innovative technologies capable of providing robust solutions. Blockchain technology has attracted attention in years especially in relation, to digital currencies like Bitcoin. Its essential characteristics—transparency, immutability, and decentralization—make blockchain well suited for improving evidence management systems. A system with distributed ledger and blockchain technology for evidence protection can provide increased security, dependability, and transparency. In essence, blockchain is a ledger that records every transaction that occurs between network nodes. Each transaction is securely time stamped and added to the existing chain of transactions forming a record of all actions. Because of the blockchain's inherent immutability, data saved there is guaranteed to stay unaltered and impenetrable.

The distributed nature of blockchain allows for transparency. Because every member of the network has a copy of the complete blockchain, all recorded transactions are visible and transparent.

This function does away with the requirement for a central authority, lowers the possibility of fraud or manipulation, and improves confidence amongst interested parties.

Regarding the safeguarding of evidence, blockchain technology presents numerous significant benefits. First off, evidence's validity and integrity are guaranteed by the immutability of blockchain technology. Evidence becomes unchangeable and impervious to tampering once it is deposited on the blockchain. This feature offers a strong method for maintaining the integrity of tangible or digital evidence over the course of its existence.

Evidence protection and preservation are extremely important in a number of areas, such as law enforcement, court cases, and forensic investigations. Establishing credibility, maintaining justice, and arriving at well-informed conclusions all depend heavily on the validity and integrity of the evidence. However, issues like data loss, manipulation, or illegal access frequently arise when using conventional techniques for managing and storing evidence. These constraints make it necessary to investigate cutting-edge technology that can offer reliable solutions.

II. LITERATURE REVIEW

1) Ahmed et al. (2019) conducted a study on blockchain-based evidence management systems in the legal domain.

The research highlighted the advantages of blockchain technology in ensuring the immutability, transparency, and verifiability of evidence. the authenticity, security, and confidentiality of crucial digital evidence.

2) *In the field of forensic investigations, Kang et al. (2020) conducted research on the use of blockchain technology for preserving digital evidence integrity.*

The study demonstrated that blockchain could provide a secure and tamper-proof environment for storing and managing digital evidence.

3) *Furthermore, Ma et al. (2018) focused on the application of blockchain in ensuring the integrity of medical evidence.*

The research explored the use of blockchain technology to securely store and manage medical records, lab reports, and other forms of medical evidence.

III. OBJECTIVE

The main goal of this research project is to progress the creation of a cutting-edge Digital Evidence Protection System (DEPS) that tackles important issues related to the integrity, security, and preservation of digital evidence in modern legal, investigative, and regulatory settings. The goal of the project is to improve the integrity of digital evidence by developing advanced procedures that can identify and stop unlawful changes made to the evidence at any point in its lifetime.

This entails looking into cutting-edge techniques and technologies to strengthen the dependability and quality of digital data against changing threats. The objective is to reduce the risks of illegal access, data breaches, and cyberattacks by investigating encryption techniques, access management models, and cybersecurity best practices. This will protect confidential digital evidence and preserve sensitive information.

Lastly, the research aims to ensure compliance with legal and regulatory standards, focusing on protocols that guarantee the admissibility of digital evidence in legal proceedings. By aligning with established legal requirements, the Digital Evidence Protection System intends to provide irrefutable proof of the authenticity and integrity of digital evidence, facilitating its acceptance in a court of law.

IV. SYSTEM REQUIREMENTS

A. *Hardware Requirements*

1) *Processor:* DUAL CORE 2 DUOS and aboveRAM: 2GB
2) *Hard Disk:* 250GB

B. *Software Requirements*

- OPERATING SYSTEM: WINDOWS 10, MACOS, LINUX
- PLATFORM: Any Web-Browser
- FRONT END: REACT, STYLED-COMPONENTS.
- BACK END: NODE JS, EXPRESS JS, SOLIDITY, IPFS, MONGODB. TOOLS: GANACHE, METAMASK.

a) *React:* React stands out as an used JavaScript framework, for crafting user interfaces. Originating from Facebook and launched in 2013 React empowers developers to craft responsive web applications by handling the applications status and displaying components in response to alterations in that status. Below are some attributes and qualities of React that position it as a favored option, among developers.

b) *Component-Based Architecture:* React utilizes a component based structure dividing the user interface of an application, into components that can be reused independently. Each component contains its logic, state and rendering simplifying the codebases organization and upkeep.

c) *Virtual DOM:* React uses something called the Virtual DOM, which's, like a version of the real Document Object Model (DOM). This Virtual DOM helps React to update and display the parts that have actually changed making it faster and improving how users interact with it.

d) *JSX:* React introduces JSX, an extension of syntax that enables developers to write code resembling HTML, within JavaScript. JSX streamlines the creation and control of the user interface offering a descriptive method, for constructing UI components.

e) *Unidirectional Data Flow:* In React data moves, in one direction from parent components, to child components. This straightforward flow simplifies how we grasp and troubleshoot the applications status since we can easily predict and track data changes.

f) *Component Reusability:* React emphasizes the idea of reusability enabling developers to design components that can be conveniently utilized in sections of the application. This methodical strategy enhances the manageability of code and shortens the time required for development.

g) *Efficient Updates:* React utilizes a reconciliation algorithm that effectively updates the DOM by identifying the necessary changes to mirror the updated state of the application. This leads to rendering and enhanced performance.

h) *Rich Ecosystem:* React boasts an array of libraries, tools and a strong community backing, which simplifies the process for developers to discover answers, extensions and proven methods. Within this network are resources such, as React Router for navigation Redux, for handling state management and numerous others.

i) *Cross-Platform Development:* React is versatile as it can be utilized to create web apps as mobile apps, for both iOS and Android systems using tools, like React Native. This enables developers to reuse code and accelerate development across platforms.

1) *NODEJS*

Node.js, a server side platform using Google Chromes JavaScript Engine (V8 Engine) was created by Ryan Dahl in 2009. Its recent release is v0.10.36 offering a source, versatile runtime environment, for building server side and networking applications across different platforms. Nodejs applications are written in JavaScript, and can be run within the Nodejs runtime on 05 X, Microsoft Windows, and Linux. Nodejs also provides a rich library of various JavaScript module which simplifies the development of web applications using Nodejs to a great extent Nodejs Runtime Environment + JavaScript Library Following are some of the important features that make Node is the first choice of software architects.

- Asynchronous and Event Driven: Node.js librarys APIs operate asynchronously meaning they do not block operations. This allows a Node.js server to proceed to the API call without waiting for data retrieval. The server relies on Node.js Events for notifications and responses, from API calls.
- Node.js library is known for its code execution thanks, to its foundation, on the Google Chrome V8 JavaScript Engine.
- Single Threaded but Highly Scalable:Node.js follows a model with a thread that utilizes event looping. The event mechanism enables the server to respond without blocking leading to scalability compared to servers that rely on limited threads, for request handling.
- Node.js uses a threaded approach, which enables it to effectively manage a volume of requests when compared to servers, like the Apache HTTP Server.
- Node.js applications do not buffer data; instead they output data in chunks without any buffering.

2) *EXPRESS JS*

Express is a Node.js web application framework that offers a range of features, for creating web and mobile apps. It speeds up the development process for Node.js web applications by allowing the setup of middleware to handle HTTP requests defining routes, for actions based on HTTP methods and URLs and enabling rendering of HTML pages by passing arguments to templates.

3) *MongoDB*

MongoDB, a source NoSQL database management system offers an alternative, to relational databases. NoSQL databases are particularly beneficial for handling distributed datasets. MongoDB allows for the management of document oriented data. Supports data formats. It is part of the array of database technologies that emerged in the mid 2000s within the NoSQL realm typically used in data applications and tasks involving data that does not neatly fit into a structured relational model. Unlike databases that utilize tables and rows MongoDB organizes data into collections and documents. Organizations appreciate MongoDB for its flexibility, in ad queries, indexing capabilities load balancing features, aggregation functions and server side JavaScript execution.

4) *SOLIDITY*

Solidity is a contract-oriented programming language specifically designed for developing smart contracts on blockchain platforms, with Ethereum being the most prominent example. It is a statically typed language that ensures type safety during compilation, helping to prevent common programming errors and improving code reliability. The contract-oriented nature of Solidity is one of its primary characteristics. With the conditions of the agreement directly encoded into the code, smart contracts are self-executing contracts that developers can build and implement. Without the need for middlemen, smart contracts allow for the definition of the logic and rules governing interactions inside a decentralized network, fostering transparency and trust.

Because of Solidity's tight integration with the Ethereum blockchain, developers may implement smart contracts in a reliable and safe environment. The Ethereum Virtual Machine (EVM), the runtime environment used to carry out smart contracts Ethereum network, is completely compatible with it.

A multitude of capabilities are provided by the language to make the building of smart contracts easier. Because it enables intricate data types like maps, structs, and arrays, developers are able to create and modify data structures as needed. Additionally, Solidity offers robust support for event-driven programming, which enables contracts to generate and manage events and improves communication between various decentralized application components.

5) IPFS

The Interplanetary File System, or IPFS for short, is a decentralized and distributed protocol that allows content addressing and peer-to-peer file sharing. With the creation of a distributed, permanent web where data are saved and retrieved according to their content rather than their location, IPFS aims to overcome the shortcomings of conventional online protocols. It attempts to build an internet infrastructure that is more efficient, censorship-resistant, and resilient.

- Content addressing is one of IPFS's main characteristics. IPFS employs content-based addressing, in which files are identified by their cryptographic hash, as opposed to location or IP address. This ensures integrity and avoids duplication by enabling distinct file identification depending on content. To store and distribute files, IPFS makes use of a dispersed network of nodes. A file is divided into smaller pieces and dispersed among several network nodes when it is added to IPFS. Nodes can request individual chunks from other nodes in order to retrieve them and confirm the file's integrity. Each chunk is given a unique hash.
- Versioning and deduplication support are two more significant features of IPFS. Multiple instances of the same file are automatically deduplicated, saving storage space and bandwidth costs because files are identifiable by their content. IPFS also makes file versioning possible, making it simple to retrieve several versions of the same file. Peer-to-peer file sharing, which allows network nodes to directly exchange files without depending on a central server, is another feature that IPFS enables. This makes it possible to provide content more quickly and effectively, particularly for widely dispersed files that can be cached by several nodes.

V. PROBLEM DEFINITION

In todays age the growing dependence, on data for legal, investigative and regulatory purposes presents a significant challenge; protecting the integrity of digital evidence. With the vast increase, in evidence comes a risk of unauthorized access, manipulation and compromise posing threats to its reliability.

The lack of a Digital Evidence Protection System (DEPS) intensifies these issues highlighting the need to enhance the genuineness, safety and secrecy of vital digital evidence.

The main issue here is that digital evidence can easily be altered, which undermines the reliability and trustworthiness of the information. With the increasing amount of evidence being generated it is crucial to have a system, in place to guarantee the accuracy of this evidence at every stage.

More over the risks related to storing and sending evidence call, for enhanced data security measures to stop access avoid data breaches and protect sensitive information from cyber dangers.

VI. EXISTING SYSTEM

A. Chain of Custody

Documenting and maintaining a clear record of who accessed the evidence, when, and for what purpose. This ensures the integrity of the evidence and its admissibility in court. It is the duty of the police officials to maintain an unbroken chain of custody for the successful trial of a case. Keeping the evidence collected safe in sealed bags with unique identification numbers. The Digital Evidence Protection System (DEPS) employs a Chain of Custody approach to ensure the integrity and authenticity of digital evidence. At the moment of collecting, thorough documentation is first made, recording information such as the date, time, and identity of the collector.

Using cryptography, evidence is "sealed" symbolically, and safe packaging guards against manipulation while storage or transit. To preserve data integrity, transfers are recorded and safe techniques are applied. Digital evidence is protected in environments that use encryption and are secure for storage.

Analysis is conducted according to strict protocols, and any modifications are carefully recorded. The presentation of evidence in court proceedings maintains the Chain of Custody and offers a comprehensive record of handling. The return, preservation, or safe disposal of digital evidence is recorded during the disposition process. Throughout the lifecycle of digital evidence, dependability and admissibility are guaranteed by this methodical and recorded process.

B. Digital Signatures

By comparing the Digital Evidence Protection System (DEPS) to a digital signature, one can better understand how cryptographic methods are used to ensure the validity and integrity of digital evidence. Cryptographic hashes are used by the Digital Evidence Protection System (DEPS), which is comparable to a digital signature in that it allows for the integrity and unique identification of digital evidence. By using hashing techniques, DEPS creates fixed-size hash values that function similarly to a digital fingerprint and may identify changes in these hashes that indicate evidence tampering. Every digital piece of evidence is symbolically "signed" with a distinct digital signature, guaranteeing authenticity and offering corroborating evidence of its provenance. To ensure security and transparency, DEPS uses a public-private key pair, which is similar to the asymmetric cryptography used in digital signatures.
Digital evidence is sent securely thanks to encryption mechanisms, which guard against unwanted access and modification. For the purpose of authentication, the digital signature restricts access to the evidence to only those who are allowed. By offering indisputable proof of provenance and integrity—a critical component in legal contexts—DEPS guarantees non-repudiation. DEPS time-stamping procedures generate a safe and auditable timeline by recording when evidence is created or amended. DEPS essentially provides a strong cryptographic framework for protecting digital evidence in legal, investigative, and regulatory contexts when viewed through the lens of a digital signature.

C. Access Control

The Digital Evidence Protection System (DEPS) can be understood through the lens of access control, emphasizing the strategic regulation of digital evidence access to ensure its security, integrity, and confidentiality. The Digital Evidence Protection System (DEPS) employs access control measures to enhance the security and integrity of digital evidence. Robust user authentication, including multi-factor methods, verifies individual identities. Role-Based Access Control (RBAC) assigns specific permissions based on responsibilities, limiting access to authorized personnel. Encryption safeguards digital evidence confidentiality during storage, transmission, and processing. Detailed access logs track every interaction for audit trails and accountability. Access revocation and timebased controls enhance security by promptly removing unnecessary access and limiting exposure to specific timeframes. Granular permissions provide administrators precise control over user privileges. Secure storage practices, including access-restricted servers and encryption, ensure physical and digital safeguards. The Digital Evidence Protection System (DEPS) employs access control measures to enhance the security and integrity of digital evidence. Robust user authentication, including multi-factor methods, verifies individual identities. Role-Based Access Control (RBAC) assigns specific permissions based on responsibilities, limiting access to authorized personnel. Encryption safeguards digital evidence confidentiality during storage, transmission, and processing. Detailed access logs track every interaction for audit trails and accountability. Access revocation and timebased controls enhance security by promptly removing unnecessary access and limiting exposure to specific timeframes. Granular permissions provide administrators precise control over user privileges. Secure storage practices, including access-restricted servers and encryption, ensure physical and digital safeguards.
Physical and digital protections are ensured via secure storage procedures, such as encryption and access-restricted servers. By blocking unwanted access attempts, intrusion detection systems improve general security. Admissibility of the evidence is ensured by compliance measures that match DEPS with legal and regulatory requirements. To summarize, DEPS's approach to access control places a high priority on controlled access while maintaining the integrity and evidentiary value of digital evidence in compliance with legal mandates.

VII. LIMITATIONS OF THE EXISTING SYSTEM

The paper's limitations include specific restrictions or variables that could have affected the study's findings.

Among them are:

1) *Complexity and Technological Advancements:* The rapid pace of technological advancements poses a challenge for Digital Evidence Protection Systems (DEPS), as new methods of data manipulation and unauthorized access may outpace the development of protective measures. The increasing complexity of digital systems also introduces vulnerabilities that may be difficult to anticipate and address comprehensively.
2) *Human Factor and Insider Threats:* Despite advanced technological safeguards, human factors remain a significant limitation. Insider threats, whether intentional or unintentional, can compromise the security of digital evidence. Human error, lack of awareness, or malicious intent from individuals with authorized access can undermine the effectiveness of protection measures.

A. Architecture

1) On the website, the user will be able to register first, and after registering, it should be approved by admin. After that, the user can login, see all the existing
2) cases, and create a new case.
3) Investigators need to fill out all the details and upload the evidence one after the other. The evidence is stored in ipfs, and the ipfs returns a hash.
4) The hash returned by the IPFS, along with the case details, are stored in the local Ganache blockchain network and used for retrieval later.
5) The Smart contracts are first written and compiled with Truffle, which creates a contract call on the blockchain.
6) The MetaMask is used as a wallet to make transactions and add block details to the blockchain.

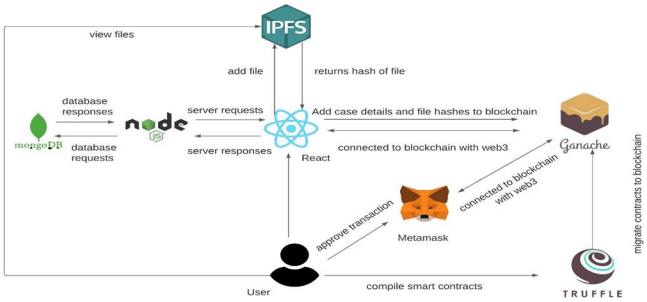


Fig 4. Architecture

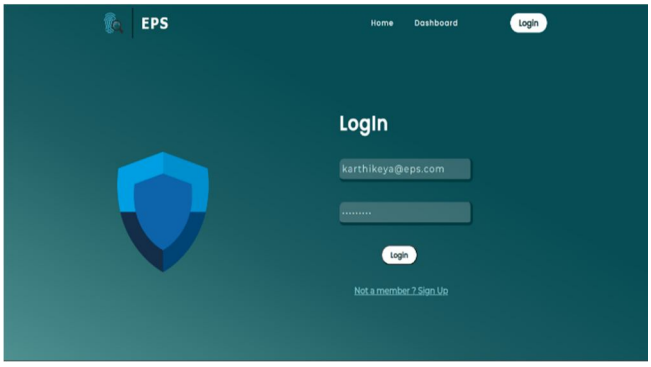
VIII. CONCLUSION

In conclusion, the application of blockchain technology in evidence protection systems offers promising solutions to the challenges faced by existing methods. By leveraging blockchain's inherent features such as immutability, transparency, and cryptographic integrity, the integrity and authenticity of digital evidence can be ensured.

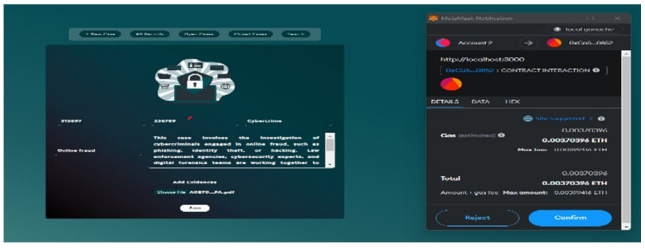
VIII. RESULTS AND DISCUSSION

The implementation of a blockchain-based system can also provide secure access and sharing capabilities while meeting legal requirements and maintaining compliance with chain of custody regulations and data privacy laws.

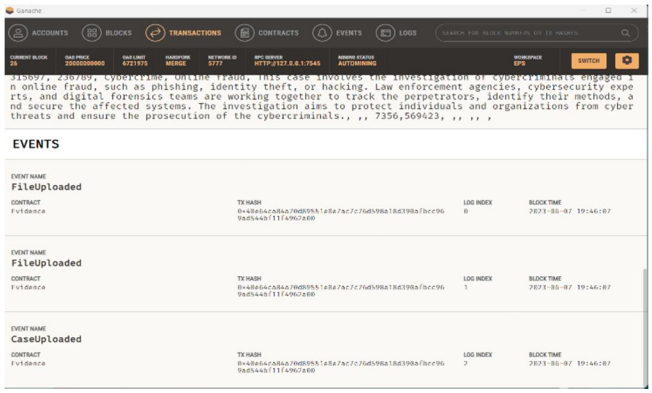
A. Login Page



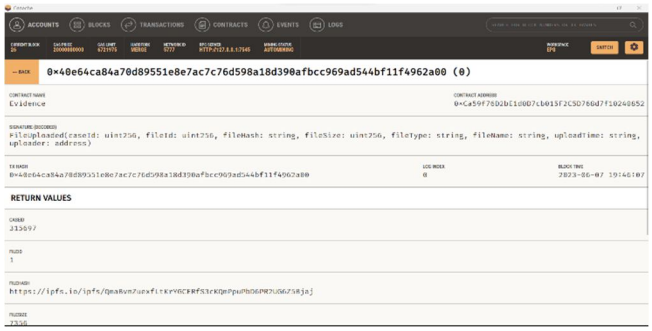
B. New Case Page



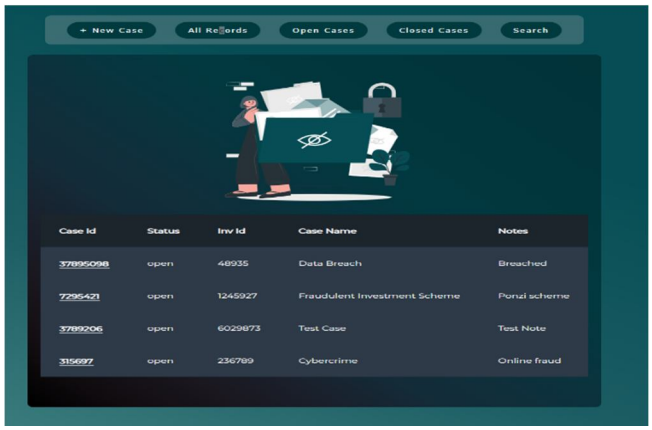
C. Ganache Events



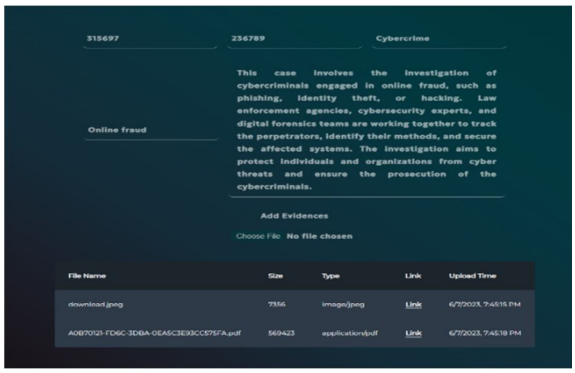
D. Ganache Storage



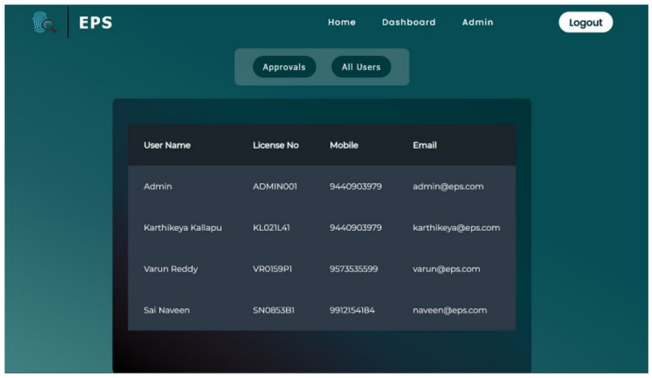
E. Records



F. Case Details

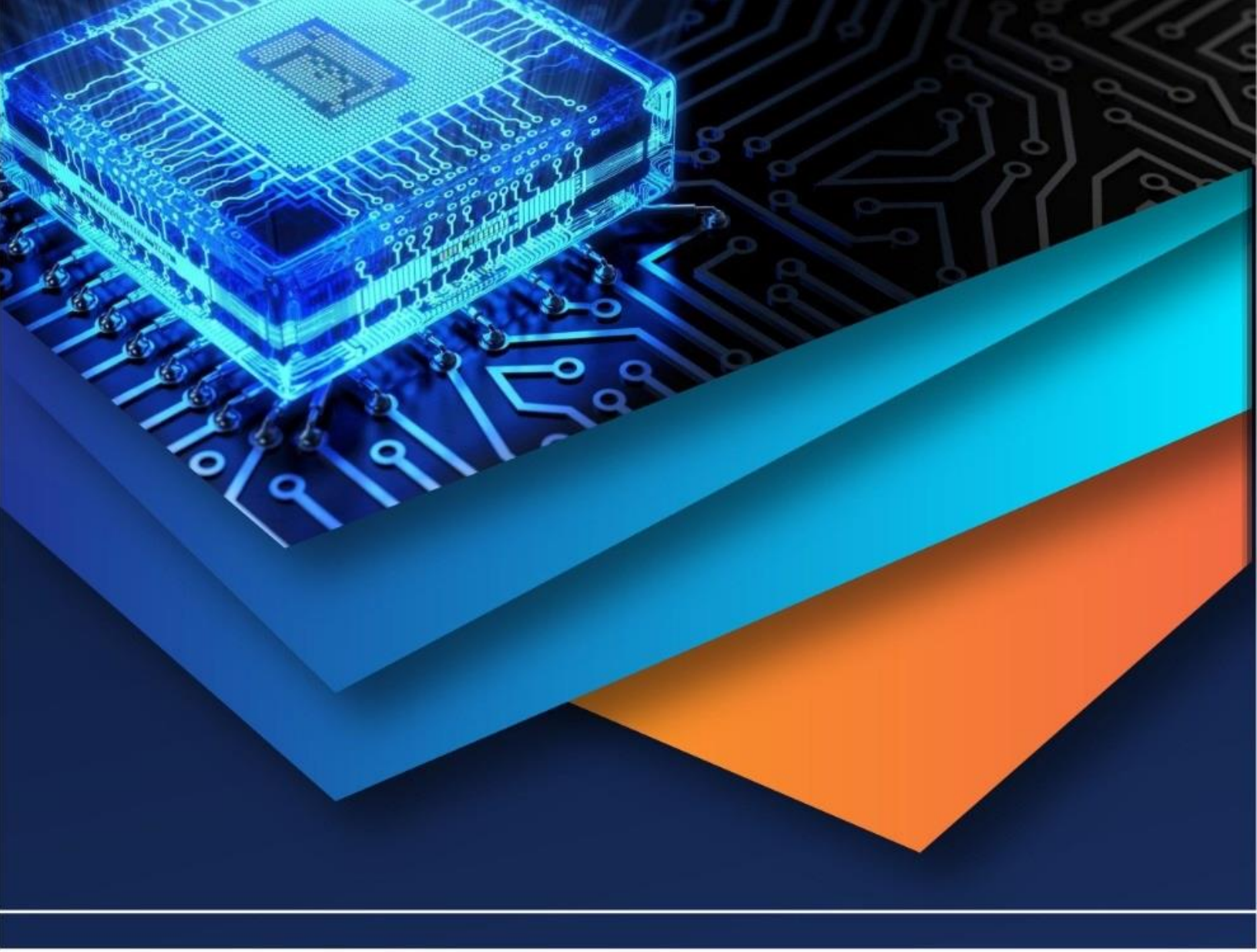


G. Admin Page



REFERENCES

[1] Chen, Y., Qian, H., & Mao, Z. M. (2018). Network Security. Springer.
[2] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. PenguinChen, T., & Abu-Amara, H. (2007). Network Security Technologies and Solutions. Cisco Press.
[3] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
[4] Buterin, V. (2013). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. Retrieved from https://ethereum.org/whitepaper/
[5] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
[6] Harkins, D. & Carrel, D. (2007). Wireless Network Security: A Beginner's Guide. McGraw-Hill Education.
[7] Ferguson, P., Peralta, R., & Ross, G. (2007). Network Security Essentials: Applications and Standards. Pearson.
[8] Northcutt, S., Novak, J. I., & winters, S. (2002). Network Intrusion Detection: An Analyst's Handbook. New Riders.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY