IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 7 ISSUE : 03 Print / Issue Publication Date: 29-Aug-2022

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2022.v07i03.035

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 222-228
Published Online July 2022 in IJEAST (http://www.ijeast.com)

ENIGMA - A SECURE FORENSIC DATA SHARING USING BLOCKCHAIN

Karthik, Trishar T Suvarna, Karthik Shetty, U Ashvitha
Department of Computer Science and Engineering, Sahyadri College of Engineering & Management, Adyar, Mangaluru (575007), Karnataka, India

***Abstract* -A forensic laboratory is often referred to as a crime lab. The forensic laboratory examines evidence such as DNA, fingerprints, used bullet casings, and even tyre tracks to establish if a crime has been committed and who the offender is. For example, everything collected during the examination of victims of sexual assault such as body fluids, hairs, fibers, or anything found on the victim's clothing may be analyzed at a forensic laboratory. The type of analysis will depend on the type of evidence being analyzed. Evidence is the most important part of the investigation to proceed. In some of the cases, we can see that pieces of evidence are being altered or modified, or changed even before it reaches the judiciary system. Because of this, justice won't be served to the needy and eventually, the crime rate will increase. The project's goal is to create a blockchain network that takes the forensic report as input from the pathology lab and that tamper-proof forensic report will be sent to the police station securely.**

***Key Words*: Blockchain, Decentralized Application, Smart Contract, Ethereum, Forensics.**

I. INTRODUCTION

An essential part of the criminal justice system is played by forensic science. In order to establish facts that can aid in the investigation and conviction of criminals or the exoneration of innocent individuals, forensic scientists assess, analyse, and scrutinise evidence from crime scenes and other places. The most often used forensic science research lab specialisations are forensic genetic biology (DNA), trace proof examination, forensic biochemistry, firearms, latent fingerprint investigation and handwriting analyses, tool marks study, fire and explosives research, forensic toxicology, and digital evidence. In addition to forensic laboratories, additional intelligence disciplines include forensic pathology, forensic nursing, forensic psychology, forensic entomology, and forensic engineering. Practitioners of these professions could be found at medical examiners and coroners offices, institutes, or private clinics. Intelligence scientists collect, maintain, and analyse scientific evidence during the investigation. While some intelligence scientists were visiting the crime scene to gather evidence on their own, others were taking on a laboratory role, analysing the material presented to them by other people. However, some have participated in the analysis of financial, banking, or other numbers that will be used to investigate financial crime, and maybe employed as consultants for private companies, academics, or government employees. With the fast rise in cybercrime in today's digital environment, digital evidence is becoming increasingly important for the provenance of person-to-person cybercrime links. The chain of custody for digital evidence has its own set of issues. Block chain technology is a distributed system that uses ledger based transactions, which could store linked records within the range of a decentralized database within the P2P network. The advantage of using block chain in digital forensics is to ensure secure and reliable sharing of data between the sender and the receiver [1]. When a crime is committed, the corpse is sent to the forensic lab where they analyse the body and generate the report of the evidence. Evidence gathered at a crime scene is crucial in solving the case and bringing the persons involved to justice. It is extremely difficult to guide a case in the proper path without proof. As a result, safeguarding this evidence from any type of tampering is critical. Maintaining the integrity of evidence requires proper handling and packing. Enigma is a secure forensic data sharing application in which the pieces of evidence are securely transferred from the forensic lab to the police station. In [15] the paper focuses on implementing deep learning technology based on different methodologies to classify different malware families. In [16] the paper highlights the role and importance of image processing in the service industry and how location-based image querier would be used for extracting important values to improve services. In [17]the paper discusses the role of video in painting in detecting missing frames of unvarying images in the field of video analytics.

A. Problem Statement

It is observed that forensic reports are changed most of the times during the investigation process. Unrecognized sources may change data of forensic reports. In most of the cases, due to this the judgment may not be fair and justice may not be provided to the needy. This is due to the lack of security in the existing systems. The existing forensic data sharing system includes sharing data via emails, third party websites, physical forms, etc which leads to issues like lack

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 222-228
Published Online July 2022 in IJEAST (http://www.ijeast.com)

of data security, allowing unknown websites to access confidential data, modification of data content, and viruses of infecting shared files, etc. Hence, this problem faced by the people brings to rise the need of implementing a system that ensures the complete security of forensic report/data, all the way starting from their generation until the time they used finally for the purpose of serving justice to the needful. Our aim is to develop a data sharing system that is used to send the forensic report from the pathology lab to the police station using Blockchain Technology.

B. System Overview

The system is conceptualized, designed and proposed by us in a manner which mainly aims towards increasing the overall security of confidential or forensic data sharing while maintaining the authenticity as well as integrity of the system. The system designed by us will take the forensic report as an input initially from the pathology lab which will be further processed to the doctor. After a brief and thorough examination of the document by the doctor, the status of the report will be marked as verified by the doctor if the report is found to be authentic. Further, the tamper-proof verified report can be viewed by the police station for further examination.

C. Blockchain in Forensics

One of the primary benefits of storing data in a digital form is its versatility. Authorized individuals can quickly have access to it. Without inflicting any harm to the actual document, several copies can be made and saved. It is readily available from every location on the planet. It is possible to transfer many documents at once. It enhances efficiency since searching for information preserved in digital medium takes only a few seconds compared to searching for traditional papers, which takes much longer. Evidence documentation can be damaged by natural or man-made calamities. As a result, including blockchain technology into the field of Forensic Science will reduce the chances of these papers being corrupted. This technology will also eradicate human error. It is vital to incorporate such technologies into forensic evidence management systems as the world moves toward digitalization.

1.) Private Blockchain:

A private blockchain is a permissioned blockchain since it is run by a network administrator and only approved users can connect to the network. The network is controlled by one or more organizations, which makes it necessary to conduct transactions via third parties. Only the parties involved in the transaction will know about it in this sort of blockchain; others won't be able to access it, making the transaction private.

2.) Public Blockchain:

Public blockchains, sometimes referred to as permissionless blockchains, are totally open and strictly adhere to the decentralisation principle. Public blockchains include ones like Bitcoin and Ethereum. Anybody with access to the network can contribute blocks to the chain. In contrast to private blockchains, where the identities of the parties to a transaction are kept secret, public blockchains are likewise mostly anonymous.

D. Smart Contracts in Blockchain

Smart contract is the agreement involving two parties that are maintained in computer code. It does not necessitate the involvement of a third party. Smart contracts function similarly to traditional contracts in which specific code can be inserted immediately and the parties concerned can check the respective code before the deadline. Smart contracts include certain terms and circumstances that must be adhered to. Adhering to agreements, defining regulations and executing the business logic, relying on blockchain technology for encryption to help protect and authenticate all messages it contains, processing, and lastly updating the blockchain network are all part of a smart contract's anatomy. It is stored in a database because it works with blockchain and is irreversible. A smart contract's transactions must be handled primarily by blockchain technology, which eliminates the need for a third party and, as a result, saves time.

II. LITERATURE SURVEY

Revathy Sathyaprakasan et al [1].Management of evidences plays an important role when it comes to forensic science.. In forensic investigations, the most pressing issues are evidence management and documentation. It is very important to retain the authenticity and integrity of the evidence right from the time it is collected until it is finally decided by a court of law. The documenting of the confidential proofs being handled during the inquiry in chronological sequence is known as Chain of Custody (CoC). We can obtain flexibility in storing records in digital form with the help of blockchain. Authorized individuals can simply gain access to it. Without inflicting any modifications to the actual document, multiple copies can be made and saved. It is easily accessible from anywhere on the planet. Implementation of a Hyper-Ledger Fabric architecture to ensure the participating nodes' integrity and authorisation. When it comes to data encryption and decryption, symmetric key cryptography uses only one key. Although it is quicker and safer, the information can be easily altered once it reaches the hands of the invader.

Sonali M Patil et al [2]. Blockchain technology is a decentralized technology which employs ledger-based transactions to keep connected records within the range of a P2P network's decentralised database. The benefit of adopting a blockchain system in digital forensics is that the

administrator can give validation before accessing digital evidences, which uses hash functions to create a verifiable evidence chain. The blockchain employs encryption to ensure the immutability, visibility, and public trust of the case investigation. The management of evidences is one of the most important concerns in digital forensics. Evidences may be viewed by various parties involved from the time they are acquired until they are exploited in a legal court.

Sonali Patil et al [3]. Blockchain is a distributed ledger in which all thedata is organized into units called blocks. Aninnumerableamount of signed transactions are contained in each block of the ledger. Blockchain refers to the use of cryptographic technologies to link the blocks together. The new blocks are appended using a methodical cryptographic process. This will ensure that the information saved in the blockchain is reliable. When there are numerous partners participating, this also assures the information's integrity. One of the benefits of blockchain is that it eliminates intermediaries, lowering transaction costs and reducing fraud with a central authority. This speeds up company processes and allows for peer-to-peer sharing. Many use cases involving enterprises for which provenance is important benefit from distributed ledger technology.

Ruhi Tas et al [4]. The first implementation of blockchain technology was lash coins. Blockchain applications are currently being used in all domains following the implementation of smart contracts. Ethereum has recently surpassed Bitcoin as the most widely used blockchain platform. Smart contracts and Ethereum D Apps are utilised in tandem. Ethereum is a decentralised application platform that aspires to develop an alternative protocol. It is claimed to have the advantages of short code creation time as well as security measures. The use of D App resulted in a considerable amount of data being generated. Developing a Blockchain-based application comes with its own set of obstacles. On the internet, there are many alternative development environment options. Modern web applications are based on a framework that eliminates the natural occurrence of a solitary failure point.

Emmanuel Nyaletey et al [5]. IPFS (Interplanetary File System) is a distributed P2P file storage system that intends to link all computer machines to a single file system. Users may efficiently move files and information over the network thanks to the distributed network, which leverages Git and BitTorrent to achieve high throughput. The IPFS network is built to interact with a number of protocols and is suitable for sharing large data which relies on high bandwidth to perform uploading and or downloading across the Internet. Blockchain is a logical match for enabling file tracing schema in a DFS like IPFS since it is a distributed data management platform eternality.

Morteza Alizadeh el at [6]. Blockchain is basically a distributed ledger technology that provides a high level of transaction security. It gives distributed applications a secure and immutable environment in which to handle and store data.The blockchain holds an encrypted sign of data or data records.. Decentralisation refers to the method of moving functions, applications, people, objects or power far with respect to central point or source. A decentralised system is one that is not governed, managed, or run by only one person or organisation. Some of the key application areas are home automation, office automation, environmental control, transportation, healthcare, education, safety and entertainment.

Sabrina Kirrane et al [7]. There are a variety of blockchain platform options available. Bitcoin1 is generally considered for transactions related to finance, Coins like Permacoin-2 and Filecoin-3 allow untrustworthy entities to reserve data of their peers whilst at the same time technologies like Ethereum-4, Hyper ledger Fabric-5 can successfully provide the capability to include storage of data (state) along with the execution of code, generally alluded to as smart contracts or chain code. Although blockchain executable code platforms can support use cases in a wide range of fields, the viability of blockchain platforms for the definition of data and service restrictions needed to realize such use cases is still under investigation.

Dr.S. Velliangiri et al [8]. The blockchain is a system that aggregates all cryptographic transactions into a decentralised, digitized, and public ledger which basically is open. These transactions are maintained in a consecutive order, allowing members to keep track of computerised transactions without having to retain a central record. One of the blockchain's main features is its distributed database. This type of database resides in multiple copies across various PC frameworks, forming a dispersed system, indicating that there is no one, concentrated database or server. Decentralized and Scalability, Transparency, Identity and Access, Open Source, Autonomy, Immutability, Anonymity, and Consensus Model are all properties of Blockchain Technology. The data present in the blockchain depends on two factors namely user and the network.

Siddharth Rajput et al [9]. Bitcoin is a fantastic example of Blockchain application. Blockchain is thought to be a one-of-a-kind wonder in the field of enlisting sanctionative unfathomable applications, such as protecting and verifying definitive reports, deeds and different validations, medicinal administrations data, IoT, Cloud, and so on. Any advanced resource exchange listed on the internet can benefit from the Blockchain innovation. Because of the secure third-party UN agency approach and intervention in any electronic exchange, the internet business is fully reliant on fund foundations filling out forms.

Pinyaphat Tasatanattakool et al [10]. Blockchain is a non-centralized, dependable, and impossible to utilise for fraudulent purposes method of database storage. Bitcoin, on the other hand, is a sort of digital money that uses the Blockchain public ledger to conduct transactions across peer-to-peer networks. Smart contracts and hyper ledgers are two additional financial applications that use Blockchain technology. As a result, blockchain technology can be applied to a wide range of applications. This paper addressed the meaning of various technical terminology, such as Decentralized, Transparent, Miner, Consensus, Forks, Hash, Node, Timestamp, and others, in the context of business systems that support only registered members.

Shangping Wang et al [11]. If users wish to share confidential data on a third-party cloud server, they will need a way to control access to data that can only be read and removed to encrypt a single user to common cloud storage solutions. In response to this desire, an encryption method which is based on attributes (ABE) was presented and implemented immediately. This approach allows the owner of data to implement a policy related to data access depending on user identification and features in order to achieve better characterized data access control. For configuration of the system and distribution of private keys to users, almost every ABE encryption scheme relies on using a private key generator (PKG).

Mohamed Fartitchou and colleagues [12]. Due to various qualities like as decentralisation, immutability and peer-to-peer (P2P) transactions, Blockchain (BC)technology has established itself as one of the most promising techniques that will transform the world. It offers a practical and well-thought-out solution to a number of real-world issues. The BC-based crypto currency and accompanying apps are referred to as 1.0.. BC 2.0 refers to all financial applications made possible by the combination of smart contracts (SCs) and digital currency. BC 3.0 applications are other BC technology applications that offer a larger variety of non-crypto currency-related applications i.e distributed ledger.

Wei-Chiao Huang, et al [13]. Blockchain technology is a distributed ledger that is immutable and has a more complex fault tolerance rate. Blockchain transactions employ an add-only file system which implies that no changes or deletions are permitted. This basically leads to bloating problem of storage in public chains, resulting in synchronisation performance delays. The peer-to-peer network system is now widely regarded as the standard way for distributing data for a wide range of applications. Users will be able to pool their computing resources, data, and bandwidth. Unlike a centralised network, the P2P architecture regards every computer as an independent block. This implies that each block functions as both a client as well as a file server.

Bhavani Thuraisingham et al [14]. Blockchain technologies, in essence, create a environment for the safe flow of information that belongs to all transactions, including Contracts and financial transactions. A blockchain is made up of a series of various blocks which are connected together through chains. A block is nothing but a file which includes transaction-related data. Publishing of blocks can be permission based or permissionless, according to the NIST paper, which implies that a block can be published by anyone without or with permissions, which means that blocks can only be published by the consent of a centralised or decentralised authority. Cryptographic hash functions are an important part of blockchain.

Harisha Airbail et al [15]. The two parties namely governments and dark hat programmers use malware today to steal personal, financial, or corporate information. In this research, a system for classifying malware using advanced learning techniques is presented. Malware duplicates are conceptualised as grayscale images, with the observation that for some malware families, the images sharing a location with a similar family are nearly identical in surface and layout. The proposed approach for obtaining common visual attributes. On a malware knowledge set containing 9,339 models and 25 distinct malware families, the exploratory results show that 97.45 percent of the plan grouping is malware.

Suhas Kandiga et al [16]. The amount of information being created today is increasing, and information mining and image processing may be combined in a variety of ways to provide a unique solution for each unique problem in the support industry that involves image processing. The kind of administration provided to the consumer is greatly influenced by the pictures created on the internet; various photos have distinct characteristics that choose different behaviour variables for different customers who use picture-based information.

Vijetha Shetty et al [17]. The quantity of videos being captured is growing steadily these days because to the rapid expansion of mixed media in line and technological developments in computerised video. Since the majority of the video that was created is much larger than what the administrators can view, finding any interesting articles or events has become a very time-consuming task. This assignment may be possible for a few recordings, but this tedious task is difficult when there are many videos. For sorting and browsing such a large amount of videos, a video outline is a handy tool. By include essential activities, a video outline may be used to create a condensed representation of a unique film. In this study, a formula for creating video rundown using video inpainting is proposed.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 222-228
Published Online July 2022 in IJEAST (http://www.ijeast.com)

Harisha Airbail et al [18]. For a significant time, connection verification using face images has been recognised to stand out. The vast majority of applications are now able to employ connection connections thanks to the ability to distinguish between basic instances that are present in photographs and examine the link concealed between them. This work serves as a focus on the extent to which genetic markers can influence the families created via heredity in determining whether or not their connection succeeds as planned. The approach involves using the Siamese Network, which consists of two indistinguishable convolutional brain networks that share normal weight values, to identify the link between the given facial images.

Ahmed Afif Monrat et al [19]. The backbone behind several computerised digital currencies is called blockchain. Numerous research efforts revolve on the opportunities that blockchain presents in various application areas. This study includes a close assessment of the blockchain trade-offs' and further clarifies its scientific classification and design. It also compares alternative agreement instruments and discusses challenges including flexibility, security, interoperability, energy use, and administrative concerns. Additionally, this article also considers the future potential of blockchain technology.

Tien Tuan Anh Dinh et al [20]. In this paper, the cutting edge is initially reviewed, focusing on private blockchains (in which gatherings are verified). This study examines four areas: shared records, cryptography, agreement convention, and brilliant agreement, which together make up both ongoing and research frameworks. The next section of this paper introduces BLOCKBENCH, a benchmarking framework for analysing how private blockchains perform when compared to information processing tasks. In light of BLOCKBENCH, this paper focuses a detailed evaluation of three important blockchain frameworks, namely Ethereum, Parity, and Hyper ledger Texture.

III.PROPOSED TECHNIQUE

A fresh and unique way is offered by blockchain technology as to how forensic applications can be employed, with various benefits for the procedure of investigations, such as data gathering, enhancement, validation, data analysis, evidence preservation, and presentation of the findings.
By providing high level integrity, transparency, ensured authenticity, security, and the capacity to audit digital evidences to reach the desired objective, a block chain based digital forensics investigation system has significant potential to bring huge benefits to forensic applications. [2]

Our system can be mainly grouped into 3 nodes: -
1. Pathology Lab: The victim's forensic report will becreated by a pathology lab and shared with respective doctor assigned for the same. Reports usually are supplied in the form of e-mail or hard copies in the current system, and they could be effortlessly changed when accessed by many sources including doctor.. However, under the suggested approach, we would upload a forensic report on the immutable and distributed block chain network. Block chain is a highly secure network that cannot be hacked or interfered with in any way. Furthermore, because data is kept in a distributed fashion, we can simply retrieve data if a node fails.
2.Doctor:It is the proposed system's second node. The pathology lab sends the doctor the forensic report. The doctor then thoroughly reviews the report and marks it as validated, after which the verified documents are shared with the respective police department for additional inquiry. Doctors are unable to change the received report uploaded to the server by the officials of pathology lab department due to the generation of a 16-digit hash code which is a static value. The hash code changes whenever someone tries to edit the report. Due to the fact that the value of hash value stays fixed throughout the whole process, we can determine which node it was modified through and thus identify the offender. The report can be saved in the Doctor node's ledger.
3. Police Station:It is the proposed system's third and final node. The doctor's output will be received by the police department in the form of a digitally signed forensic report. Following that, the police officer will begin his investigation based on the forensic report. As a result of the pathology lab's report, which has been successfully checked by the assigned doctor, the police department now has access to the deceased's details, that have in advance been examined and verified. As a result, the police officer's job gets easier because he only has to focus on the investigation. Any attempts to modify the report by the police officer will be highlighted once again as the value of the hash code will be updated from the third node.

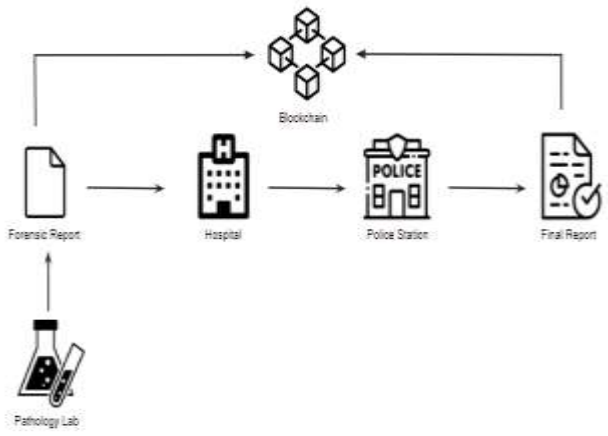

Fig 1: Proposed System Architecture Overview

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 222-228
Published Online July 2022 in IJEAST (http://www.ijeast.com)

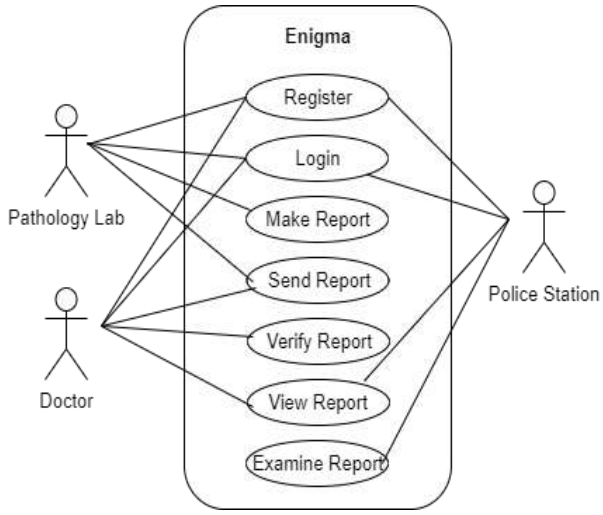

Fig 2: Use case Diagram for the Proposed System

IV. METHODOLOGY

- The forensic report will be taken as an input from the pathology lab.
- The data obtained will be encrypted and stored as a block. This block contains all the information about the transaction like sender, receiver, time etc.
- This data block is then sent to the hospital where a particular doctor will be assigned to verify the report
- The final verified and tamper free report will be further sent to the police department
- The data will be received successfully by the police department where all the details will be verified. and the transaction is completed.

V. RESULTS AND DISCUSSION

After reviewing and going through a considerable number of papers published by different authors, we were successfully able to develop an application which securely carries out the procedure oftamper-proof forensic data transfer among the different entities of the system ensuring confidentiality, integrity and security of the data involved whilst favourably preserving the chain of custody. In the future we aim towards increasing the security of the application by increasing the strength of the cryptographic encryption algorithm.

VI. CONCLUSION

Right after obtaining the respective proof from the incident that took place till it is reviewed by a court of law, Ensuring the validity and authenticity of the evidence is crucial.Preserving the chain-of-custody also is critical because it can demonstrate whether or not the evidence was tampered with during the collecting and process of analysis. Because blockchain enforces validity, accountability, authenticity, safety, and auditability by nature, it is the greatest solution for forensic custody chain management and traceability. Because of this trust, Blockchain helps to eliminate friction, bringing true promise to forensic culture. We intend to develop a blockchain application that will accept the pathology lab's forensic report as input and send a tamper-proof forensic report to the police station whilst ensuring that developed system is scalable, efficient, traceable and helps in managing the data records in an efficient manner.

VII. ACKNOWLEDGEMENT

This project has been supported by VGST, Department of ITBT&ST, Government of Karnataka. Project has been developed as a part of Project CoE Digital Forensics Intelligence GRD 853.

VIII.REFERENCES

[1]. Sathyaprakasan, R., Govindan, P., Alvi, S., Sadath, L., Philip, S., & Singh, N. (2021, March). An Implementation of Blockchain Technology in Forensic Evidence Management. In 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 208-212). IEEE.

[2]. Patil, S. M., Agarwal, R., Ashtekar, S., Dolwani, M., & Nagare, S. (2020). Analyzing Need of Secure Forensic Report System using Blockchain. (IRJET), 7(04).

[3]. Patil, S., Kadam, S., & Katti, J. (2021, February). Security enhancement of forensic evidences using blockchain. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 263-268). IEEE.

[4]. Taş, R., & Tanrıöver, Ö. Ö. (2019, October). Building a decentralized application on the Ethereum blockchain. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.

[5]. Nyaletey, E., Parizi, R. M., Zhang, Q., & Choo, K. K. R. (2019, July). BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 18-25). IEEE.

[6]. Alizadeh, M., Andersson, K., & Schelén, O. (2020, December). Efficient decentralized data storage based on public blockchain and IPFS. In 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) (pp. 1-8). IEEE.

[7]. Kirrane, S., & Di Ciccio, C. (2020, November). Blockconfess: towards an architecture for blockchain constraints and forensics. In 2020 IEEE International

Conference on Blockchain (Blockchain) (pp. 539-544). IEEE.

[8]. Velliangiri, S., & Karthikeyan, P. (2020, January). Blockchain technology: challenges and security issues in consensus algorithm. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-8). IEEE.

[9]. Rajput, S., Singh, A., Khurana, S., Bansal, T., & Shreshtha, S. (2019, February). Blockchain technology and cryptocurrenices. In 2019 Amity international conference on artificial intelligence (AICAI) (pp. 909-912). IEEE.

[10]. Tasatanattakool, P., & Techapanupreeda, C. (2018, January). Blockchain: Challenges and applications. In 2018 International Conference on Information Networking (ICOIN) (pp. 473-475). IEEE.

[11]. Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access, 6, 38437-38450.

[12]. Fartitchou, M., El Makkaoui, K., Kannouf, N., & El Allali, Z. (2020, September). Security on blockchain technology. In 2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-7). IEEE.

[13]. Huang, W. C., Yeh, L. Y., & Huang, J. L. (2019, September). A monitorable peer-to-peer file sharing mechanism. In 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 1-4). IEEE.

[14]. Thuraisingham, B. (2020, October). Blockchain technologies and their applications in data science and cyber security. In 2020 3rd international conference on smart blockchain (SmartBlock) (pp. 1-4). IEEE.

[15]. Airbail, H., Mamatha, G., Hedge, R. V., Sushmika, P. R., Kumari, R., & Sandeep, K. (2021). Deep learning-based approach for malware classification. International Journal of Intelligent Defence Support Systems, 6(2), 61-80.

[16]. Kandiga, S., Kini, U. N., Kini, U. K., & Mamatha, G. (2020, August). Image Processing and Location based Image Querier (LBIQ). In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 856-861). IEEE.

[17]. Shetty, V., Vishwakarma, S., & Agrawal, A. (2017, May). Design and implementation of video synopsis using online video inpainting. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 1208-1212). IEEE.

[18]. A, Harisha et al. (2022), A Performance Evaluation of Convolution Neural Networks for Kinship Discernment: An Application in Digital Forensics'. Intelligent Decision Technologies, vol. 16, no. 2, pp. 379-386 DOI: 10.3233/IDT-210132.

[19]. [19] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151.

[20]. [20] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143