Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 14, Issue. 1 : 2023
ISSN : **1906-9685**

SAFEGUARDING FORENSIC EVIDENCE WITH BLOCKCHAIN TECHNOLOGY

[#1]Mrs.BHEERAM SANKEERTHANA, *Assistant Professor*
[#2]Mr.VANGAPALLI RAVITEJA, *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: In this highly advanced and contemporary day, data plays an extremely significant role in all aspects of business. The safety of data is of the utmost importance because of the dynamic nature of its content. A corporation that is inclusive will address concerns such as how data is represented and what it can do with that data. It is possible that sensitive information belonging to a particular company will be attacked by a third party. As the rate of cybercrime continues to skyrocket, those with malicious intentions are working to alter these numbers. In spite of this, the scientific evidence that is anticipated to establish provenance is quite robust. It makes sense to save the forensic evidence in this manner given the multiple stages that are involved in conducting a scientific investigation. This procedure involves following a legal order in which the report is communicated through a number of different representatives and levels, including the authorities, a pathology lab, a forensic lab, and so on. Utilizing blockchain technology is quickly becoming the most common method for developing a straightforward system that ensures the incorruptibility of measured confirmations.
Index Terms **-** Forensic evidence, Blockchain Technology.

INTRODUCTION

Blockchains are made up of a network of blocks that are linked together and store and record all activities on a decentralized platform. These blocks are linked together by cryptographically secure links. Due to the fact that it is dispersed, it has progressed past the typical stages. The manner in which ideas, concepts, and application platforms are put into action is one area in which several examples of Blockchain innovation may be observed. Hacking continues to be a problem in this day and age despite the fact that technology is continually improving. As a result of this, intricate evidence is required to demonstrate where these cybercrimes originate and how they are connected to one another. The use of online proof is fraught with several difficulties. The custody chain is an important component of advanced proof management because it safeguards the timeline and records it in a fashion that can be validated.

When used to the investigation of cybercrime, the findings of electronic forensics move from a less trustworthy level of understanding to a more trustworthy level of understanding. When individuals communicate with one another by electronic confirmations, there is frequently a complex cycle of mistrust and denial that ensues. There is a significant requirement for a system that is able to fulfill the requirements of accountability, consistent quality, and safety, in addition to having the capacity to conduct reviews.

LITERATURE SURVEY

In order to obtain information about criminals, a Blockchain-based architecture is utilized. Every hub has the ability to monitor the changes that are pushed out by the Director hub. When a new report is added to the chain, cryptography rules are applied in order to generate a hash that is unique to that report. If one hub tries to send a report after several other reports have already been delivered to the

initial square, it will have repercussions for the entire chain. This illustrates how uniform everything is. The structure is well-known, without a shadow of a doubt, for its capacity to bring clarity to the situation.

The blockchain combines a number of desirable characteristics, including honesty, openness, reliability, safety, and the capability to be checked on purpose. Because of this, it is likely to be the ideal choice when it comes to following and maintaining track of the science chain. The blockchain technology helps to reduce latency in a number of different ways, two of which are by boosting confidence and assuring forensic locations. The ultimate objective is to build a sophisticated digital system using Ethereum and smart contracts to keep track of who has access to what kinds of research materials. The use of online investigative tools by an increasing number of people to investigate into attacks on an increasing number of cloud-based data storage facilities has contributed to the rise in popularity of cloud computing. What the results of the study were.

Legal research is utilizing cloud-based technologies in order to investigate potential threats to the expansion of cloud data storage. This is something that is happening more frequently as both technology and the number of individuals who use the internet continue to advance. The importance of distributed computing to the field of advanced legal studies has been the subject of research from a number of different studies. In this study, a comparison is made between the various stages of traditionally offered computerized legal services and those offered through the cloud.

The B-CoC project is an engineering effort that makes use of blockchain technology to simplify and expedite the process of computerized information transfers. The emphasis here is placed on making the Chain of Custody (CoC) processes less physically demanding. Additionally, we provided you with a B-CoC building model that simplified the process of running Ethereum nodes on the Geth platform. It has been demonstrated that the B-CoC is an effective tool for CoC interaction because it can successfully allow responsibility allocation. This is facilitated by having sufficient memory to hold the chain, which also makes the process of allocating responsibilities simpler.

A fresh method for the computerized administration of proofs is introduced here with the assistance of the Blockchain technology. The characteristics of trustworthiness, openness, security, credibility, and the capacity to be checked are all possessed by blockchain technology. As a consequence of this, it becomes one of the greatest choices available for maintaining the continuity of the scientific chain of control.

1. PROPOSED METHODOLOGY

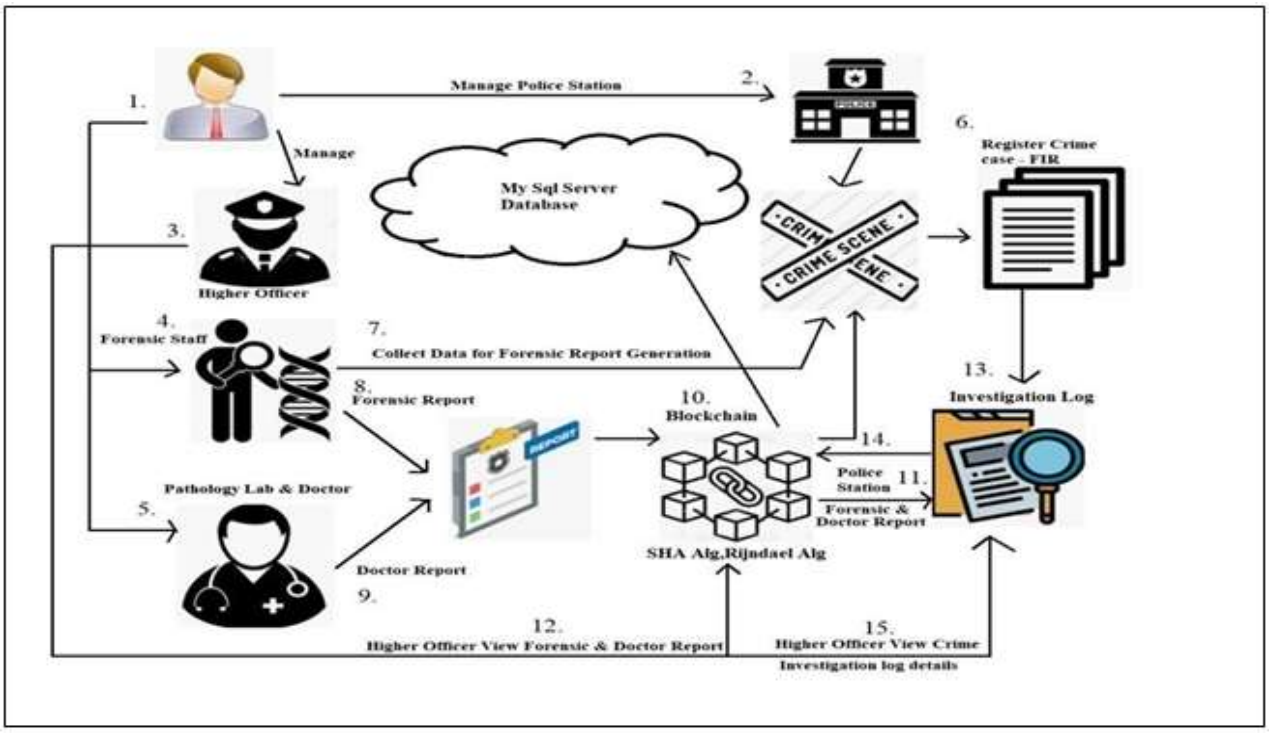

Fig. 1.System Architecture

Modules

Application Manager

---Login(Default ID,Password)
---Manage area & Police Station(Generate Unique ID,Password)- - Login Id & Password
---Manage Forensic Staff
(Generate Unique ID,Password)- - Login Id & Password
---Manage Pathology Lab Staff
(Generate Unique ID,Password)- - Login Id & Password
---Manage Doctor
(Generate Unique ID,Password)- - Login Id & Password
---Manage Higher Officer
(Generate Unique ID,Password)- - Login Id & Password

Police Station

---Login (ID,Password)
---Register Crime - FIR
---Collect crime forensic data(forensic staff & Doctor)--Blockchain
---Manage Crime Investigation & evidence

Forensic Staff

---Login (ID,Password)
---Visit crime place & collect data for forensic lab test
---Generate report for crime forensic data based on police station crime - blockchain
---View Details

Pathology Lab

---Login (ID,Password)
---Visit crime place & collect data for patholgy lab test
---Generate report for crime forensic data based on police station crime - blockchain
---View Details

Doctor

---Login (ID,Password)
---Examination based on crime(murder - death body)
---Generate report based on police station crime - blockchain
---View Details

Higher Officer

---Login (ID,Password)
---Monitor crime investigation based on police station
---View Forensic data report & doctor report based on police station crime

Rijndael Algorithm

The process consists of four discrete stages all together. The word that was entered is altered in a variety of ways as a result of these stages. There are three key lengths that can be used with this method: 128 bits, 192 bits, and 256 bits. These can be used regardless of the block length. In total, there could be 10, 12, or 14 rounds, and every single one features a variety of different shifts. The four stages are referred to as Shift Rows, Sub Bytes, Mix Columns, and Add Round Key respectively. This is done to ensure the confidentiality of the reports generated by the various applications. This technology is utilized by a large number of various offices over the world to safeguard their reports.

Secure Hash Algorithm

The abbreviation SHA refers to the Secure Hash Algorithm. A hash number can be assigned to data or certificates using SHA, which is an upgraded version of the MD5 algorithm. Hashing is a process that takes data and converts it into a format that cannot be understood by using bitwise operations, modular additions, and compression functions. Hashing is also known as one-way encryption. Hash codes are generated in order to verify the accuracy of the information.

CONCLUSION

The use of blockchain technology helps to ensure that forensic findings are kept secure. Establishing a hierarchy of restricted users who are in charge of the investigation is one strategy for enhancing the way of gathering forensic evidence in a secure manner. Every single person has their very own access, which ensures that everything is crystal transparent and cannot be altered in any way.

REFERENCES

1. Omi Aktera, Arnisha Aktherb, Md Ashraf Uddinc, Md Manowarul Islamd.2020.Cloud Forensics: Challenges and Blockchain Based Solutions, I.J. Wireless and Microwave Technologies.
2. Dr.S. Harihara Gopalan,S. Akila Suba, C. Ashmithashree, A. Gayathri, V. Jebin Andrew.2019.Digital Forensics Using Blockchain, ISSN: 2277-3878, Volume-8, Issue-2S11.
3. lvia Bonomi, Marco Casini, Claudio Ciccotello.2019 B-CoCA Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics.
4. Sagar Rao, Shalomi Fernandes, Samruddhi Raorane, Shafaque Syed.2021.A Novel Approach for Digital Evidence Management using Blockchain.
5. Derick Anderes, Edward Baumel, Christian Grier, Ryan Veun, and Shante Wright.2019.The Use of Blockchain within Evidence Management Systems.
6. Lamprini Zarpala,Fran Casino.2021A Blockchain-based Forensic Model for Financial CrimeInvestigation: The Embezzlement Scenario, 30 June 2021.
7. Sonali M Patil,Rahul Agarwal, Saburi Ashtekar , Muskan Dolwani, Snehal Nagare.2020.Analyzing Need of Secure Forensic Report System using Blockchain.
8. Giuliano Giova.Improving chain of custody in forensic investigation of electronic digital systems.2016. International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 1–9.
9. Mats Neovius, Magnus Westerlund.2018.Providing Tamper-Resistant Audit Trails for Cloud Forensics with Distributed Ledger based Solutions" IARIA, ISBN: 978-1-61208-607-1 CLOUD COMPUTING :The Nineth International Conference on Cloud Computing, GRIDs, and Virtualization.
10. Duc-Phong Le, Huasong Meng, Le Su, Sze Ling Yeo, and Vrizlynn Thing.2018. BIFF: A Blockchain-based IoT ForensicsFramework with Identity Privacy, Proceedings of TENCON 2018 - 2018 IEEE Region 10 Conference,