IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN TECHNOLOGY FOR SECURING FORENSIC EVIDENCE

[1]Dr. Reshma Banu

Professor, Department of ISE,
GSSS Institute of Engineering & Technology for Women, Mysuru, India

[2]Deeksha G

Student, Department of ISE,
GSSS Institute of Engineering & Technology for Women, Mysuru, India

[3]M Preethi

Student, Department of ISE,
GSSS Institute of Engineering & Technology for Women, Mysuru, India

[4]Triveni S

Student, Department of ISE,
GSSS Institute of Engineering & Technology for Women, Mysuru, India

Abstract: Data assumes a significant part in each period of work in the present advanced time. Data should be safe since it can modify. Portrayal and capacity of data will be addressed in heterogeneous organization. There are chances of assault on information which is crucial for specific association. With quick expansion in cybercrime, assailants act perniciously to change those data. Be that as it may, it's incredibly affecting scientific proof which is expected for provenance. In this manner, it's expected to keep up the forensic evidence since it goes through different stages during scientific examination. during this methodology, there's a legal chain during which produced report goes through different levels or delegates like pathology lab, forensic lab, police and so on to make the straightforward framework with changelessness of measurable confirmations, blockchain technology innovation is more appropriate.

Index Terms **- Forensic evidence, Blockchain Technology.**

I. INTRODUCTION

Blockchain is an assortment of squares which are connected, that contains and tracks generally that occurs on a conveyed framework. Because of its dispersed nature, it has supplanted customary stages. Blockchain innovation is used in various evidence of idea executions, models and application frameworks. In this powerful time, there are constant cybercrimes occurring, so there is fundamental job of advanced proof to check the confirmation of beginning and verification of connection associated with cybercrimes. There is parcel of difficulties with online proof. The guardianship chain can be portrayed as a framework used to hold and record the authentic history of advanced proof taking care of.

Electronic Forensic confirmations goes through different degrees of ordered progression, that is from the lower mindful substance to the higher dependable substance for dealing with cybercrime examinations. There is generally an intricate advance of break of trustworthiness and disavowal during this exchange of computerized confirmations. The requirement for the hour is to have a framework that guarantees responsibility, unwavering quality, security and capacity of review.

II. LITERATURE SURVEY

[1] The Blockchain based framework is carried out for getting criminological reports. Director hub can see refreshes at each hub. Whenever any report is added to chain, extraordinary hash is created by applying the ideas of cryptography. When report is added into beginning square, in the event that the other hub attempts to transfer report, so it'll be applicable to chain completely. This gives the unchanging nature. The framework is certainly recognizable which gives straightforwardness.

[2] Blockchain intentionally implements uprightness, straightforwardness, legitimacy, security and auditability hence pursuing it conceivably the easiest decision for keeping up with and following scientific chain. Blockchain technology helps in grinding decrease with more trust and helps in bringing the 000 guarantee for criminological local area. the more extended term work targets creating total Ethereum based brilliant computerized scientific chain of guardianship utilizing savvy contracts. Cloud computing has grown in popularity as a result of technological breakthroughs and the widespread usage of the internet techniques to forensics for investigating attacks on greater data storage on the cloud The study's findings.

[3] Innovative improvements, as well as widespread online use, have boosted the employment of cloud-based methodologies in legal sciences to investigate attacks on larger data storage on the cloud. As a result of the varying research, the commitment of distributed computing in advanced legal sciences has been addressed. The study work focuses on the various stages of traditional and cloud-based computerized legal services.

[4] B-CoC, a blockchain-based engineering to dematerialize the CoC interaction in computerized criminology. We additionally gave a model of the B-CoC engineering upheld the Geth execution of Ethereum hubs. upheld the presentation assessment, B-CoC demonstrated to be a decent help for the CoC interaction since it is prepared to support reasonable responsibility with an appropriate upward as far as memory acclimated store the chain.

5] A fresh out of the box new framework for computerized proof administration is proposed which uses Blockchain innovation. Blockchain by its example applies the ideas of trustworthiness, straightforwardness, security, credibility, and auditability. This makes it one in everything about best decisions for the upkeep and following back of the scientific chain of guardianship

III. PROPOSED METHODOLOGY

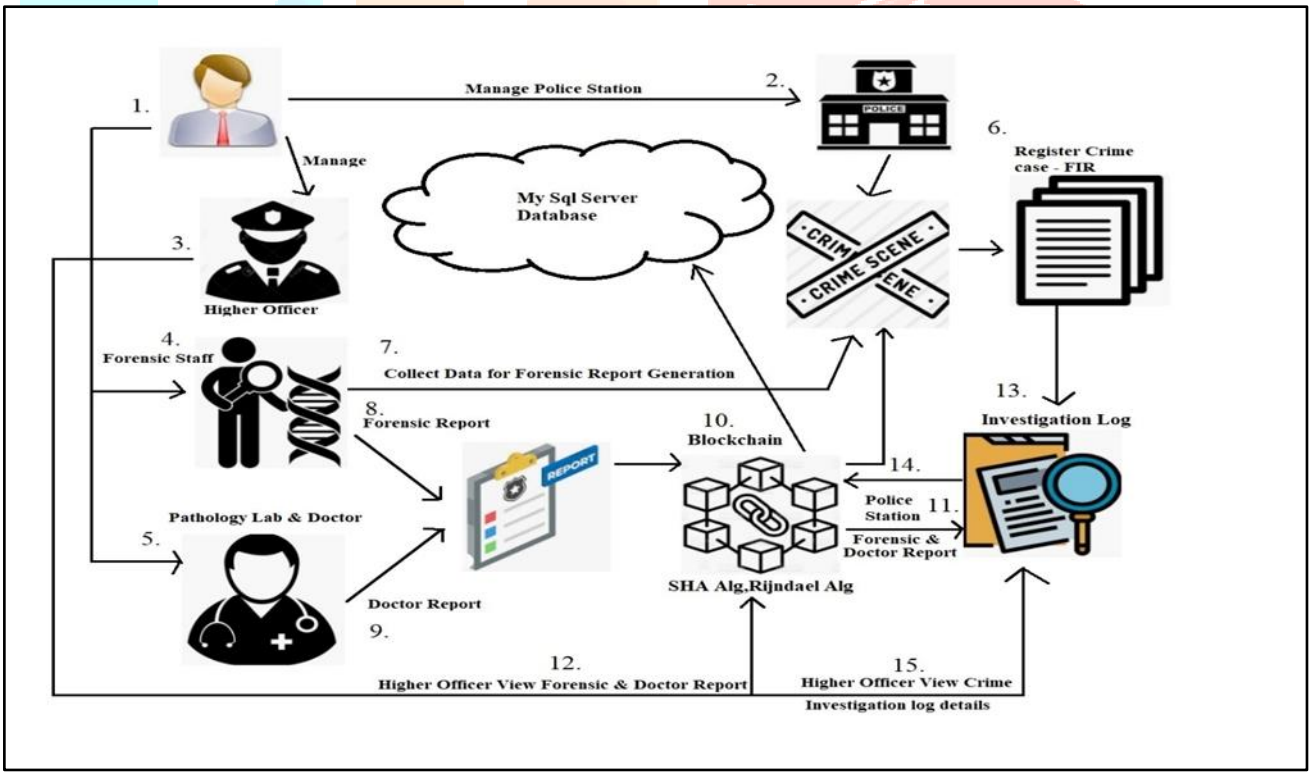

Fig. 1.System Architecture

3.1 Modules

1. 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

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

3. 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
4. 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
5. Doctor
   ---Login (ID,Password)
   ---Examination based on crime(murder - death body)
   ---Generate report based on police station crime - blockchain
   ---View Details

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

3.2 Rijndael Algorithm

There are four steps involved in the algorithm. These steps perform specific transformations in the input plaintext. The algorithm can be used with three key lengths (independent of selected block length): 128, 192, or 256 bits. It can consist of 10, 12 or 14 rounds where each round consists of transformations. The four steps are Shift Rows, Sub Bytes, Mix Columns, Add Round Key. This is used to encrypt the report generated by the respective modules. The reports generated by the respective departments is encrypted using this algorithm.

3.2 Secure Hash Algorithm

SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions.This is used to verify the informaiton by generating hash codes.

IV. CONCLUSION

The Blockchain based system is implemented for securing forensic reports. The secure forensic evidence system has been proposed to achieve optimization by creating chain of limited users responsible in the investigation. They are given their respective access to achieve transparency and immutability.

REFERENCES

[1] Sonali Patil, Sarika Kadam, Jayashree Katti.2021. Security Enhancement of Forensic Evidences Using Blockchain.

[2] Omi Aktera, Arnisha Aktherb, Md Ashraf Uddinc, Md Manowarul Islamd.2020.Cloud Forensics: Challenges and Blockchain Based Solutions, I.J. Wireless and Microwave Technologies.

[3] 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.

[4] lvia Bonomi, Marco Casini, Claudio Ciccotello.2019 B-CoCA Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics.

[5] Sagar Rao, Shalomi Fernandes, Samruddhi Raorane, Shafaque Syed.2021.A Novel Approach for Digital Evidence Management using Blockchain.

[6] Derick Anderes, Edward Baumel, Christian Grier, Ryan Veun, and Shante Wright.2019.The Use of Blockchain within Evidence Management Systems.

[7] Lamprini Zarpala,Fran Casino.2021A Blockchain-based Forensic Model for Financial CrimeInvestigation: The Embezzlement Scenario, 30 June 2021.

[8] Sonali M Patil,Rahul Agarwal, Saburi Ashtekar , Muskan Dolwani, Snehal Nagare.2020.Analyzing Need of Secure Forensic Report System using Blockchain.

[9] Gongzheng Liu,Jingsha He, and Xinggang Xuan.2019.A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics.

[10] Auqib Hamid Lone, Roohie Naaz Mir.2020. Forensic-Chain: Ethereum Blockchain Based Digital Forensics Chain Of Custody.

[11] 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.

[12] Shijie Chen, Chengqiang Zhao, Lingling Huang.2020.Study and implementation on the application of blockchain in electronic evidence generation, Elsevier Forensic Science International: Digital Investigation

[13] 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.

[14] Duc-Phong Le, Huasong Meng, Le Su, Sze Ling Yeo, and Vrizlynn Thing.2018. BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy, Proceedings of TENCON 2018 - 2018 IEEE Region 10 Conference,.

[15] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, R. Buyya, and A. Y. Zomaya.2016.Cloud log forensics: foundations, state of the art, and future directions, ACM Computing Surveys