JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FUZZY HASH BLOCK CHAIN BASED CHAIN OF CUSTODY TO SECURE DIGITAL EVIDENCE MULTIMEDIA FORENSICS

THIRUMALAI SAMY. M1 Mrs. S. KALAIVANI 2

PG Student 1, Assistant professor 2,

PG & Research, Department Of Computer Applications

HINDUSTHAN COLLEGE OF ARTS AND SCIENCE

COIMBATORE, INDIA

Abstract: ***Digital forensics deals with digital evidence. Digital forensics is the study of data detection, acquisition, processing, analysis, and reporting. Encouraging the use of digital forensics in law enforcement investigations. With digital forensics, you can find out what data was taken and how it was copied or spread. Some hackers purposefully destroy data to harm their targets. In other cases, malicious software or hacker involvement can accidentally corrupt vital data. Digital forensics faces challenges of security and integrity. The system can collect digital forensic evidence in an setting, putting cybercrime agencies at danger owing to security and integrity. Many studies have been done recently to improve police based digital forensics integrity and security, but researchers face the risk of confidentiality. Recent research shows that digital forensics still faces manipulation and security issues. So a clever and effective approach is needed that not only protects security and integrity but also anticipates threats. So we propose an intelligent and effective solution based on Block chain and Hashing algorithms. We will store the data collected from the police side into Block chain. Anomalies in the evidence and transactions will be predicted using Machine Learning boosted models. So the proposed model works well because it can predict attacks early on.***

Keywords: Digital Forensics, Digital Evidence, Acquisition, Processing, enforcement investigation, Block chain and hashing algorithms

I. INTRODUCTION

Criminal histories are extremely private pieces of information. The validity and rigidity of records may be upheld by adding criminal records into a block chain, which also helps to protect the data from adversaries. The decentralization of data is made possible by a peer-to-peer cloud network. It assists in preventing unauthorized data alterations. In order to achieve integrity and security, this article offers a system for storing criminal records that uses block chain technology. Our system

offers suggestions for effective ways for the government to keep track of criminals' records. With the aid of block chain technology, unfairly targeted police officers and defendants can be shielded from problems with the chain of custody that could result in false imprisonment for defendants and, worse, wrongful termination for officers. This paper will outline the unique difficulties associated with keeping evidence on a block chain and offer a practical fix. The writers and researchers of this study will address some of the issues raised by David Billard in his white paper 1Tainted Digital Evidence and Privacy Protection in Blockchain Based Systems.

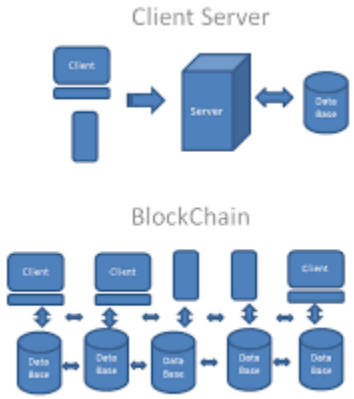

Fig 1.1 Fuzzy Block chain

Databases are extremely valuable sources of information for any system. Database management requires digital management as a result of the expanding digitization. The simultaneous rise in threats makes database management challenging. The greatest method for managing databases is block chain. Data is given integrity, validity, and transparency thanks to block chain's decentralized nature. This study outlined the areas in which block chain technology can be used in cities to maintain criminal records. It makes it easier for authorities (courts, government agencies) to obtain the data. Also, this article assesses the crime graph based on criminal history. Using block chain technology will reduce time, costs, paperwork, and corruption.

The upkeep of reliable information about people, groups, things, and activities is a crucial duty of the government. Maintaining records that include, for example, birth and death dates or information about marital status, business licencing, property transactions, or criminal activity is the responsibility of local, regional, and national agencies. Even for highly developed administrations, managing and using these data can be challenging. Certain documents are only available in paper form, and people frequently need to visit in person to make changes to official registries. Of course, these data must be safeguarded with absolute precision against unwanted access and alteration.

Paper documents can be authenticated in a variety of ways, including by looking for watermarks, signatures, and embossed seals. The downside of paper is that it can be lost, is difficult to keep and locate specific records, takes time to duplicate and change, is difficult to communicate, and poses a serious threat to data security. Hence, digital Records are presented. Digital documents can be edited and copied secretly without anybody knowing.

Moreover, data processing is done more quickly, which lowers the chance of data errors. There are numerous goods and services that offer secure and certified document management, but they can be pricey and frequently call for a third party's involvement.

BLOCK CHAIN LOG

Since block chain has extensive implications for data security and authentication at reduced cost and improved efficiency, it is crucial for records management experts to comprehend it. In order to prevent tampering or change, it accomplishes this by including authentication within the document itself and employing a closed loop tracking mechanism. You already have a general idea of how the procedure operates if you've ever used a synchronized file-sharing programmed like Microsoft One Drive or Drop Box. These services allow users to exchange files while keeping local copies by syncing the data across all users. A document is automatically copied to everyone else's local folder when one person makes modifications to it.

The method is the same in block chain, but a block-like layer of code is added. A block is nothing more than a collection of distinct characters and numbers that have been encrypted using public key, a very safe method. The use of public key encryption is crucial because it allows the information's owner to maintain control over it without disclosing sensitive data like names or Social Security numbers. On a block chain network, each participant receives a "golden copy" of the file containing the embedded block. A new block is inserted and the updated file is synchronized throughout the network if the document changes, a procedure that typically takes just a few seconds. A chain is created as more changes are performed and new blocks are added.

Professionals in records management should learn more about blockchain for the following reasons. The most obvious advantage is cost savings. Processes can be made more cost-effective and efficient because bloc kchain transactions don't need middlemen. As auditors and attorneys are not required to verify the accuracy of material, their fees are not included in the process.

- Efficiency: Quicker turnaround is achieved with fewer workers. Transactions can be completed in a matter of seconds rather than taking days to wait for several sign-offs.
- Security: The chance of things going wrong in a transaction decreases with the number of participants.
- A key weakness is at handoff points, which block chain effectively eliminates.
- Flexibility – Block chain can be used with any digital asset, even those that are challenging to preserve, like multimedia and email records.

Various types of mathematical evidence administration have existed grown. Development is accomplished offset from plain XML documents to complex foundations. The Digital Evidence Cabinet (DEC) is individual of bureaucracy [6]. DEC is a mathematical evidence administration approach accompanying the idea of locking away material evidence. DEC was erected the idea of evidence depository cabinets for mathematical evidence. In exercise, the rules for utilizing tangible cabinets must within financial means visit in the mathematical rule. DEC has little stage. There are government, rack, bag and evidence tag. Some tag clarifies for the specific level. Digital evidence management and maintenance are individual stage of mathematical judicial process. This part is very important because mathematical evidence is the action of mathematical judicial process. The mathematical evidence must be maintained for regulation and court process. Process of protection of mathematical evidence famous as chain of

jailing (CoC). CoC is a document that used to guarantee that mathematical evidence debris and does not change. Both all the while the analysis process just before the finishing of the judicial process. Electronic evidence proof is various from mathematical evidence documentation. The various are individuality and the metadata. Some adaptations need expected accommodated on scheme for mathematical evidence. Digital evidence is smooth to change in addition to allure CoC document. It needs expected shielded. A new electronics is wanted that can guarantee uprightness of mathematical evidence and CoC Document like the blockchain. In this study, mathematical evidence administration will be buxom on the CoC idea accompanying blockchain electronics. More precisely, this design integrates the foundation of the Digital Evidence Bag (DEC) accompanying blockchain science. This example is famous as the Blockchain Digital Evidence Bag (B-DEC). B-DEC appropriates the data conversion uprightness to adapt mathematical evidence administration that refers to DEC.

II. RELATED WORKS

Legal evidence stored on computers and digital recording media is the focus of digital forensics. This is a process and a method for formally establishing and proving the facts of a certain digital device-related action. Inspectors and analysts in local, state, and federal law enforcement agencies regularly employ digital forensics technologies. Due to format incompatibility, encryption, or a lack of knowledge, more and more businesses are running into data that cannot be evaluated with the technologies available today [11]. Many ,researches are currently being done to increase operational effectiveness through a methodical method of expressing forensic data and carrying out forensic activities. The US federal court system is looking into how to make digital surveillance more accountable.

The authors of [12] provide an example of how accountability and secrecy can be achieved at the same time when using contemporary cryptography. To do this, the authors employ a hierarchical form of multi-party computation that mimics the judicial system's hierarchy. Currently, there are seven steps to a criminal investigation in Korea for managing digital evidence: the initial investigation, the internal investigation, the arrest, the conclusion of the investigation, the request for analysis, the transmission of the digital evidence and investigation documents, and the trial [3]. step one, the preliminary research, is carried out whilst a criminal offense takes place. that is initiated via on-web site research corporations that apprehend the characteristics of a case. in the 2nd step, the internal investigation, criminal evidence is collected by using traveling the website after a warrant has been issued for a promising suspect. The suspect is arrested in the 1/3 step, the arrest technique. inside the fourth step, the investigation is concluded, and on-web page investigators gain pictures of the criminal proof. within the 5th step, the crook evidence for the case is gathered, and statistics about the investigator and research are registered inside the Korea records machine of criminal Justice services (KICS). If an in depth analysis is required, a request is dispatched to the challenge analysis crew of each local police agency, and the consequences are back. in the sixth step, the tough disk that contains the authentic crook proof, research files, and criminal evidence analysis effects is dispatched to the prosecution and recorded in the research documents for storage. inside the last step, digital proof that has been despatched to the prosecutor’s workplace and reviewed is submitted to the courtroom for use as proof in the trial.

Studies on approaches of enhancing the original identity, integrity, and reliability of crook virtual proof received inside the investigation manner in Korea have been performed [4,5]. However, most of those research focus on identifying the traits of digital facts, and establishing an existence-cycle-based totally management surroundings with integrated virtual proof control. Determine 1 indicates one proposed incorporated virtual crime management system in Korea. Its goal turned into to integrate virtual proof and investigation data through the countrywide transmission community by using linking KICS a crook justice information system operated by using the police, prosecutors, and courts and the case control structures of the country wide police organization [4].

But, in previously proposed integrated digital evidence control structures in Korea, a server became operated as a centralized device in an included server/purchaser environment. A centralized machine is a gadget that techniques all data from every vicinity on a primary computer. In different phrases, it refers to a machine wherein one particular computer methods, as opposed to using all of the computer systems in a server machine connected through a verbal exchange network to manner data. A centralized device has the blessings of without problems integrated records management, and occasional control charges, due to the fact the records are targeting a critical server. However, in this type of gadget, whilst a server is attacked, critical operations and research records of the applicable institution can be leaked, and the continuity of storage cannot be maintained for digital proof. Therefore, virtual proof and research statistics have to be managed reliably and transparently in distributed surroundings, no longer in the current centralized digital incorporated control gadget.

III. METHODOLOGY

(i) Multimedia statistics garage.

After the multimedia statistics is encrypted, records garage starts. In this link, the database is the provider of multimedia facts records storage, so the layout of the database is very vital. There are numerous types of multimedia information and the number is big. Consequently, the database should meet functional necessities: classifying and storing record statistics; users can timely and as it should be extract the required records from the database [7]. The facts performance desires to be flexible, efficient, secure, dependable, and much less redundant. After the database is established, the block chain stores the multimedia data records in a disbursed records garage mode. In every storage operation, the block chain takes the preceding encrypted records as the basis, and then integrates the facts that wish to be stored inside the modern-day time to shape new multimedia facts. Ultimately, the block chain is once more quad-tree encoded and encrypted to complete cozy statistics storage. This reality that encryption is achieved every time there's new information makes it difficult for the multimedia facts in the block chain to be modified and leaked [8]. In e-commerce records information, there are numerous photograph information, inclusive of magnetic resonance imaging, CT, ultrasound, and so on. consequently, on this storage study, handiest photo storage become studied. After the photograph information is encrypted, the blocks can be classified according to their specific traits, including their colors, effects, and textures. And for fast storage, there should be appropriate index. Index is a structure that kinds the values of one or more columns in a database table. it could be used to speedy get right of entry to precise data in a database table. In relational database, index is a desk-

related database shape which could make square statements that correspond to tables be accomplished faster. Storage is a standard e-commerce facts index.

IV. RESULT AND CONCLUSION

On different study skilled are many exercise of block chain on another fields. Such as [17] that implement block chain for control of product quality. On additional study [18] design an unification of block chain accompanying IoT. Another supply chain accompanying block chain again defined refers to [19]. This resources that block chain is an appealing science to expand. One of reason is block chain guarantees dossier completeness and safety. The design of DEC idea accompanying block chain electronics (BDEC) was completed activity by translating DEC necessities into a struct dossier type. Smart contract arrange administering DEC on the block chain when keeping dossier. It has acquired a mathematical evidence administration design. It must accommodate the minimum needs of mathematical evidence dossier by hoarding it harmlessly on the block chain. The DEC foundation may be buxom on the block chain. Some adaptations are wanted in the data conversion portion. One of ruling class is plotting a foundation growth expected capable to adjust a sort of mathematical dossier containing many files (split files). In addition, few adaptations created are increasing the record idea that follows mathematical evidence. Furthermore, the foundation was grown by merging accompanying the depository district of evidence. It may be decided if the DEC-located block chain maybe grown until unification accompanying mathematical evidence depository (DES).

V. REFERENCES

1.Jonston, A. Murder Charges Filed in 1985 Cold Case. Available online: **https://oag.ok.gov/articles/murder-charges-filed-1985-cold-case** (accessed on 27 April 2021).

2.Choi, S.W. Every Crime Leaves a Mark. Available online: **https://sedaily.com/NewsView/1OMAEK89A4** (accessed on 27 April 2021).

3.Police Agency in Korea Police. *White Paper: A Society Safe from Crime*; Korean National Police Agency: Seoul, Korea, 2019; p. 232. [**Google Scholar**]

4.Jung, H.H. Management from the perspective of the Life Cycle of Digital Evidence. *J. Digit. Forensics* **2016**, *10*, 1–20. [**Google Scholar**]

5.Jeong, J.; Kim, D.; Lee, B.; Son, Y. Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric. *J. Inf. Process. Syst.* **2020**, *16*, 760–773. [**Google Scholar**]

6.Tak, H.S.; Lee, W.S. *A Study on a Model Frame for the Integration of Digital Forensic Processes*; Korean Institute of Criminology: Seoul, Korea, 2016. [**Google Scholar**]

7.Arslan, S.S.; Goker, T. Compress-Store on Blockchain: A Decentralized Data Processing and Immutable Storage for Multimedia Streaming. In Proceedings of the IEEE BCCA, Antalya, Turkey, 2–5 November 2020. [**Google Scholar**]

8.Sahoo, S.; Fajge, A.M.; Halder, R.; Cortesi, A. A Hierarchical and Abstraction-Based Blockchain Model. *Appl. Sci.* **2019**, *9*, 2343. [**Google Scholar**] [**CrossRef**][**Green Version**]

9.Oktian, Y.E.; Lee, S.-G.; Lee, H.J. Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment. *Electronics* **2020**, *9*, 1050. [**Google Scholar**] [**CrossRef**]

10. Albizri, A.; Appelbaum, D. Trust but Verify: The Oracle Paradox of Blockchain Smart Contracts. *J. Inf. Syst.* **2021**. [**Google Scholar**] [**CrossRef**]

11. Garfinkel, S.L. Digital forensics research: The next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73. [**Google Scholar**] [**CrossRef**][**Green Version**]

12. Frankle, J.; Park, S.; Shaar, D.; Goldwasser, S.; Weitzner, D. Practical accountability of secret processes. In Proceedings of the 27th USENIX Security Symposium, Baltimore, MD, USA, 15–17 August 2018. [**Google Scholar**]

13. Norvill, R.; Pontiveros, B.B.F.; State, R.; Cullen, A. IPFS for Reduction of Chain Size in Ethereum. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1121–1128. [**Google Scholar**]

14. Hoffman, A.; Becerril-Blas, E.; Moreno, K.; Kim, Y. Decentralized Security Bounty Management on Blockchain and IPFS. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 241–247. [**Google Scholar**]

15. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [**Google Scholar**] [**CrossRef**]