A Block-chain based Enforcement to Reduce Cybercrimes in Digital Forensics

Susheel George Joseph[1], Tincy Thomas[2], Sahal P Najeeb[3], Sangeetha Sathyapal[4]

([1]Associate Professor, Kristu Jyoti College of Management and Technology, Kottayam, Kerala, India)

([2]MCA, Kristu Jyoti College of Management and Technology, Kottayam, Kerala, India)

([2]MCA, KristuJyoti College of Management and Technology, Kottayam, Kerala, India)

([4]MCA, Kristu Jyoti College of Management and Technology, Kottayam, Kerala, India)

Abstract-*The fundamental aim of digital forensics is to discover, investigate, and protect an evidence, increasing cybercrime enforces, digital forensics team have to more accurate evidence handling. It makes digital evidence as an important factor to link persons with criminal activities. A chain of custody refers to a process of recording and preserving in court of law. It forms the forensic link of evidence sequence of control, transfer, analysis to preserve integrity, and to prevent its contamination. Thus, it is of utmost importance to guarantee integrity, authenticity, of digital evidences in cyber-crime investigation. So, guaranteeing the authenticity and legality of processes and procedures used to gather and transfer the evidence in a digital society is a real challenge. Block-chain technologies of enabling view of transaction back to origination provide enormous promise for the coming era.it is also used for securing IoT devices through efficient authentication and data transfer mechanisms. Block-chain based digital forensics chain of custody, influence forensic applications in bringing integrity to digital forensics.*

Key words- Block-chain, Cybercrime, Chain of custody, Digital forensics

1. Introduction

Today Cybercrimes are increasing day by day in this world. India has seen an increase of 37% cyber-attacks in the first quarter of 2020 compared to fourth quarter of the last year. India ranks 27th globally in the number of web threats detected by the company. The increased usage of internet has led to 500% increase of cyber threats within the country alone. A cybercrime is a crime involving computers and networks. Cyber criminals are not always financially motivated. There are many types of cybercrimes prevalent today such as identity theft, psychological tricks, social media attacks, banking frauds etc.

Block chain is a decentralized, public distributed ledger, which permits transaction across peer to peer network using cryptography without having a central authority. It provides trust and transparency among individuals. The characteristics of block chain technologies are anonymity, immutability, traceability, integrity, and confidentiality. With these, block chain can greatly save the cost and improve efficiency. It is a driving force and an indispensable part of next revolution in this digital field.

These new technologies are make our life easier and faster but these are also providing easier way for the criminals in their activities in this field. Digital evidences are playing an important role in cybercrime investigations. So it can connect the peoples with criminal activities so it is important to guarantee the integrity, traceability in evidences. But a problem in digital forensics I the management of evidences. Block chain technologies is a promise for the forensic community.it is a technology that permits transactions, the data gathered into blocks and recorded as cryptographically in chronological order; and allows the resulting ledger to be accessed by different servers.it is linked by chain and are added into blocks after solving a cryptographic puzzle. Each block contains a data and timestamp which points to the previous block. the data in each block cannot altered by a person. Mining is performed by high powered computer that solve complex math problems, once they solve a puzzle they are awarded with some bitcoin. Cryptocurrency is a medium of exchange, created and stored electronically in the block-chain using encryption techniques to control the creation and to verify the transaction. bitcoin is the best known example. Block-chain is successfully working

in transactions, supply chain, industries etc. The benefit of block-chain in digital forensics that it provides self-verifications for digital evidences. It makes use of cryptography to maintain the chain of evidences, cryptography, chain of custody.

2.Theory

A. Blockchain -In Block chain, the data are distributed among nodes. After verification, new block is added in the chain by broadcasting others. It is open to everyone at any time. A block contains the hash value of previous block. The first block is known as Genesis block. Once a block is added, we can't make any changes. They added the block after solving a cryptographic puzzle. If the submitted answer is correct, then it will have broadcasted among miners. Else, redo the calculation. The first miner gets rewarded.

Blockchain by proposal harvests the best of security, integrity, transparency and audit thus making it the unsurpassed choice for maintaining and securing the forensic CoC. Blockchain decreases conflict and increases belief through the distributed blockchain making it impossible to alter every block. Blockchain is the most effective solution for CoC for the digital era of forensics.

B. Chain of custody (CoC) - Chain of custody is the sequential documentation or paper trail that records the grouping of guardianship, control, move, investigation, and air of physical or electronic proof. Of specific significance in criminal cases, the idea is likewise applied in common case—and now and again more comprehensively in drug testing of competitors, and in flexibly chain the board, for example to improve the recognizability of food items, or to give confirmations that wood items begin from reasonably oversaw backwoods. It is regularly a dull cycle that has been needed for proof to be demonstrated lawfully in court. The person who taken the evidence will be responsible for it. It will invalid if it has any sign of changes.

The structure of a block can be represented as follows,

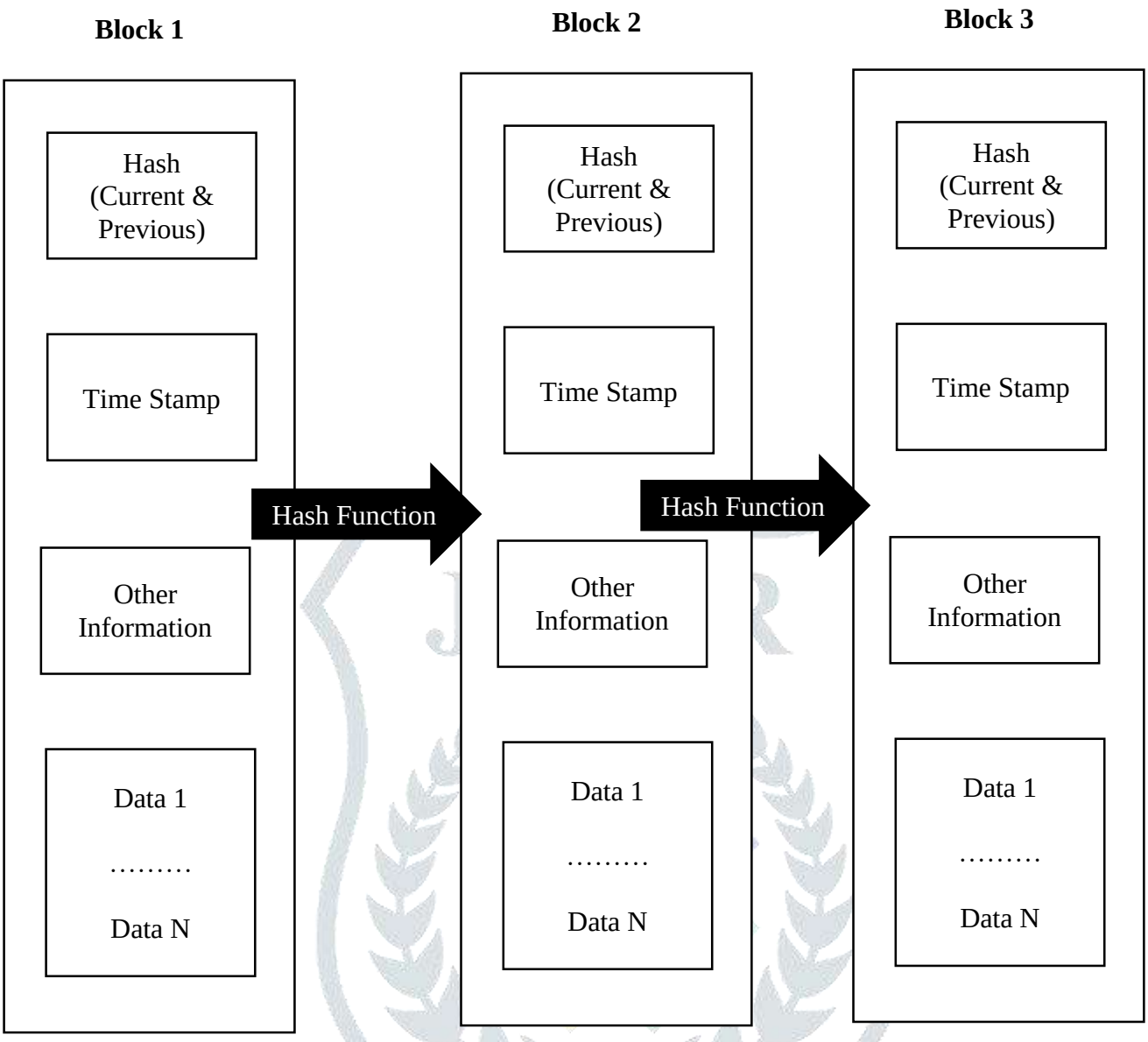

Figure 1. Structure of a Block

3. Materials and Methods

Some steps are given below in order to show the chain of custody in digital forensics with blockchain technology.

Step1- The evidences are collected and gathered in form of DNA analyzer, video, sound, text, pictures or even framework logs including the hour of the proof gathered to maintain a timeline

Step2-The gathered information is transferred to the database to make them tamper proof which assists to store the details of cases. A URL is created as per the information transferred to it. The created URL is utilized for hashing in the blockchain.

Step3-The URL is considered as string and it is gone through hash calculation for hashing. The timestamp likewise hashed alongside URL for greater honesty. The hashed value is put away in the block itself.

Step4-The block is made with a timestamp. The timestamp assists with finding when the proof was transferred to the blockchain. In case of any tamper, it will change, which prompts breaking of chain. If it is not beaks the block will be in the proper state.

Step5-proof of work (: Pow) is a strategy to guarantee whether the evidence have been altered, as the connection of block would've been lost after a specific point. This should be possible by reiterating the current squares to cross-reference with the current information.

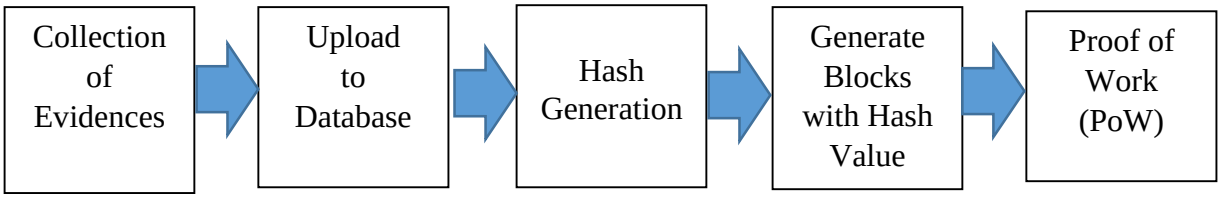

Figure 2.: Steps to show CoC in DF with BC Technology

Blockchain is a distributed public ledger which keep the whole transaction. The copies are given to the multiple participants called node and distributed among them. So the CoC should protected without any changes after the collection. It will increase the purity of evidences in the court. if any changes were done it will detect b the all nodes.so the hashing promise the security of each block.

B . Blockchain for chain of evidence management in IoT

In IoT, the data are storing digitally, so the evidence will be in a form of digital assets. Fingerprinting digital evidence is a way for generating a fingerprint for each piece of evidence. By, hashing the blocks are encrypted. The hash value is unique.

- Block chain can make data secure and it is verified by evidences and addition information.
- The data are stored in a certain order, so it can track to its origin.

In IoT, block chain helps the forensic community in an economic and efficient way

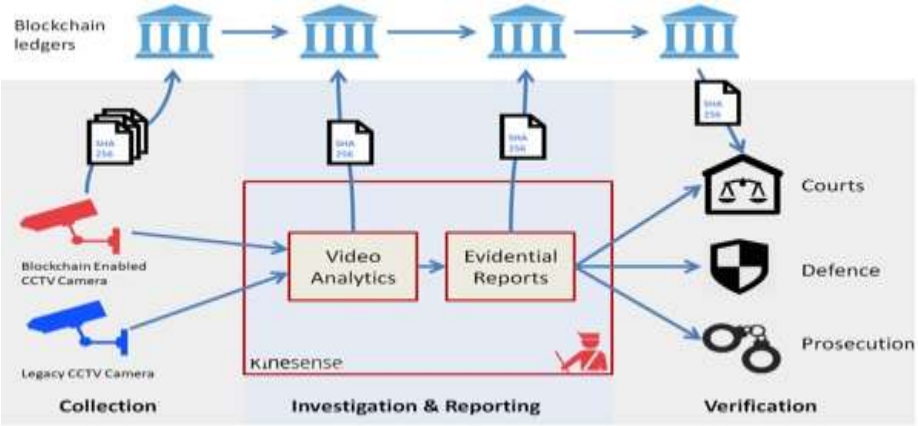

Figure 3: Blockchain for Chain of Management (CoM) in CCTV

C . Blockchain cyber security solutions

Security of data properties in various states requires execution of security controls are mechanisms, calculations and complex algorithms. Besides, every security framework requires a wellspring of trust, in whom trust is unrestricted. With each activity that happens on a blockchain being carefully marked and timestamped, there can be no contesting who's gotten to or moved it and when. Each exchange on the chain can be related with the cryptographic mark of a specific client. Utilizing decentralized capacity innovation. Therefore, they can store documents and other computerized things on a distributed ledger that is consistently available, and that it is not possible to destroy, by eliminating a great part of the human component from data storage, blockchains fundamentally alleviate the danger of human mistake, which is the biggest reason for information penetrates. Bitcoin blockchain has not been effectively hacked since its origin. At the point when designed appropriately and reasonably dispersed, a blockchain can protect information, everything being equal, and for all. Cyber security experts can be considered as the guardians of the world's information. Blockchain is certified currency, yet it's an effective way to transfer, store and encrypting data and monitoring.

4. Result and discussion

The focal point of Blockchain IoT security is reasonable. Since there are presently 9 billion such gadgets. These gadgets have feeble security designs and many are being hacked also, selected into botnet networks. One such botnet network involved IoT Gadgets is the Mirai Botnet which has been utilized with high paces of achievement against huge targets. Thus, numerous security scientists are taking a gander at manners by which these gadgets can be made sure about through Blockchain. Information stockpiling is the second famous focus of Blockchain network protection research. This is a direct result of the expanded information robbery situations where programmers have had the option to exfiltrate information having a place with billions of clients from organizations. Thus, security specialists are checking out discovering Blockchain security answers for information extra rooms including cloud stages. It can likewise be seen that specialists are investigating the use of Blockchain in making sure about organizations. The greater part of the exploration in these regions is around verification since current organization safety efforts.

Blockchain innovation can be utilized to improve network safety. Indeed despite the fact that the current security arrangements offer exemplary levels of security to IT assets, they are as yet inclined to disappointment. This is on the grounds that most security instruments are conveyed to work autonomously while making sure about an IT asset. As has been the situation with assaults, for example, DDoS (Distributed Denial of Service), programmers can focus on a solitary security arrangement, put it unavailable and afterward continue to assault the now-uncovered IT asset. Analysts on the courses through which Blockchain can help improve the current trends of security and their contentions on the expanded capacity of circulated security devices to be in an ideal situation at offering security than a solitary device. In IoT organizations, the main security danger is unapproved access and control of the gadgets. Blockchain security arrangements can help oversee access control and information sharing for all IoT gadgets all the more viably.

A qualitative analysis is done to check the application of BCT in today’s cyber security industry. It is focused on a study by Taylor et al., who reviewed 30recent research studies on BC cyber security use areas.

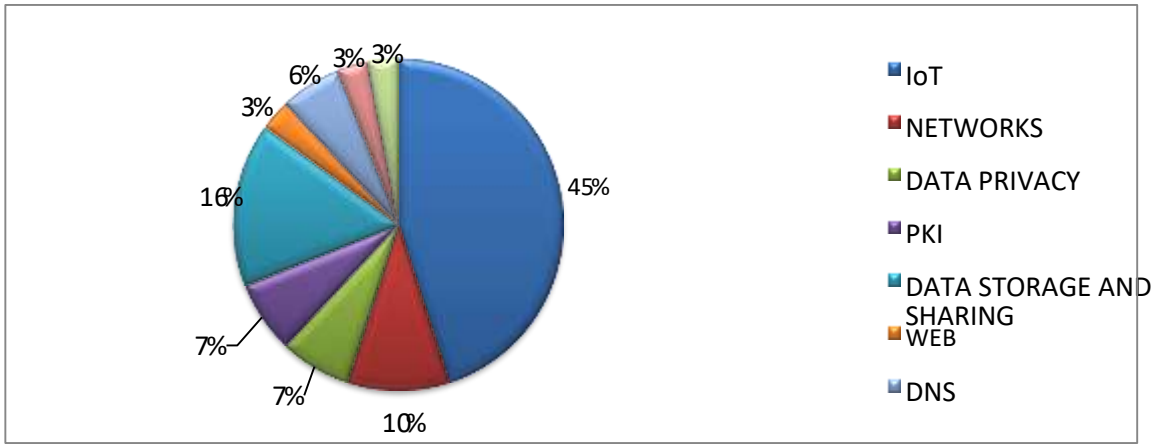

Figure 4: Most Researched Blockchain Security Application Areas

The pie chart shows the evaluation of 30 studies in most researched areas in blockchain applications.it is clear that IoT, network and data storage security is more feasible than others. In recent implementation of blockchain security. In the themes of primary studies 45% are concerned with IoT devices security. Data Storage and Sharing is the second most famous topic with 16%. blockchain applications are looking encoded cloud-based information and forestalling altering of record names and the information contained inside. Organizations are the third most regular topic with 10% and are generally worried about how blockchain can give security and legitimacy to virtual machines and holders. Information Privacy and Public Key Infrastructure are the fourth most regular topic with 7% each; the blockchain applications consider end clients to verify here and there with another element or administration and do as such that they don't have to depend on a weak focal worker of data. The fifth most normal subject is Domain Name Systems and how blockchain can adequately have DNS records in a circulated climate to forestall malignant changes and refusal of administration assaults. The most un-regular subjects identify with Wi-Fi, Web and Malware with 3% each.

5.Conclusion

Block Chain Technology is applicable on many areas in the modern world. It is also applied and studied in the field of cybercrimes. Block Chain infrastructure is the effective solution on current security challenges in areas chain of IOT devices, data transmission and storage in digital area of forensics. Blockchain can secure the data in transmission and storing by cryptography which an open by the parties and it is not prone to manipulation.

Technology alone will ever be an answer to battle against cybercrime on its own. Human experts and experience are essential for perceiving and detect criminal activities. Here the blockchain technology will help to manage data in a secure manner and give a tool for experts to operate in an effective manner, by this we can prevail over the challenges in cyber-crime. Thus, Block Chain might be a part of a long-term solution. It recommends that future researchers go for the practicality of a single Block Chain used to develop security more than from current situation.

7.References

[1] Lone, A.H., &Mirren. (2019).Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28,44-55

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[3] Crosby, Michael,etal."Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): pp. 71 T. M.H. 2012. *Computer forensics: Cybercriminals, laws and evidence*. Canada: Jones and Bartlett Learning

[4] Hreinsson, E. M., & Blöndal, S. P. The future of blockchain technology and cryptocurrencies (Doctoral dissertation).

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system

[6] Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 463-467). IEEE.

[7] Buterin, V. (2013). Ethereum white paper. (2013). URLhttps://github. com/ethereum/wiki/wiki/White-Paper.

[8] Bonomi, S., Casini, M., &Ciccotelli, C. (2018). B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. arXiv preprint arXiv:1807.10359.

[9] Lone, A. H., & Mir, R. N. (2018). Forensic-chain: ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J.

[10] Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. Procedia computer science, 98, 461-466.

[11] Halpin, H., &Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 1-3). IEEE.

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

[13] Susheel George Joseph, "A Machine Learning (ML) Modelling Approach in Monitoring and Controlling the Viral Pandemic- COVID 19", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.7, Issue 6, page no.1709-1717, June 2020: http://www.jetir.org/papers/ JETIR2006575.pdf

[14] Susheel George Joseph, "The Usage of Machine Learning Evolutionary Algorithms in Medical Images Formed by Computer Tomography (CT) or X-Rays to Detect the Infections due to COVID 19", PENSEE (penseeresearch.com) ISSN: 0031-4773. Volume 51, Issue 4, Page No:1512-1518, April 2021. Available at: https://app.box.com/s/n6nsv8myosb0wb16psvtb8conekpy ohj

[15] S.Binny, "A survey concept on Deep Learning", International Journal of Scientific & Engineering Research (www.ijser.org), ISSN 2229-5518 , Volume 10, Issue 6, page 1570-1575, June-2019.

[16] Susheel George Joseph, "A Machine Learning (ML) Modelling Approach in Monitoring and Controlling the Viral Pandemic- COVID 19", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.7, Issue 6, page no.1709-1717, June 2020: http://www.jetir.org/papers/ JETIR2006575.pdf

[17] Susheel George Joseph, Dr. Vijay Pal Singh, "Denoising of Images using Deep Convolutional Neural Networks (DCNN)", International Journal of Engineering Development and Research (IJEDR), ISSN:2321-9939, Volume.7, Issue 3, pp.826-832, September 2019, http://www.ijedr.org/papers/IJEDR1903143.pdf.

[18] S. Binny, Dr. P. Sardar Maran, "Classification of Lung disease using deep learning neural networks, " PENSEE (penseeresearch.com) ISSN: 0031-4773. Volume 51, Issue 6, Page No: 466-470, June 2021.