Blockchain based Digital Forensics Investigation Framework in the Internet of Things and Social Systems

Mr.S. Nelson M E.,
Assistant Professor,
Department of Information Technology
V. S. B. Engineering College
Karur, Tamilnadu

Mr. K. Ponvasanth B.Tech.,
Department of Information Technology
V. S. B. Engineering College
Karur, Tamilnadu

Mr. S. Karuppusamy B.Tech.,
Department of Information Technology
V. S. B. Engineering College
Karur, Tamilnadu

Mr. R. Ezhumalai B.Tech.,
Department of Information Technology
V. S. B. Engineering College
Karur, Tamilnadu

***Abstract*— The decentralized nature of blockchain technologies can well match the needs of integrity and provenances of evidences collecting in digital forensics (DF) across jurisdictional borders. In this paper, a novel blockchain-based DF investigation framework in the Internet of Things (IoT) and social systems environment is proposed, which can provide proof of exis- tence and privacy preservation for evidence items examination. To implement such features, we present a block-enabled forensics framework for IoT, namely, IoT forensic chain (IoTFC), which can offer forensic investigation with good authenticity, immutabil- ity, traceability, resilience, and distributed trust between evi- dential entitles as well as examiners. The IoTFC can deliver a guarantee of traceability and track provenance of evidence items. Details of evidence identification, preservation, analysis, and presentation will be recorded in chains of block. The IoTFC can increase trust of both evidence items and examiners by providing transparency of the audit train.This Project describe the secured communication using Blockchain for defence Application.This proposed scheme is used to establish privacy to sign a message using the corresponding private key.The decentralized nature of blockchain technologies can well match the needs of integrity and provenances of evidences collecting in digital forensics (DF) across jurisdictional borders.we present a block-enabled forensics framework for IoT, namely, IoT forensic chain (IoTFC), which can offer forensic investigation with good authenticity,immutability, traceability, resilience, and distributed trust between evidential entitles as well as examiners.**

1.INTRODUCTION

Blockchain cloud storage solution take the user's data and break it up into small chunks. Then they add an additional layer of security and distribute it throughout the network. This is possible by using Blockchain features like hashing function private/public key encryption and transaction data (ledgers).

Another benefit is that the owner is hidden since the node does not store the owner's data. The participants or user only gets a chunk of data, Hence all the sensitive info is protected and secured.

Data redundancy and load balancing mechanisms are applied for high availability and quick access.

Blockchain is the newest and possibly the cheapest way to get cloud storage because many small entities participate is cloud storage by providing their computing power and space to store data.

Blockchain is a growing list of records called block, that are linked using cryptography each block contains cryptographic hash of the previous block, a timestamp, and transaction data.

2.*EXISTING SYSTEM*

Many of IoT nodes are collecting and processing private information,they are becoming a goldmine of data for malicious actors.

Security and specially the ability to detect compromised nodes,together with collecting and preserving evidences of an attack or malicious activities emerge as a priority in successful deployment of IoT networks.

First introduce existing major security and forensics challenges within IoT domain and then briefly discuss about papers published in this special issue targeting identified challenges.

DISADVANTAGE

Not able to provide,

1) Trustworthy
2) Integrity
3) Improved provenance
4) Availability and Resiliency
5) Scalability

3.PROPOSED SYSTEM

Blockchain Technology overcome the above challenges and it can makes the data acquisition and validation more accurate and informative by integrating the TEs and additional information.

For each TE item, its provenance as well as all related examining events can be traced back to its origination.

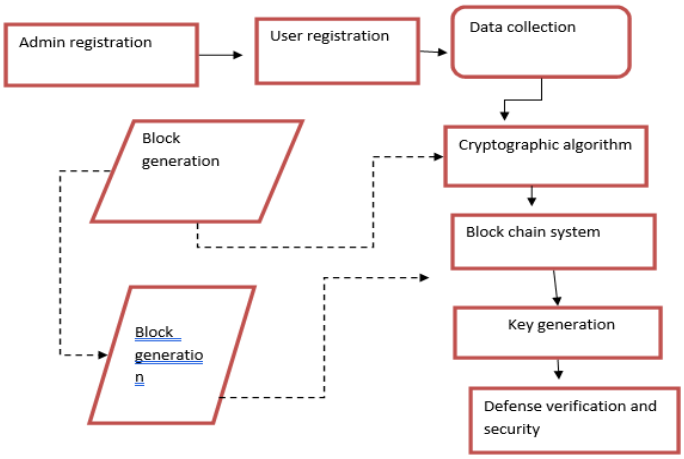
The IoTFC uses Blockchain to build a close-loop system that provides significant forensic analysis benefits in an efficient and economical way.

ADVANTAGE

- Security
- Faster processing
- Traceability
- Process integrity

4.MODULES

- Registration
- Data collection
- Cryptographic function



- Block chain computing
- Performance evaluate

REGISTRATION

- The registration module allow the user and data owner to create login username and the password by submitting their information like mail id, phone number, name, etc.
- By registering the network or cloud the user can gain access to the resources stored in the cloud.

DATA COLLECTION

- Data is collected based on the wireless sensor network in the den fence field.
- The **blockchain** is a decentralized, digital ledger that is used to record transactions occurring in a network, secured using cryptographic technology.
- Due to the immutable and cryptographically verified security of a **blockchain** network, it offers a way to remedy the issues currently present in the **data** industry.

CRYPTOGRAPHIC

- The cryptographic hash function is used to create the digital signature for each unique block. There is a large variety of hash functions, but the hashing function that is used by the Bitcoin blockchain is the SHA-256 hashing algorithm.
- The cryptographic hash function is used to create the digital signature for each unique block. There is a large variety of hash functions, but the hashing function that is used by the Bitcoin blockchain is the SHA-256 hashing algorithm.

BLOCK CHAIN SYSTEM

- A blockchain is all about organizing and storing information in accordance with a predefined logic.
- Instead of data being accounted and stored on a central server's database, it's encrypted, and a copy is stored on every node connected to the network.

PERFORMANCE EVOLUTION

- The performance of the system is analyzed by security of the system.
- Accuracy and integrality is analyzed for security of the system.

ALGORITHM

Cryptography involves written code that requires authorized decoding and encryption. Blockchain is managed by a network that adheres to *protocols* for nodal communication and validating new blocks. Miners validate transactions to be recorded to the blockchain. Mining requires the application of an *algorithm*, to validate and retrieve data. Cryptocurrency is a digital currency in which encryption is used for the regulation and generation of units of currency. Cryptocurrency uses cryptography for security and blockchain technology to record transactions. This mechanism from adding to the chain of records to validating transactions in its entirety is referenced as a blockchain algorithm.

In blockchain, every node in the network results in the same conclusion, each updating the record independently, with the most

popular record being the de-facto official record in lieu of a master copy. Transactions are broadcasted, and every node creates its own updated version of events. This makes blockchain technology unique it represents innovation in recording information and distribution that eliminates the need for a third party to facilitate digital relationships.

Blockchain technology is a combination of technologies applied in various new ways. It is built on a platform using protocols, it is on a peer-to-peer-network that is a system of record and uses private key cryptography for identity. An algorithm is part of a protocol.

The result is a system of transactional interactions that do not require a trusted third party. The work of securing digital relationships is inherent supplied by the robust, simple, yet sophisticated network architecture of blockchain technology itself.

CONSENSUS ALGORITHMS

Consensus algorithms are complex but help when purchasing coins or running a node. Consensus algorithms achieve reliability on networks involving multiple nodes, making sure all nodes conform to the said rule or action. Nodes define consensus in bitcoin, not miners.

Consensus is defined by the chain with the most work. If you fork and change the POW, you will not have the mining power to secure it. Nodes accept the transactions, validate the transactions, replicate the transactions, validate the blocks, replicate the blocks, serve the blockchain, and store the blockchain. Nodes even define the Proof-of-Work algorithm that miners have to employ.

The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.Now, we will discuss various consensus algorithms and how they work.

1. Proof of Work (PoW): This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block. For more details on PoW, please read Proof of Work (PoW) Consensus
2. Practical Byzantine Fault Tolerance (PBFT): Please refer to the existing article on practical Byzantine Fault Tolerance (pBFT).
3. Proof of stake(Pof):

This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake.

After that, all the validators will start validating the blocks. Validators will validate bl ocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly.

In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

Proof of Burn(PoB) With PoB, instead of investing into expensive hardware equipment, validators 'burn' coins by sending them to an address from where they are irretrievable. By committing the coins to an unreachable address, validators earn a privilege to mine on the system based on a random selection process. Thus, burning coins here means that validators have a long-term commitment in exchange for their short-term loss. There are various inherent advantages of this approach which includes excellent color, high brightness quality and high luminous efficacy of the emitter –within the range of 150 lumens per watt or greater. The architecture that one is mechanically robust without typical degradation and that is a failure mechanism associated with tungsten electrodes and glass to metal seals, resulting in useful lamp life of 30,000+ hours. In addition, the unique combination of high temperature plasma and digitally controlled solid state electronics results in an economically produced family of lamps scalable in packages from 3,000 to over 100,000 lumens.

4.CONFIGURATION

HARDWARE SYSTEM CONFIGURATION:-

1) Processor – Pentium –IV
2) RAM – 4GB (minimum)
3) Hardware Disk – 20GB
4) LI-FI Module

SOFTWARE SYSTEM CONFIGURATION:-

1) Operating System: Windows 7,8,10
2) Application Server: Net Beans
3) Front End: Java
4) Back End: SQL

5.SYSTEM DESIGN

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.

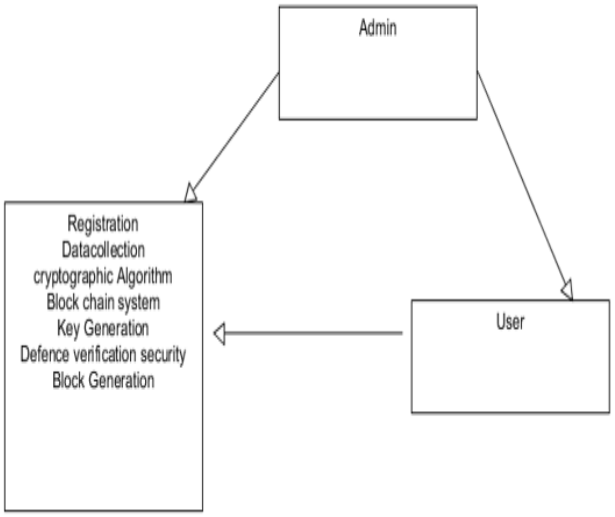
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

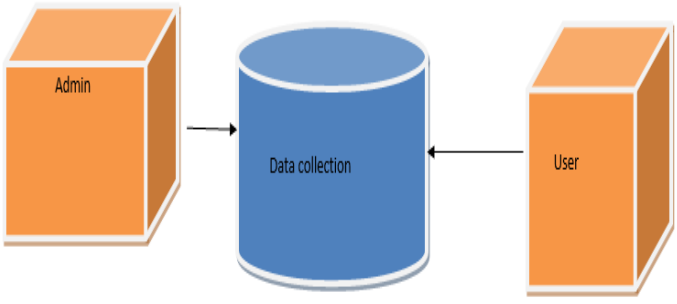
USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.





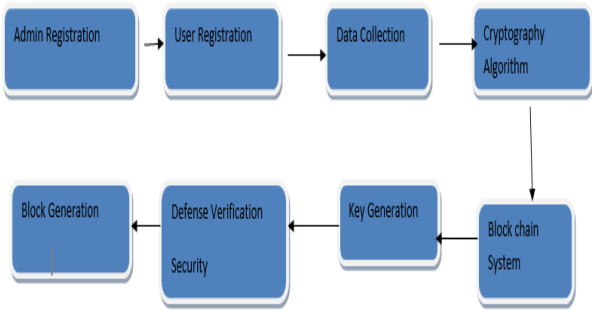
DEPLOYMENT:

Component diagrams are used to describe the components and deployment diagrams shows how they are deployed in hardware. UML is mainly designed to focus on the software artifacts of a system. However, these two diagrams are special diagrams used to focus on software and hardware components.

DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



6.CONCLUSION

Forensic research on the blockchain-based forensic investigation framework by considering the diversity of devices, evidence items, data formats, and more in the complicated IoT environment. The main idea is to retrieve artifacts from IoT devices and further write to blockchain-based IoTFC after analyzing the connections between evidence items, provenance, traceability, and auditability of each evidence item.

Blockchain solutions have recently been proposed for both intrusion detection and forensic evidence applications, since in both cases blockchain can solve issues pertaining to trust, integrity, transparency,

accountability, and secure data sharing. Addressing the issue of trust management, Alexopoulos, applied blockchain in collaborative intrusion detection networks to deal with insider threats but also enhance the security of the information shared among the participating IDS nodes. More precisely, the authors proposed to store the generated (raw) alerts of the network as transactions in a permissioned blockchain.in addition to the dimension of trust between the IDS nodes, refer to issues that pertain to privacy when collaborating nodes belong to different trust domains, as shared data may have sensitive information linked to individuals or organizations, e.g., IP addresses and packet payloads. Methods for exchanging encrypted content, or only hashed data rather than raw, are considered. In forensic investigations, it is important that the evidence is not modified while passing from one entity to another.

The blockchain can be used in order to certify the authenticity and legitimacy of the procedures used to gather, store and transfer digital evidence, as well as, to provide a comprehensive view of all the interactions in the CoC. In a blockchain-based CoC, it is crucial to assure that members, having read/write access to the distributed ledger, are authenticated and the evidences are verified via a consensus algorithm. Towards that direction, Lone, et al. propose a private blockchain that can be used in digital forensics to ensure the integrity of evidences the authors also aim at recording the actions taken by each entity when interacting with the evidence. On the other hand, ProbeIoT uses a blockchain to discover criminal events, which can be used as evidence, by collecting interactions between IoT devices and verify their authenticity

7.REFERENCES

[1] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "SCLPV: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors," IEEE Trans. Comput. Social Syst., vol. 5, no. 3, pp. 854–857, Dec. 2018.

[2] A. Shah, R. Ganesan, S. Jajodia, and H. Cam, "Understanding tradeoffs between throughput, quality, and cost of alert analysis in a CSOC," IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1155–1170, May 2018.

[3] Y. Wu, G. Min, and L. T. Yang, "Performance analysis of hybrid wireless networks under bursty and correlated traffic," IEEE Trans. Veh. Technol., vol. 62, no. 1, pp. 449–454, Jan. 2013.

[4] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey" J. Ind. Inf. Integr., vol. 10, pp. 1–9, Jun. 2018.

[5] S. Wang, X. Wang, P. Ye, Y. Yuan, S. Liu, and F. Wang, "Parallel Crime Scene Analysis Based on ACP Approach," IEEE Trans. Comput. Social Syst., vol. 5, no. 1, pp. 244–255, Mar. 2018.

[6] Y. Liu and S. Hu, "Cyberthreat analysis and detection for energy theft in social networking of smart homes," IEEE Trans. Comput. Social Syst., vol. 2, no. 4, pp. 148–158, Dec. 2015.

[7] G. Min, Y. Wu, and A. Y. Al-Dubai, "Performance modelling and analysis of cognitive mesh networks," IEEE Trans. Commun., vol. 60, no. 6, pp. 1474–1478, Jun. 2012.

[8] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Trans. Ind. Inform., vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[9] L. M. Cullell. (2019). Digital forensics and blockchain. [Online]. Available: https://medium.com/@blockxlabs/digital-forensics-andblockchain- bf3af5e7153c

[10] Y. Teing, D. Ali, K. Choo, M. T. Abdullah, and Z. Muda, "Greening cloud-enabled big data storage forensics: Syncany as a case study," IEEE Trans. Sustain. Comput., vol. 4, no. 2, pp. 204–216, Apr./Jun. 2018.

[11] S. Li, L. Da Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and Internet of Things," IEEE Trans. Ind. Inform., vol. 9, no. 4, pp. 2177–2186, Nov. 2013.

[12] D. Zhao, L. Wang, Z. Wang, and G. Xiao, "Virus propagation and patch distribution in multiplex networks: Modeling, analysis, and optimal allocation," IEEE Trans. Inf. Forensics Security, vol. 14, no. 7, pp. 1755–1767, Jul. 2019.

[13] D. Zou et al., "A multigranularity forensics and analysis method on privacy leakage in cloud environment," IEEE Internet Things J., vol. 6, no. 2, pp. 1484–1494, Apr. 2019.

[14] S. Li, K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "IoT forensics: Amazon echo as a use case," IEEE Internet Things J., to be published.

[15] A. Paradise et al., "Creation and management of social network honeypots for detecting targeted cyber-attacks," IEEE Trans. Comput. Social Syst., vol. 4, no. 3, pp. 65–79, Sep. 2017.

[16] G. Mezzour, W. Frankenstein, K. M. Carley, and L. R. Carley, "A sociocomputational approach to predicting bioweapon proliferation," IEEE Trans. Comput. Social Syst., vol. 5, no. 2, pp. 458–467, Jun. 2018.

[17] J. Lee. (2018). Leveraging Blockchain for Forensic Applications. [Online]. Available: https://www.blockchaindailynews.com/Leveragingblockchain- for-forensic-applications_a25271.html

[18] S. Li, S. Zhao, P. Yang, P. Andriotis, L. Xu, and Q. Sun, "Distributed consensus algorithm for events detection in cyber-physical systems," IEEE Internet Things J., vol. 6, no. 2, pp. 2299–2308, Apr. 2019.

[19] M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT: A forensic investigation framework for IoT using a public digital ledger," in Proc. IEEE Int. Congr. Internet Things (ICIOT), Jul. 2018, pp. 33–40.

[20] M. M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of vehicles (IoV)," in Proc. IEEE Int. Congr. Internet Things (ICIOT), Jun. 2017, pp. 25–32. [21] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of Things forensics: The need, process models, and open issues," IT Prof., vol. 20, no. 3, pp. 40–49, May/Jun. 2018.

[21] D. Quick and K. R. Choo, "Iot device forensics and data reduction," IEEE Access, vol. 6, pp. 47566–47574, 2018.

[22] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The future of digital forensics: Challenges and the road ahead," IEEE Security Privacy, vol. 15, no. 6, pp. 12–17, Nov./Dec. 2017.

[23] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," 2018, arXiv:1802.00561. [Online].

[24] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: A smart contract enabled collusion-resistant e-auction," IEEE Trans. Inf. Forensics Security, vol. 14, no. 7, pp. 1687–1701, Jul. 2019.

[25] L. V. Der Horst, K.-K. R. Choo, and N.-A. Le-Khac, "Process memory investigation of the bitcoin clients electrum and bitcoin core," IEEE Access, vol. 5, pp. 22385–22398, 2017.

[26] H. Ritzdorf, C. Soriente, G. O. Karame, S. Marinovic, D. Gruber, and S. Capkun, "Toward shared ownership in the cloud," IEEE Trans. Inf. Forensics Security, vol. 13, no. 12, pp. 3019–3034, Dec. 2018.

[27] G. Tziakouris, "Cryptocurrencies—A forensic challenge or opportunity for law enforcement? an INTERPOL perspective," IEEE Security Privacy, vol. 16, no. 4, pp. 92–94, Jul./Aug. 2018.

[28] Z. Liu and H. Seo, "Iot-nums: Evaluating nums elliptic curve cryptography for iot platforms," IEEE Trans. Inf. Forensics Security, vol. 14, no. 3, pp. 720–729, Mar. 2019.

[29] A. Valjarevic and H. Venter, "A harmonized process model for digital forensic investigation readiness," in Advances Digital Forensics. Berlin, Germany: Springer, 2013.

[30] T. Killalea and D. Brezinski, Guidelines for Evidence Collection and Archiving, RFC Editor, 2002.

[31] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A blockchain-based decentralized efficient investigation framework for IoT digital forensics," J. Supercomput., pp. 1–16, 2019.

[32] Y. Zhang, S. Wu, B. Jin, and J. Du, "A blockchain-based process provenance for cloud forensics," in Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC), Dec. 2017, pp. 2470–2473.