International Journal in IT & Engineering (IJITE)
Volume 10 Issue 10, Oct 2022 ISSN: 2321-1776 Impact Factor: 7.256
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

Digital Forensics Investigation Framework Based on the Blockchain, IoT, and Social Networks

Vinod Kumar Uppalapu
(Computer Science & Engg.)
Dr. Prerna Sidana (Associate Professor)
Glocal School of Technology and Computer Science

Abstract
Digital forensics involves the identification, preservation, analysis, and presentation of digital evidence to support legal investigations. This paper introduces a novel blockchain-based framework for digital foren- sics (DF) within the context of Internet of Things (IoT) and social systems. The proposed framework, named IoT forensic chain (IoTFC), capitalizes on the decentralized nature of blockchain technology to ad- dress the integrity and provenance challenges of evidence collection across jurisdictional boundaries. By leveraging blockchain's features, IoTFC ensures authenticity, immutability, traceability, resilience, and dis-tributed trust among involved parties. The framework enhances transparency through recorded chains of blocks, covering evidence identification, preservation, analysis, and presentation. This project also presents a secured communication scheme using Blockchain for defense applications, providing privacy through message signing with corresponding private keys.
Keywords: *blockchain, digital forensics, Internet of Things, evidence integrity, privacy preservation*

Introduction

In the rapidly evolving landscape of Internet of Things (IoT) networks, the proliferation of interconnected devices has ushered in unparalleled convenience and efficiency. However, this connectivity comes at a cost, with IoT nodes becoming prime targets for malicious actors seeking to exploit the wealth of sensitive data they collect and process. Consequently, ensuring the security and integrity of IoT networks has become an imperative to prevent potentially devastating breaches. Detecting compromised nodes and preserving evi- dence of malicious activities have emerged as paramount challenges, underscoring the need for innovative solutions**(Zhang,et al 2018).**

This research paper explore into the prevailing security and forensic challenges within the realm of IoT networks, illuminating the vulnerabilities that threaten the viability of these systems. It explores the vul- nerabilities posed by IoT nodes, which are increasingly likened to goldmines of valuable data for malicious actors. To address these issues, the paper presents a forward-looking proposal that capitalizes on the dis- ruptive potential of Blockchain Technology.

The proposed system advocates the integration of Blockchain Technology to fortify the security and en- hance the forensic capabilities of IoT networks**(Agamy,et al 2020).** This integration is achieved by lever- aging the unique features of Blockchain, such as hashing functions, private/public key encryption, and transaction data (ledgers). By breaking down user data into smaller, cryptographically secure chunks and distributing them across the network, the system establishes an additional layer of security that safeguards against unauthorized access and tampering. The blockchain's decentralized nature ensures that the owner's identity remains concealed, fostering a heightened level of privacy**(Yu, Zhou, & Hu, 2020).**

A pivotal advantage of the proposed system is its ability to address the data acquisition and validation challenges that plague IoT networks. Through the integration of Tracking Entities (TEs) and supplemen- tary information, the provenance of each TE item can be meticulously traced, allowing for a comprehen- sive analysis of examining events. This integration culminates in the creation of an enclosed-loop system, underpinned by the Blockchain, which not only bolsters the forensic analysis process but also accom- plishes these goals in an efficient and cost-effective manner**(Dudani, et al 2023).**

By aligning with the tenets of Blockchain Technology, the proposed system offers a promising avenue for mitigating the security and forensic challenges prevalent in the IoT landscape **(Arianna, et al 2022).**This research paper aspires to contribute to the ongoing discourse on safeguarding IoT networks and fortifying their resilience against the ever-evolving threat landscape. Through a holistic exploration of the proposed system's mechanics and its potential to revolutionize IoT security paradigms, this paper seeks to under- score the transformative power of integrating Blockchain Technology in reshaping the future of secure and accountable IoT networks.

Existing System

The current situation in the IoT landscape suffers from notable shortcomings **(Bagaa,et al 2020)**. It fails to provide a trustworthy environment, lacking mechanisms to ensure data integrity and demonstrate prove- nance. Moreover, the absence of robust availability and resiliency strategies exposes networks to potential disruptions. Scalability challenges further exacerbate these limitations, hindering the seamless expansion of IoT networks. This study's purpose is to bridge these gaps by proposing a comprehensive solution that leverages blockchain technology to fortify security, enhance provenance, and provide the necessary foun- dation for scalability, resiliency, and trustworthiness.

Proposed System and Methodology

The proposed system introduces a groundbreaking solution by harnessing the capabilities of Blockchain Technology to overcome the multifaceted challenges posed by IoT networks. By integrating Tracking Enti- ties (TEs) and supplementary information, the system enhances data acquisition accuracy and validation, fostering informative insights **(Li,et al 2019)**. This integration enables the tracing of each TE item's provenance and related examining events back to their origination, ensuring a robust foundation for data integrity and traceability. The system adopts a blockchain-driven closed-loop architecture, offering effi- cient and economical forensic analysis benefits, which are particularly crucial in securing IoT networks against malicious activities **(Hossain, Karim, & Hasan, 2018).**

Modules: The proposed system consists of several pivotal modules that collectively drive its functionality. The registration module facilitates user and data owner registration, empowering them to create secure login credentials through the submission of essential information such as email addresses, phone numbers, and names. Thisgrants authenticated access to cloud-stored resources. Data collection, orchestrated through wireless sensor networks in designated fields, ensures seamless data acquisition. Cryptographic functions implement the SHA-256 hashing algorithm to generate digital signatures, guaranteeing the integrity ofeach unique block of data. Blockchain computing stores encrypted data across a decentralized network of nodes, enhancing security, traceability, and process integrity. The system's performance evaluation encom-passes analyses of security, accuracy, and integrality**(Zhang,et al2017)**.

Blockchain Algorithm and Configuration: The proposed blockchain algorithm ensures a trustworthy and decentralized data management approach. It leverages consensus mechanisms such as Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), and Proof of Stake (PoS) to guarantee agreement, collaboration, and equal participation across network nodes. Moreover, Proof of Burn (PoB) is explored, offering an alternative approach by committing coins irretrievably to enhance stakeholder commitment **(Ryu, et al 2010)** The system's hardware configuration comprises a Pentium-IV processor, 4GB RAM, and a minimum hardware disk of 20GB. The software configuration entails operating systems such as Windows 7, 8, 10, NetBeans as the application server, Java for the front end, and SQL as the back end. This robust configura- tion supports the seamless execution of the proposed system, ensuring reliability and efficiency in ad- dressing IoT network challenges.

System Design using UML Diagrams

Unified Modeling Language (UML) serves as a standardized and expressive tool for the design of software systems, enabling users to visually represent, construct, and document complex software and business models. The primary goals of UML encompass providing a ready-to-use modeling language, supporting extendibility, independence from specific programming languages, offering a formal basis for understanding the language, promoting tool development, accommodating higher-level concepts, and integrating best practices **(Marchesi, Marchesi, & Tonelli, R. (2018)**.

UML diagrams serve as powerful tools for system design, aiding in visualizing and understanding software and business models. Use case diagrams provide an overview of system functionality, class diagrams depict system structure, deployment diagrams showcase software and hardware relationships, and DFDs elucidate data flow and processing within a system. The adoption of UML promotes effective communication, documentation, and development of complex systems **(Rocha, & Ducasse, (2018).**

- **Use Case Diagram:** A use case diagram serves as a graphical representation of a system's functionality, detailing actors, their goals (use cases), and interdependencies between use cases. It provides an overview of system behavior and interactions, aiding in the comprehension of the system's capabilities and user interactions.
- **Class Diagram:** A class diagram, a type of static structure diagram, illustrates a system's structure by depicting classes, their attributes, methods, and relationships. It showcases how information is encapsulated within classes and demonstrates associations between classes, contributing to a comprehensive understanding of the system's architecture.
- **Deployment Diagram:** Deployment diagrams offer insights into the relationship between software components and hardware deployment. While UML mainly focuses on software artifacts, deployment diagrams provide a visual representation of how these components are situated within the hardware environment.
- **Data Flow Diagram (DFD):** DFD is a fundamental modeling tool that showcases information flow and transformation within a system. It delineates the input, processing, and output stages, capturing the interactions between system processes, data, and external entities. DFD is an effective way to illustrate data movement and transformation within a system**(Kombe, Manyilizu, &Mvuma, 2017).**

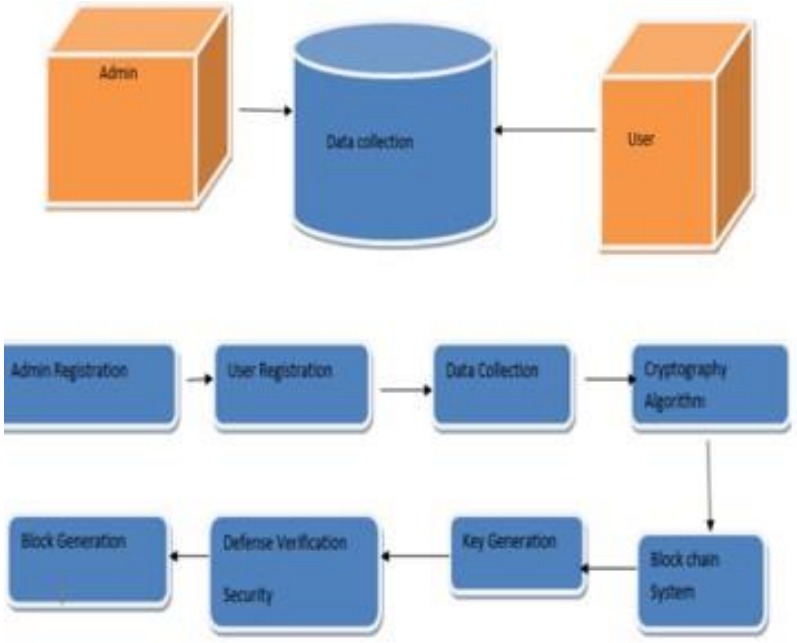

Figure 1.1 System Design using UML Diagrams(Kombe, Manyilizu, &Mvuma, 2017).

Conclusion

The realm of blockchain technology has witnessed growing interest in its application to forensic investigations within the intricate Internet of Things (IoT) landscape. The complexity arising from diverse devices, evidence items, data formats, and connections necessitates innovative frameworks. The integration of blockchain-based solutions offers a promising approach, addressing key challenges encompassing trust, integrity, transparency, accountability, and secure data sharing.

Blockchain's potential is harnessed in both intrusion detection and forensic evidence applications, addressing insider threats and bolstering security. Collaborative intrusion detection networks benefit from blockchain's ability to store raw alerts as transactions, ensuring trust among participating IDS nodes. While trust is a central focus, privacy considerations emerge when collaborating nodes belong to distinct trust domains, necessitating encryption or hashed data exchange to safeguard sensitive information.

In the domain of forensic investigations, blockchain plays a crucial role in certifying the authenticity of procedures for gathering, storing, and transferring digital evidence. Its application offers an unalterable record of interactions within the Chain of Custody (CoC), reinforcing integrity and accountability. The authentication of members with read/write access and verification of evidence via consensus algorithms ensures the reliability of the CoC.

Various studies showcase the diverse applications of blockchain in forensic investigation. Private blockchains are proposed to safeguard evidence integrity, recording actions taken by entities interacting with the evidence. Additionally, blockchain-based discovery mechanisms, such as ProbeIoT, facilitate the identification of criminal events and verify the authenticity of interactions between IoT devices.

The fusion of blockchain and forensic investigation represents a significant stride toward enhancing the security and trustworthiness of IoT ecosystems. The technology's unique attributes address pressing challenges and ensure the integrity of evidence, actions, and interactions. As the IoT landscape evolves, the continued exploration and refinement of blockchain-based forensic frameworks hold the promise of revolutionizing how digital investigations are conducted and how trust is established within IoT networks.

References

Zhang, Y., Xu, C., Yu, S., Li, H., & Zhang, X. (2015). SCLPV: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors. *IEEE Transactions on Computational Social Systems*, *2*(4), 159-170..

Agamy, A., Ali, A. M., & Mohamed, A. M. (2020). Performance analysis of WiFi networks based on sporadic traffic model using NS3. *International Journal of Mobile Network Design and Innovation*, *10*(1), 1-9...

Yu, B., Zhou, J., & Hu, S. (2020). Cyber-physical systems: An overview. *Big data analytics for cy- berphysical systems*, 1-11..

Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, *46*, 301576.

Bagaa, M., Taleb, T., Bernabe, J. B., &Skarmeta, A. (2020). A machine learning security framework for iot systems. *IEEE Access*, *8*, 114066-114077.

Li, S., Zhao, S., Yang, P., Andriotis, P., Xu, L., & Sun, Q. (2019). Distributed consensus algorithm for events detection in cyber-physical systems. *IEEE Internet of Things Journal*, *6*(2), 2299-2308.

Hossain, M., Karim, Y., & Hasan, R. (2018, July). FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. In *2018 IEEE International Congress on Internet of Things (ICIOT)* (pp. 33-40). IEEE.

Zhang, Y., Wu, S., Jin, B., & Du, J. (2017, December). A blockchain-based process provenance for cloud forensics. In *2017 3rd IEEE international conference on computer and communications (ICCC)* (pp.2470-2473). IEEE.

Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient inves-

tigation framework for IoT digital forensics. *The Journal of Supercomputing*, *75*, 4372-4387.

Marchesi, M., Marchesi, L., & Tonelli, R. (2018, October). An agile software engineering method to design blockchain applications. In *Proceedings of the 14th Central and Eastern European Software Engineering Conference Russia* (pp. 1-8).

Rocha, H., & Ducasse, S. (2018, May). Preliminary steps towards modeling blockchain oriented software. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (pp. 52-57).

Kombe, C., Manyilizu, M., &Mvuma, A. (2017). Design of land administration and title registration model based on blockchain technology.