EAI Endorsed Transactions
on Creative Technologies
Research Article EAI.EU

Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment

Muhammad Shoaib Akhtar, Tao Feng*

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

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. IoT devices can collect digital forensic evidence in an IoT setting, putting cybercrime agencies at danger owing to security and integrity. Many studies have been done recently to improve IoT 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 Blockchain and Hashing algorithms. We will store the data collected from IoT devices into Blockchain. 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: Blockchain, IoT Forensics,, DDOS, Machine Learning

Received on 12 February 2022, accepted on 03 June 2022, published on 03 June 2022

doi: 10.4108/eai.3-6-2022.174089

*Corresponding author. Email: febgt@lut.cn

1. Introduction

Digital forensics is the branch of forensics which deals with digital evidences. Detection, acquisition, processing, analysis, and reporting on data stored electronically is the subject of digital forensics. Digital forensics support is critical for law enforcement investigations since electronic evidence is present in nearly all illegal activity. Using digital forensics, it's possible to determine what information has been taken and how it was copied or disseminated. In order to do harm to their targets, some hackers may purposefully destroy data. In other circumstances, malicious software or hacker involvement can corrupt important data inadvertently.

Some challenges faced by digital forensics is the risk of security and integrity. Collection of digital forensic evidence can be done by IoT devices in an IoT environment, which may lead to high risk for cybercrime agencies due to security and integrity. Recently many studies has been done to improve the integrity and security of IoT based digital forensics but risk of confidentiality is the main issue faced by researchers [1].

Many researches has been done using Blockchain technology to ensure integrity and security of Digital forensics. In a study, [2] author stored data into Blockchain and converted these blocks into hot and cold Blockchain in order to make it more secure for criminal investigation. In this paper [3] author produced a temper resistance method for the security and integrity of evidences by using Blockchain technology.

In another study, [4] author proposed a model of BLOFF, Blockchain based forensics IoT model. It avoid tempered logs to enter into the evidence and made it secured. In this paper [5], author proposed cloud based Blockchain technology solutions for forensic evidences. In another paper, author [6] proposed a model of Blockchain for IoT based data collection system in social environment and social media. In this paper, [7] author proposed a solution in

the form of chains of custody to avoid data tampering in court and make it secure.

In paper [1] author proposed a model of Blockchain for IoT based data collection system in social environment and social media. By reviewing some research and related work it was found that tampering and security based challenges are still issues of recent times in digital forensics. So there is a need of an intelligence and effective model which not only ensure security and integrity but also predict attacks on early basis in order to provide early assistance to the system [8].

A secure IoT service provisioning mechanism became possible with the advent of Blockchain technology. The Internet of Things (IoT) connects electronic devices. The fast proliferation of IoT devices generates large volumes of data. This massive amount of data requires a decentralized data control method. Smartphones and tablet computers are growing more complex as intelligent technology advances. As more criminals utilize smart terminals to perpetrate crimes, a new field called "digital forensics" emerges to address the issue. To preserve the primordial nature of digital evidence, it must be easily made, saved, moved, used, and modified in forensic investigations. As a result, we must ensure the data is reliable. Data preservation techniques including cryptography, data hiding, digital signature, timestamp, and data digest have become more common as crime scene investigations have evolved. This has helped preserve judicial evidence both throughout the investigation and in court. It has also been used to protect sensitive data in cloud computing and wireless sensor networks. For example, storing evidence safely and securely away from the crime scene, and doing assessments and measurements without access to the crime scene. With more data preservation solutions available, performance and costs will improve. Industry standard data preservation technologies include data encryption and data digest. The author of an essay elaborates on the procedure. It is required to perform symmetric and asymmetric encryption and decryption, add timestamps in the data, and create a digest using the hash algorithm. Investigators can use the same procedures to establish if data utilized for judicial purposes has been manipulated. Despite its many benefits, data preservation has a fatal flaw. No one can guarantee that investigators will not make mistakes, whether on purpose or by accident. So the author visited with cops and data preservation experts to learn about practical data preservation procedures. Experts in both law and technology agree that data preservation must always maintain originality and integrity. It's also worth noting that no one can participate in the entire procedure.

Reviewing recent research and related studies revealed that tampering and security-related difficulties still exist in digital forensics. So a smart and effective model is required that not only ensures security and integrity but also predicts attacks in advance to aid the system. So we are proposing here an intelligent and effective system using Blockchain technology along with Hashing algorithm. After the collection of crime evidence from IoT devices we will store the data into Blockchain. At that time we will be using Machine Learning boosted models to predict the anomaly in the evidence and transactions. For this reason the proposed model is effective because it can predict the attacks on early basis.

This thesis consists of five sections. Section 1 consists of introduction background and problem statement. Section 2 consists of literature review and critical analysis. Section 3 is about proposed methodology. Section 4 is about results and implementation. Section 5 is the conclusion section of this thesis.

A. Research Questions

RQ1: Is it possible that the involvement of humans in digital forensics can help to improve the security of Blockchain?

RQ2: Is it possible that the Blockchain model for digital forensics solve the problem of data confusion

B. Research Objectives

Following are the objectives in this research:

To ensure the integrity of digital forensic evidence by using Blockchain method in IoT based environment

To show the security and effectiveness of the proposed model.

To evaluate the models on the basis of performance metrics

2. Literature Review

This section shows the basic review of previous Digital Forensics based attack detection in IoT environments.

Digital evidence is the focus of digital forensics, a subfield of forensics. In digital forensics, material stored electronically is detected, acquired, processed, analyzed, and reported on. Because of the prevalence of electronic evidence, digital forensics support is essential to law enforcement investigations. You can find out what information has been stolen and how it was copied or distributed using digital forensics. Some hackers may deliberately delete data in order to harm their targets. When malicious software or hacker activity is involved, valuable data can be corrupted unintentionally.

The integrity and security of digital forensics can be a problem. Security and integrity concerns for IoT devices put cybercrime agencies at risk while collecting digital forensic evidence. A major concern for academics working on IoT-based digital forensics is that the data they collect may be compromised due to lack of adequate safeguards against unauthorized access.

Digital forensics have been the subject of numerous studies utilizing Blockchain technology to ensure their own integrity and security. While conducting research (Hahn, 2010), it was discovered that this author had created a hot and cold Blockchain to better protect his data in the event of an investigation. With the help of Blockchain technology, the author of this work (Hamid Lone and Naaz Mir, 2017) developed a way for ensuring the security and integrity of evidence.

BLOFF is a Blockchain-based Forensics on the Internet of Things (IoT) concept described in another study (Agbedanu & Jurcut, 2021). It protected the evidence by keeping tempered logs out. A cloud-based Blockchain technology solution was offered in this research (Akhter et al., 2020). According to Nelson (2020), a model of Blockchain for IoT-based data collecting in social environments and social

media was proposed in another study (Nelson, 2020). Data tampering in court can be avoided through chains of custody, as the authors (Gopalan et al., 2019) recommend.
This research (Li et al., 2019) proposes a Blockchain model for a social environment and social media data gathering system based on Internet of Things (IoT). It was discovered that tampering and security-related concerns in digital forensics have not gone away in recent years. Because of this, there is a need for an intelligent and effective model that provides security and integrity while also predicting attacks in order to aid the system in its early stages.
As a result of the development of Blockchain technology, it is now possible to provide safe IoT services. Electronic gadgets are linked via the Internet of Things (IoT). Fast growth of Internet of Things (IoT) devices creates a lot of data. In order to handle this enormous volume of information, a decentralized approach is necessary. Intelligence-enhanced smartphones and tablet computers are becoming more and more complicated. A new area dubbed "digital forensics" is emerging to deal with the problem of criminals using smart terminals to commit crimes. Forensic investigators must be able to quickly create, save, move, use, and modify digital evidence in order to preserve its primal character.
It is imperative that the data is accurate as a result. More and more solutions for preserving evidence from a crime scene have emerged, such as digital signatures, cryptography, data concealing, timestamps, and data digests. Courtroom evidence has been preserved thanks in large part to this. It has also been utilised in cloud computing and wireless sensor networks to protect sensitive data. For example, storing evidence away from the crime scene and conducting assessments and measurements without access to the crime scene are examples of best practices. Performance and prices will improve as additional data preservation technologies become available. Data encryption and data digest are two of the most often used methods for preserving data in the industry. An essay's author explains the process in detail. Encryption must be performed in both directions and timestamps must be added to the data. The hash algorithm must also be used to construct a digest. The same approaches can be used by investigators to determine whether data used in court cases has been altered. There is a fatal fault in data preservation, despite the many advantages that it offers. Everyone knows that investigators can make mistakes on purpose or by accident, and no one can guarantee that they will not. As a result, the author spoke with police officers and data archivists to learn about real-world data preservation techniques. Both legal and technological experts agree that the originality and integrity of data must be preserved at all times. Additionally, it's important to point out that no one can take part in the full process.

2.1 Research Gap

According to recent research and investigations, tampering and security-related problems in digital forensics are still present. In order to keep the system safe and secure, it is necessary to have a model that is both effective and clever. As a result, we're putting forward a solution that makes use of both Blockchain and the Hashing algorithm. We will use Blockchain to store the crime evidence gathered via IoT devices. The abnormality in the evidence and transactions will be predicted using Machine Learning boosted models at that point in time. The proposed approach is hence effective because it can foretell attacks on a regular basis and early.
There are many phases that digital forensic artefacts go through before they can be used in court for prosecution. According to (Daniel & Daniel 2012), there are four steps in the digital forensic procedure. Identification, collection, organization, and presentation are the four steps involved in this procedure. A similar breakdown of the stages of digital forensics has been provided by (Zawoad et al., 2015). According to, scientific methods are employed to acquire, store, and present evidence (Hemdan & Manjaiah 2018). Ken Zatyko, the former head of the US Defense Computer Forensics Laboratory, has established an eight-step process for making digital forensics scientific (Zawoad et al., 2015). Obtaining search authority, documenting the chain of custody, imaging, and hashing of evidence, validating forensic tools, analyzing the evidence, repeating and reproducing to ensure quality assurance, reporting by documenting the forensic procedures, and finally, presenting an expert witness in a court of law are among the eight steps.
In this phase, evidence is gathered from a variety of sources. The original copy of the evidence may be imaged as part of the extraction process. Additionally, this stage entails protecting the integrity of the data.
In reality, the Blockchain is a decentralized database that provides Byzantine fault tolerance by distributing storage, consensus mechanism, peer-to-peer (p2p) network, encryption algorithm, etc. The decentralized and trust-free nature of Blockchain makes it possible for any capable node to join the network. In contrast, traditional centralized database management, for example, restricts access to the database to a single firm or administrator. In the Blockchain network, all nodes have equal access to the database, and all nodes work together to keep it running smoothly. There is a consensus mechanism in the Blockchain network that ensures that all nodes in the network are synchronizing their information with one other.
Blockchain is a decentralized and distributed ledger in which transactions are linked together by cryptographic hashes. Gaur et al. define "blockchain" as an immutable ledger for documenting transactions over a dispersed network of mutually untrustworthy peers (2018). Any transaction initiated by a node is validated by the other nodes in the blockchain network. In the case of bitcoin, after the transactions have been validated, they are added to the block by certain nodes known as miners. Miners are nodes with adequate computer power to solve a cryptographic challenge. In the Blockchain, peer-to-peer (P2P) networks are used. Each node in this architecture may connect with a set of nearby nodes, and then each of these neighboring nodes can communicate with one another.

The Blockchain is built such that any node can join or depart at any time. The development and application of blockchain technology necessitate several essential components. These are the components:

Time stamping

In cryptocurrency applications like bitcoin, double-spending is avoided by timestamping transactions. By initially gathering all pending transactions into the block, the block's hash is utilized to produce a timestamp. The fact that the transaction's hash is included in the block demonstrates that it existed at the time it was created.

Consensus

All nodes must agree on a single version since mining nodes generate and broadcast new blocks. There are several ways in which a distributed consensus might help determine which block will be added to the Blockchain.

Data Security and Integrity

Because each transaction is signed with the user's private key, this feature or attribute prohibits a hostile node from constructing a false one.

Digital forensics is the branch of forensics which deals with digital evidences. Detection, acquisition, processing, analysis, and reporting on data stored electronically is the subject of digital forensics. Digital forensics support is critical for law enforcement investigations since electronic evidence is present in nearly all illegal activity. Using digital forensics, it's possible to determine what information has been taken and how it was copied or disseminated. In order to do harm to their targets, some hackers may purposefully destroy data. In other circumstances, malicious software or hacker involvement can corrupt important data inadvertently.

Some challenges faced by digital forensics is the risk of security and integrity. Collection of digital forensic evidence can be done by IoT devices in an IoT environment, which may lead to high risk for cybercrime agencies due to security and integrity. Recently many studies has been done to improve the integrity and security of IoT based digital forensics but risk of confidentiality is the main issue faced by researchers.

Many researches has been done using Blockchain technology to ensure integrity and security of Digital forensics. In a study, [2] author stored data into Blockchain and converted these blocks into hot and cold Blockchain in order to make it more secure for criminal investigation. In this paper [3] author produced a temper resistance method for the security and integrity of evidences by using Blockchain technology.

In another study, [4] author proposed a model of BLOFF, Blockchain based forensics IoT model. It avoid tempered logs to enter into the evidence and made it secured. In this paper [5], author proposed cloud based Blockchain technology solutions for forensic evidences. In another paper, author [6] proposed a model of Blockchain for IoT based data collection system in social environment and social media. In this paper, [7] author proposed a solution in the form of chains of custody to avoid data tampering in court and make it secure.

In paper [1] author proposed a model of Blockchain for IoT based data collection system in social environment and social media. By reviewing some research and related work it was found that tampering and security based challenges are still issues of recent times in digital forensics. So there is a need of an intelligence and effective model which not only ensure security and integrity but also predict attacks on early basis in order to provide early assistance to the system.

A secure IoT service provisioning mechanism became possible with the advent of Blockchain technology. The Internet of Things (IoT) connects electronic devices. The fast proliferation of IoT devices generates large volumes of data. This massive amount of data requires a decentralized data control method. Smartphones and tablet computers are growing more complex as intelligent technology advances. As more criminals utilize smart terminals to perpetrate crimes, a new field called "digital forensics" emerges to address the issue. To preserve the primordial nature of digital evidence, it must be easily made, saved, moved, used, and modified in forensic investigations. As a result, we must ensure the data is reliable. Data preservation techniques including cryptography, data hiding, digital signature, timestamp, and data digest have become more common as crime scene investigations have evolved. This has helped preserve judicial evidence both throughout the investigation and in court. It has also been used to protect sensitive data in cloud computing and wireless sensor networks. For example, storing evidence safely and securely away from the crime scene, and doing assessments and measurements without access to the crime scene. With more data preservation solutions available, performance and costs will improve. Industry standard data preservation technologies include data encryption and data digest. The author of an essay elaborates on the procedure. It is required to perform symmetric and asymmetric encryption and decryption, add timestamps in the data, and create a digest using the hash algorithm. Investigators can use the same procedures to establish if data utilized for judicial purposes has been manipulated. Despite its many benefits, data preservation has a fatal flaw. No one can guarantee that investigators will not make mistakes, whether on purpose or by accident. So the author visited with cops and data preservation experts to learn about practical data preservation procedures. Experts in both law and technology agree that data preservation must always maintain originality and integrity. It's also worth noting that no one can participate in the entire procedure.

Reviewing recent research and related studies revealed that tampering and security-related difficulties still exist in digital forensics. So a smart and effective model is required that not only ensures security and integrity but also predicts attacks in advance to aid the system. So we are proposing here an intelligent and effective system using Blockchain technology along with Hashing algorithm. After the collection of crime evidence from IoT devices we will store the data into Blockchain. At that time we will be using Machine Learning boosted models to predict the anomaly in the evidence and transactions. For this reason the proposed model is effective because it can predict the attacks on early basis.

Currently, we live in an era where the Internet of Things is a reality (IoT). Because of recent breakthroughs in hardware and information technology, In important infrastructures like as health care, transportation, environmental management, and home automation, there are now billions of networked, smart, and adaptable devices. Hackers have a new universe of possibilities when they use a network to send data without any human-to-computer or human-to-human connection. It does, however, create a new set of difficult issues for digital forensics specialists.

When working with IoT data, forensics professionals encounter numerous problems. There are multiple IoT devices and non-standard formats to deal with, as well as a multi-tenant cloud architecture and the resulting multi-jurisdictional litigation. End-to-end encryption also poses a dilemma because it compromises the privacy rights of users while also making forensics investigations more difficult. Digital evidence must be collected and analyzed using established methods and methodologies in order to maintain the Chain of Custody due to its volatile nature.

Consequently, the goal of this article is to identify and address the most pressing legal, privacy, and cloud security issues that arise during IoT-based investigations. It also provides an overview of theoretical concepts in digital forensics science from the past and the present. Using decentralized Blockchain-based solutions, data extraction and evidence integrity are given special emphasis in frameworks [9]. Forensics as a service and cross-cutting data reduction and forensic intelligence methodologies are also addressed in this study, as is the current FaaS paradigm. Other research trends and unresolved challenges, including the necessity for proactive Forensics Readiness programmes and generally accepted standards, are also discussed.

Using Blockchain and cryptography group signature technologies, this study [10] suggested a process provenance that proves the presence of process records while maintaining their anonymity. For cloud forensics, the provenance of the process strengthens the trustworthiness of the chain of custody.

This paper [11] presents an IoT forensic chain (IoTFC) that may provide the forensic investigation with good authenticity, immutability and traceability, robustness and distributed trust between evident and examiners. Evidence objects can be traced, and provenance tracked using the IoTFC. Chains of blocks will record evidence identification, preservation, analysis, and presentation. Transparency of the audit train is one way the IoTFC may promote trust in evidence items and examiners. The recommended method was proven to be effective in the use case.

A paper [5] discussed cloud storage forensics research and how it compares to distributed cloud forensics based on block chains. Modern technology poses several issues and methods when it comes to forensic investigations. In addition, we take a look at what the future holds for solving these problems.

Using blockchain technology, this article [12] fills in this gap by providing a safe and transparent digital forensic investigative procedure. As part of a Blockchain Hyperledger sawtooth enabled novel, secure, and efficient digital investigation architecture MF-Ledger, participants create a private network where they can communicate with each other and agree on different investigation activities before they are stored on the blockchain ledger. Using sequence diagrams, we have designed digital contracts (smart contracts) to handle the secure interaction of stakeholders in the investigative process. Using a private, permissioned encrypted blockchain ledger, the suggested architectural solution provides solid information integrity, prevention, and preservation mechanism to keep the evidence (chain of custody).

Images are a crucial aspect of investigations to gather information, document, and build a "memory" of a crime scene [13]. Therefore, the validity and verifiability of crime scene photos must be maintained to use them as evidence in court. Crime scene photographs can be doctored with ease thanks to advances in technology in our digitally dominated day. To authenticate or validate digital content or documents, digital watermarking and Blockchain have been employed previously. It is proposed in this study that forensic crime scene photographs can be authenticated using watermarking and cryptographic Blockchain.

In light of the rapid advancement of technology, cyber-threats have grown to be a significant problem requiring immediate and ongoing attention [14]. Governments, corporations, and individuals continuously battle to keep their assets safe from cybercrime, which offers a continual and growing threat. Identity theft, fraud, and system hacking are all forms of cybercrime. Deception and fraud thrive in cyberspace because of the low entrance barriers, anonymity of users, and physical and temporal separation of users. It is possible to detect fraudulent transactions and activities that differ from normal behaviour patterns using a variety of techniques, both supervised and unsupervised. Neural networks and genetic algorithms, for example, were employed to detect credit card fraud in a dataset of 13 months and 50 million transactions. The use of unsupervised approaches such as clustering analysis has successfully detected financial fraud and filtered out fraudulent online product reviews and ratings on e-commerce platforms. E-commerce has shown that blockchain technology is viable and useful. When it comes to electronic government, it is presently being used in various ways.

Despite the many advantages of global network setup and control, Software Defined Networking (SDN) can also pose problems for digital forensics and cybersecurity investigations. A variety of weaknesses in this paradigm, such as the controller and the Northbound and Southbound interfaces, are being exploited in attacks of this nature. Developing tools for digital forensics in SDN, in addition to solutions to improve network security, is a necessary step in SDN implementation. Features that locate, collect and analyze log files together with extensive information about network traffic should be included. On the other hand, hackers can alter or even destroy log files once they have gained access to a machine or device. Storing log data in a secure location with fine-grained access control is essential for digital forensics purposes and cybersecurity. For network forensics, this paper [15] presents a blockchain-

based technique to increase log management security in SDN using SDNLog-Foren. In addition, this approach is tested in various trials to show that it may assist enterprises in securely storing important log data from their network system even if SDN components are compromised.

A permissioned blockchain-based IoT forensics architecture based on blockchain technology is presented in this study [16] to improve the evidence's integrity, validity, and non-repudiation. A cryptographic-based technique is proposed to address concerns about identity privacy in the system's architecture.

Packets are rerouted from overworked switches to other nearby switches to maintain a steady traffic flow. Switches will reject packets that do not follow flow rules. In this forensic architecture [17], the blockchain-based distributed controller uses the Linear Homomorphic Signature (LHS) algorithm to verify users. Using Neuro Multi-fuzzy, each controller provides a classifier to classify harmful packets. An SDN-IoT architecture uses blockchain technology to store event records. Forensic architectural performance was examined and compared to the old model utilizing several performance metrics. An increase in throughput and accuracy and a decrease in response time were found to be the most significant factors in our evaluation results.

Using a location-based and certified device with a pre-shared secret wireless communication scheme is necessary in this case to meet legal requirements, which ensure that digital evidence is safely stored on a blockchain and that the uploading device is authenticated by the relevant legal department [18].

Throughout today's digital era, data is the most critical asset. Every application requires secure data storage and processing. Due to the danger of tampering, data must be tamper-resistant. Heterogeneous formats can be used to store and portray data. Hackers could target information that is critical to a specific company. Data is being tampered with by cyber criminals due to the significant rise in cybercrime.

On the other hand, forensic evidence is suffering greatly as a result. As a result, digital evidence must be kept trustworthy and traceable throughout a forensic inquiry. The report goes via many tiers or intermediates such as the pathology laboratory and doctors and police departments. Blockchain technology is better suited to creating a transparent and immutable system. Thanks to blockchain technology, an asset or evidence report can be exchanged in a transparent setting with no central authority. Forensic evidence can be protected by using a blockchain-based system, as advocated in this study [19]. An Ethereum implementation of the suggested system has been made available. At any point in the forensic chain, the tampering of forensic evidence can be easily traced. The installation of forensic evidence on the Ethereum platform with high integrity, traceability, and immutability enhances the protection of the evidence.

Patients are constantly monitored and treated thanks to the Internet of Medical Things (IoMT). Many factors make these services vulnerable and susceptible to exploitation: the interplay between doctors and patients, healthcare providers, and the producers of medical devices. Access control can be difficult since parties may need different levels of access and the IoMT devices have a variety of functions. A distributed chain of custody and health data privacy strategy for managing IoMT devices and medical information is presented in this research [20]. The central idea is to create trust domains for various stakeholders and IoMT devices so that fine-grain access is enabled by taking into account critical IoMT ecosystem attributes such as a) the various roles and capabilities of IoMT devices and b) their interaction with users/stakeholders. Integrity and provenance assurances and the privacy of health data can be achieved via a forensics-by-design management architecture built around on-chain smart contracts. A proof-of-medical-stake consensus mechanism authenticates the private blockchain ecosystem for medical applications.

Forensic science relies heavily on evidence handling. Crime scene evidence is critical to solving the case and ensuring justice is served to the parties. As a result, the preservation of these evidences is of the utmost importance. An evidence chain of custody is the procedure that ensures the integrity of a piece of evidence is preserved. The evidence will be inadmissible in court if the chain of custody is broken, which would finally lead to the case being dismissed. As an environmentally benign model, digitalization of forensic evidence management systems is necessary. Digitally distributed ledgers of cryptographic signatures in chronological order that are grouped into blocks in the blockchain network are known as blockchains. Blockchain framework Hyperledger Fabric was developed by the Linux Foundation and is primarily utilized by corporations. The purpose of [21] study was to design a framework and further propose an algorithm to utilize Blockchain Technology to digitalize the forensic evidence management system and preserve the Chain of Custody, based on the concept of Hyperledger Fabric.

IoT security challenges and whether or not Blockchain is a feasible solution are examined in this research. By conducting experiments, [22] examine whether blockchain technology can be used to safeguard IoT devices by ensuring the validity and integrity of their transactions, as well as the feasibility of leveraging immutable transactions for forensic analysis in an IoT device mesh network.

About digital forensics, this article [23] examines the construction and production of InnoDB-indices, as well as the navigation inside this internal structure. An understanding of the index's internal workings can be used to detect modifications on the underlying table space. To further understand B+-tree forensics, we examine the index pages' physical and conceptual structure. We've developed a real-world forensic technique for an open source database system for the first time. In addition, [23] address many forensic investigation use cases and future additions to the field of file system forensics, using the indicated methodology.

Transactions on Blockchain systems, particularly enterprise Blockchain platforms, require the production of multiple signatures from a group of peers to support a digital signature as a major component. However, this can be a lengthy and time-consuming process. Many people are interested in multi-signature, which can increase transaction efficiency by having a group of signers work together to establish a combined signature. This paper [24] proposes two new multi-signature schemes, GMS and AGMS that are

more secure and efficient than existing multi-signature methods. In addition, we use Fabric, a real-world Enterprise Blockchain platform, to put the ideas into action. In experiments, the suggested AGMS system helps meet the goal of high transaction efficiency, low storage complexity, and strong robustness against rogue-key attacks and k-sum problems.

Data held in various database management systems is always vulnerable to alteration, either inside or outside the system. There are many ways to determine if the database has been tampered with. Using one-way cryptographic hash functions and digital watermarking to identify data tampering was a key breakthrough in this domain [25]. Distributed databases are not compatible with these strategies. A Distributed Database can be used to store data, and Blockchain technology can be used to quickly identify any suspicious transactions. It's just a digital ledger that's tied together through cryptography.

A top-down organizational control perspective is used in this position paper [26] to develop an initial taxonomy for an accountability-based strategy that seeks to improve both compliance and forensic readiness. As progress towards distributed architectures like blockchain technology, [26]discover that compliance and forensic readiness may become even more challenging to achieve. An accountability-based approach will be critical to the overall acceptability of the solution, which we conclude is the case in this study paper.

There are new sorts of cyber-attacks utilizing the complexity and heterogeneity of IoT networks, as well as, the many vulnerabilities in IoT devices brought on by the technological progress of the Internet of Things It's becoming increasingly important to monitor IoT devices for signs of tampering and to collect and store evidence related to alleged harmful behavior. In this study [27], a blockchain-based solution for the collecting and storing digital forensic evidence is presented for the smart home domain. To ensure the integrity, authentication, and non-repudiation of evidence in a court of law, the system uses a private forensic evidence database and a permissioned blockchain that provides these services. Smart contracts allow the Blockchain to communicate with Internet service providers, law enforcement agencies, prosecutors, and other parties involved in an investigation. The Blockchain maintains evidentiary metadata that is crucial to providing the services above. IoT network forensic evidence must be digitally handled uniquely, and this requires a high-level architecture for the blockchain-based solution.

As the number of Internet of Things (IoT) devices grows, so will the number of assaults on such devices. Criminals can make use of Internet of Things (IoT) gadgets. It is why [28] have developed Probe-IoT, a public digital ledger-based forensic investigation platform for IoT-based criminal situations. There is a similarity to the Bitcoin network. Probe-IoT uses blockchain technology to preserve evidence of interactions between various IoT entities (such as cloud providers and IoT devices) as transactions. Using Probe-IoT, you may rest assured that any evidence saved in the public ledger is secure, secret, anonymous, and unrepudiated. Probe-IoT also provides a means to obtain evidence from the ledger and verify the validity and integrity of the evidence collected. As a result of this research [29], a taxonomy model based on Blockchain analytical tools is presented. It also looks at the future development and research difficulties still present.

Cloud-based data provenance utilizing Blockchain is presented in this paper [30], which tracks and generates provenance data for each record, begin by creating a drop box-like application utilizing AWS S3 storage. This application creates a cloud storage application for students and teachers of the institution; hence, work and resources can be easily stored and shared. In the future, a data provenance system for user's confidential files using the Ethereum Blockchain has been created.

This project [31] tries to address the issue of manipulating "large" photographs up to gig pixels in size. In many cases, the successive elaboration of these images is difficult. In many academic fields, such as forensics or medical analysis, this is a common problem and there are few known answers. A distributed ledger and Smart Contracts system will be developed in this project so that super resolution photos can be manipulated in a decentralized and competitive fashion. As a result of the Blockchain infrastructure, the suggested solution is very dependable and secure. Demographic data has been used to test a proposed solution to this problem.

The total quantity of digital media works published has increased steadily. Digital copyright infringement has become increasingly significant because of how digital copyright works can be copied and distributed. Research on copyright protection based on blockchain technology has been a prominent research direction for many scholars because of blockchain technology's security, traceability, distribution, and programmability properties. Details on the ideas and properties of Blockchain technology are presented in this article [32]. The research state, essential technologies, and research challenges of copyright protection technology are also examined in depth. Additionally, this article has done extensive research on the copyright protection technology based on the Blockchain to implement an effective yet secure and light-weight alliance chain copyright protection system.

A system supports proactive insider threat detection to track object behavior in Smart Controlled Business Environments (SCBE). Some of the framework's components were tested at a company to demonstrate anomaly detection and the formation of behavioral patterns based on the movement of items about their job role, workspace position, and the nearest entry or exit to their workplace. Proximity Monitoring Solution was used to get the empirical data. Forensic-readiness is achieved by the establishment of a digital Chain-of-Custody (CoC), as well as a collaborative environment for CPS to qualify as Digital Witnesses (DW) to support post-incident investigations [33].

This article examines the use of Blockchain technology to verify the integrity of digital forensic evidence [34]. A brief introduction to digital forensics and blockchain technology provides context. Verifying digital evidence when it was created is made easier by using Open Timestamps (OTS)

service, and testing is carried out to verify the service's assertions. However, due to variations in the accuracy of timestamps caused by Bitcoin blockchain block confirmation times, the results show that the OTS service is not suitable for time-sensitive timestamping despite its high reliability and zero false positive or false negative error rate for timestamp attestations.

IoT is a network of devices that can be remotely controlled and monitored. Even though IoT gadgets have improved our quality of life, they are often insecure. IoT devices are easy targets for hackers due to a lack of reliable key management systems, effective identity authentication, and low fault tolerance. By enhancing an authentication protocol for IoT devices and CPANs, the researchers [35] want to improve the industrial internet of things' authentication process. On the basis of this investigation, we have come up with a solution for this problem and determined the most effective contribution. Based on the evaluation, BCTrust, a Blockchain-based solution, was judged to be the best option. The goal of this work is to make improvements to BCTrust's base authentication protocol. It is primarily aimed at removing the blacklisting method, which can be used by attackers to severely damage the network, as well as enhancing other aspects of the protocol. For the second time, the IIoT devices will be identified by using an entirely new method. An improved BCTrust would be able to generate IIoT secret keys more quickly and securely.

In this work, [36] examine puncturable signatures and examine their use in the proof-of-stake Blockchain. There is an adversary who can make adaptive signing and puncturing queries and we show an efficient puncturing operation using the Bloom filter data structure and a strong Diffie-Hellman assumption in our formalization of the security model Instead of puncturing the entire message, we want to be able to do so for a specific section of it, such the prefix. Puncturable signatures are used to build viable proof of stake Blockchain protocols resistant to the LRSL attack. In contrast, the forward-secure signature was previously used to protect against this attack. It is demonstrated experimentally that our design outperforms the forward-secure signature in terms of the size, signing and verification efficiencies, and key update efficiencies compared to the forward-secure signature. Table below shows the comparative analysis of previous researches in a tabular form:

Table 1. comparative analysis of previous researches in a tabular form

Reference	Technique	Outcome
[36]	Blockchain	signatures and examine their use in the proof-of-stake Blockchain
[35]	Blockchain and IoT	Enhancement an authentication protocol for IoT devices and CPANs
[34].	Blockchain and IoT	examines the use of Blockchain technology to verify the integrity of digital forensic evidence
[33]	Security Detection using BTC	Forensic-readiness is achieved by the establishment of a digital Chain-of-Custody (CoC), as well as a collaborative environment for CPS to qualify as Digital Witnesses (DW) to support post-incident investigations

3. Methodology

Data collection and processing services for AI learning data are becoming increasingly important as their importance grows; research into the confluence of blockchain and AI has lately been initiated. AI data and blockchain are linked in this part, which introduces relevant research on the basis of this research's suggested AI learning data environment model. IoT nodes are becoming a goldmine for hostile actors since they are gathering and storing private information. Detecting compromised nodes, as well as capturing and archiving evidence of an attack or malicious activity, has emerged as a top priority for effective IoT network implementation. In this study we are using machine learning models to predict the malicious attacks on the blockchain based IoT forensics dataset to ensure the integrity and security of the dataset.

A. Proposed Framework

Algorithms, computing systems, and data learning are all intertwined in many types of AI technology, such as deep learning in particular. There must be an adequate dataset in place for AI learning in order to construct an AI model with a certain feature. Figure 1 depicts the AI machine learning process based on IoT integrity with Blockchains.

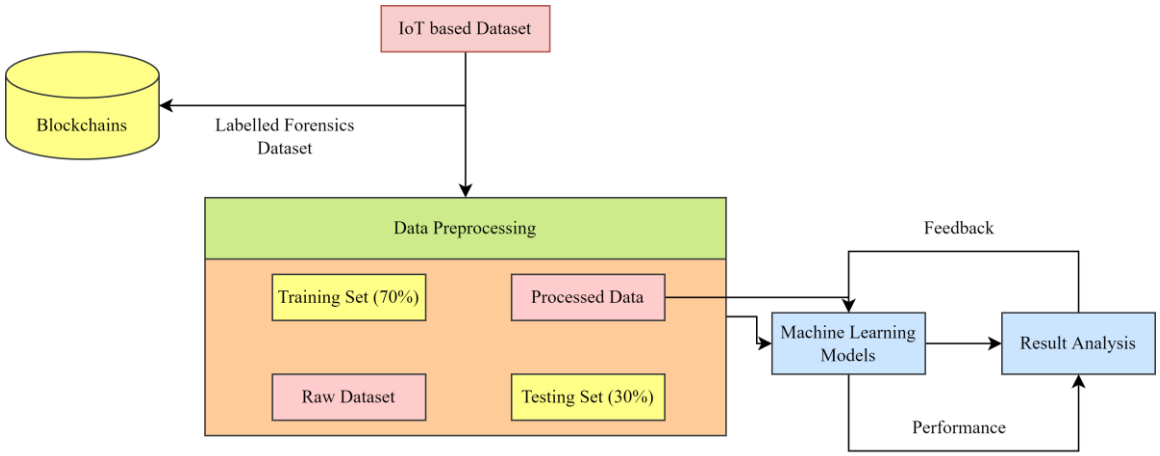

Figure 1. Proposed Framework

B. Data Collection

Non-structured data in the form of numeric can be gathered at this stage. Extracting data that is suitable for the aims and functionalities of the AI being built is the first step in preprocessing. Malicious third parties have increasingly attacked Internet of Things (IoT) technologies due to their widespread use. Countermeasures, such as network intrusion detection systems, must be developed in order to successfully handle this threat. Having a well-structured and representative dataset is essential for training and verifying the trustworthiness of the algorithms.

Despite the fact that many network datasets are available, nothing is known about the Botnet scenarios that were employed. Bot-IoT is a novel dataset proposed in this research that includes real and simulated Internet of Things (IoT) network traffic, as well as a variety of attacks on that traffic.

A realistic testbed environment is also shown to address the existing dataset's shortcomings of capturing entire network information, correct labelling as well as complicated attacks. Finally, we compare the reliability of the BoT-IoT dataset to the benchmark datasets using several statistical and machine learning methodologies. Keeping data up-to-date and fresh while keeping a record of its history is easier and more secure using blockchain technology. No one can alter or destroy the data, and you get both a history of data and a current record that is always up to date.

C. IoT based Digital Forensics Dataset

The BoT-IoT dataset was built in the Cyber Range Lab of UNSW Canberra by designing a realistic network environment. Normal and botnet traffic were both present on the network. Source files for this dataset are available in many formats, including the original pcap files, as well as generated Argus files. To aid in the labelling process, the files were categorized by attack category and subcategory.

With more than 72,000,000 records, the files are about 70 GB in size. In csv format, the extracted flow traffic is 16.7 GB. According to the protocols employed in the assaults, the dataset comprises DDoS (DDoS), DoS (DoS), OS and Service Scan, Keylogging, and Data Exfiltration. For the sake of convenience, we used select MySQL queries to remove 5% of the dataset. The extracted 5% consists of four files with a total size of 1.07 GB and a total of around 3 million records.

D. Data Storage in Blockchain

The smartest way to store data is to store the data's hash on the blockchain. Using our data as input, we construct a hash code. The cost is cheap since the hash of the data is low. A file system can also be used to store raw data. The decentralized technology of blockchain represents the answer to old centralized institutions, such as financial institutions. A digital, central "authority" is established on a blockchain network by combining machine learning capabilities. The blockchain serves as a means for distributing data to everyone with an app that can access it. Unrestricted ('permission less') or restricted ('permitted') access to this ledger is possible in terms of reading and writing. A major need for a machine learning model to be accurate is that the data it uses has no missing values, duplicates, or noise, which is why the data is stored on a blockchain network. The digital signature is generated using a cryptographic hash function for each unique block. Hash functions come in a wide range.

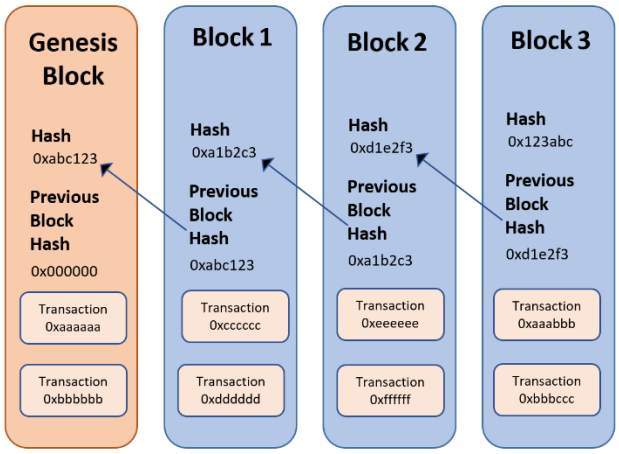

Figure 2. Blockchain and Hashing Architecture

E. Cryptography in Blockchain

Cryptography entails the use of code that can only be decoded by a specific group of people. There are procedures in place for node communication and the validation of new blocks that are adhered to by the network. In order to record a transaction on the blockchain, miners verify it. Algorithms must be used to validate and retrieve data during mining. It is a digital currency that uses encryption to regulate and generate money units. Using cryptography for security and blockchain technology to record transactions, cryptocurrencies are secure and decentralized. A blockchain algorithm refers to the entire process of building a record chain and validating transactions the same conclusion can be drawn by all nodes, each updating the record in its own unique way. Every node builds its own updated version of events and broadcasts the transactions. A third-party intermediary is no longer necessary because of blockchain technology's innovation in data recording and delivery.

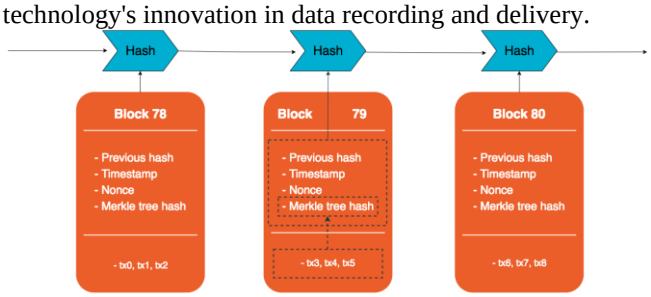

Figure 3. Cryptography in Blockchain

There are many innovative methods to use blockchain technology, which combines a variety of technologies. On a peer-to-peer-network, it is a system of record and uses private key cryptography for identity. The platform is developed using protocols. A protocol includes an algorithm. In the end, there is no need for a trusted third party in the system of transactional interactions the robust, simple, and smart network architecture of blockchain technology provides the means for securing digital interactions.

F. Secured and Privacy Preserving

To protect patient information, the suggested model makes use of a lightweight public-key cryptosystem, namely an identity-based cryptosystem based on the elliptic curve cryptosystem. The public key of the recipient is not required to be verified by the IBC. In terms of processing overhead, ECC-based arithmetic is roughly 20 times faster than modular exponentiation. In addition, the 128-bit ECC key is as secure as a 1024-bit RSA key in terms of bit length. IoT applications can benefit from the unique properties of IBC and ECC.

G. Proposed Blockchain Model

Since blockchain nodes might be located all over the world but have equal access to the application, it is up to P2P networks to make sure that communication between nodes is unrestricted. The P2P network does not have a central server, and each node is both an informed user and a provider of information. Every node is involved in the network's routing process, which includes establishing and maintaining connections with other nodes, propagating and validating transactions, and synchronizing data blocks. Each node (both transactions and blocks are data structures of the blockchain, as described below). Decentralization and the flat topology of peer-to-peer networks are exemplified by this. APIs (application programming interfaces) are provided by blockchain apps in a variety of circumstances. Through these APIs, users can communicate directly with them without having to be concerned with the underlying technological aspects.

H. Cloud Based Blockchain

Central databases are heavily used to store data safely. However, hackers are more focused. A script attack on a central database is one of the most popular ways hackers get access to large volumes of data. However, blockchain and distributed ledger technology make cracking much more difficult. Many blockchain projects aim to increase data storage security. This might be a game changer for users. While the blockchain initiative may lead to more secure data storage methods, it also gives people unfettered access to their data. Several blockchain projects use the original cryptocurrency as a markup. Apart from preventing identity theft and other issues raised by recent large-scale data breaches, this also allows users to monetize third-party data. Digital signatures ensure the message's integrity and non-repudiation in blockchain transactions.

I. Data Preprocessing

Filling in or eliminating missing data values, selecting or deleting data properties, and combining existing data properties are all examples of data preprocessing in this stage of the machine learning model creation process.

As a result of this stage's data analysis, artificial intelligence (AI) can make use of data patterns found in conventional datasets, as well as information gleaned through exploration and inference.

AI algorithms can't use raw data because it contains some noise, lacks a consistent structure and is frequently re-examined. Quality, reliability, correctness, and performance must be ensured by a stage in which professional data analysis and organization are undertaken; at this stage, errors in data are corrected, overlapping data is eliminated, and inconsistent data is deleted. 80 percent of the procedure is spent preprocessing data. Quality assurance is essential for the development of AI, and a significant volume of high-quality data is necessary.

4. Results

This section shows the implementation of Blockchain technology on digital forensics and ensure the security of each transactional database by using Machine Learning algorithms i.e. XGBoost Algorithm and KMEANS Clustering.

A. Communication vs Security Level

Signcryption adds a significant amount of overhead to communications. The size of the signed message is the primary factor in determining the transmission overhead. Each user only needs two bytes in a conventional network. On the other hand, communication overhead and security

levels are shown in Figure below. There is an increase in communication overhead as security levels rise.

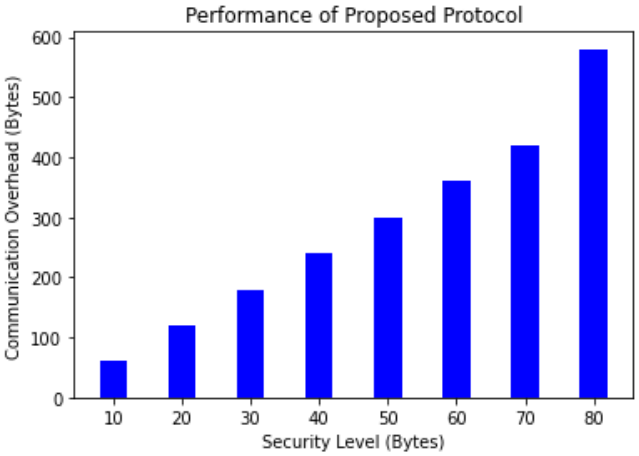

Figure 4. Performance of Proposed Protocol

B. Blockchain Performance

The proposed blockchain-enabled platform was tested in this part in terms of block size, read throughput, transaction throughput, read latency and transaction latency to validate its performance. One ordered node and four peer nodes were selected as experimental parameters for the blockchain network's performance evaluation. We calculated throughput by altering the TPS send rate in the proposed blockchain-enabled platform.

Transactional throughput and read throughput are two examples of how throughput can be divided. The number of transactions initiated in the blockchain network during the allotted time window was specified as the transaction throughput. Read-through was used to measure the reads operation on the blockchain network during the allotted time window. Variations in TPS send and random machine utilization configuration were used to gauge transaction read throughput.

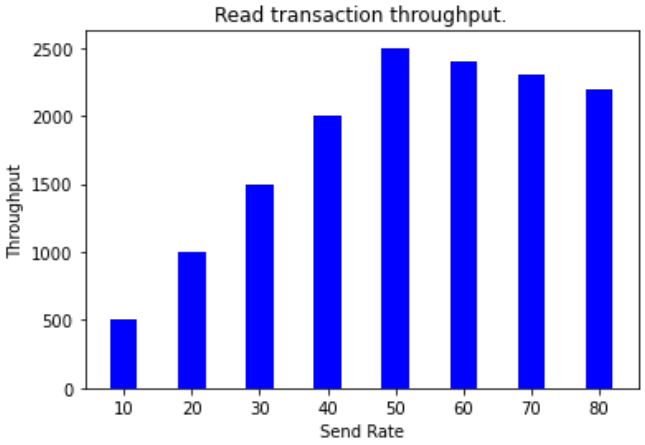

Figure 5. Read Transaction Throughout

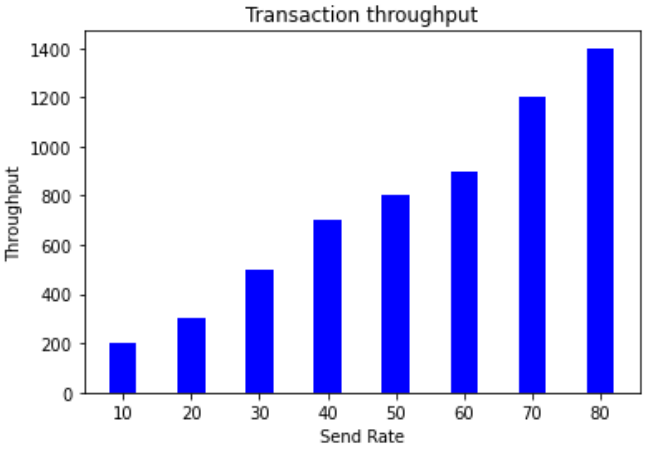

Figure 6. Transaction Throughout

Performance of Machine Learning Models for Security Prediction

In the first step we have visualize the cluster of harmful attacks. Figure below shows the cluster of two different types of Attacks.

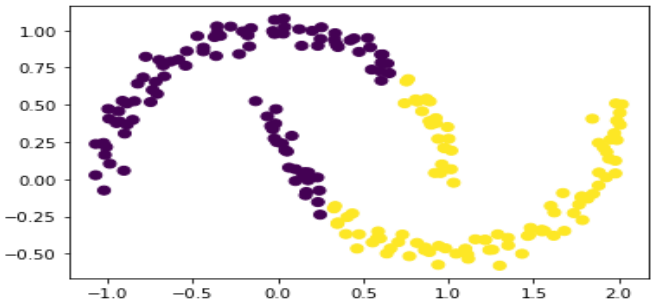

Figure 7. Visualization of Clusters

For the prediction of early time attack we have used XGBoost algorithm. In the figure below, performance of XGBoost has been shown for the prediction of attacks in early stages in order to ensure security and integrity of system, XGBoost has shown accuracy of 99.8%, 95% and 79% for early prediction of attacks in orders data, accounts data and transactional data respectively. While KMEANS has shown the confidence clustering with the accuracy of 98%, 58% and 59% for each data respectively.

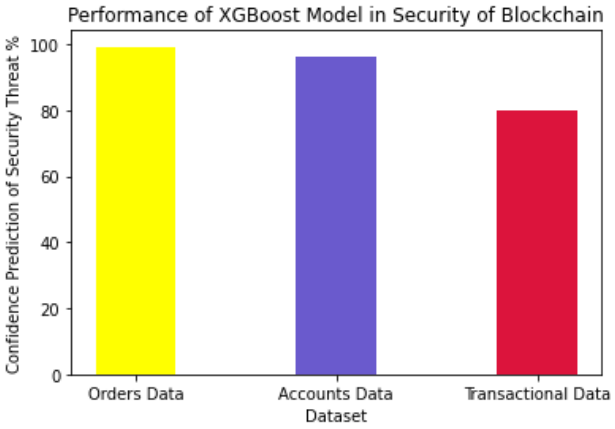

Figure 8. Performance of XGBoost in securing the blockchain

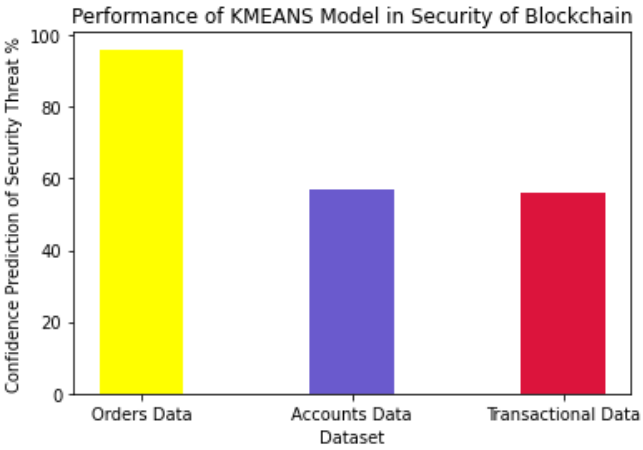

Figure 9. Performance of KMEANS model in securing the blockchain

5. Conclusions

Digital forensics is a branch of forensics that is concerned with the investigation of digital evidence. Digital forensics is concerned with the detection, acquisition, processing, analysis, and reporting of material that has been saved in an electronic format. When it comes to law enforcement investigations, digital forensics assistance is essential because electronic evidence can be found in nearly all instances of unlawful behavior. It is feasible to discover what information has been taken and how it has been duplicated or disseminated by using digital forensics techniques. It is possible that some hackers will purposely destroy data in order to cause harm to their targets. In other cases, malicious software or hacker activity might cause crucial data to be corrupted without the user's knowledge. One of the difficulties that digital forensics must deal with is the threat to security and integrity. It is possible for IoT devices to collect digital forensic evidence in an IoT environment, which may pose a significant risk for cybercrime agencies due to concerns about security and integrity of the data collected. The integrity and security of Internet of Things (IoT) based digital forensics have recently been the subject of numerous studies, but confidentiality is the most significant issue that researchers are dealing with. Recent research and related investigations demonstrated that tampering and security-related issues continue to persist in digital forensics, despite advances in technology. Consequently, a smart and effective model is necessary that not only maintains security and integrity, but also predicts threats in advance to aid the system in its operation. We are presenting a system that is both intelligent and effective, which makes use of Blockchain technology in conjunction with the Hashing algorithm. Following the acquisition of crime evidence through Internet of Things devices, the data will be stored in a Blockchain. During that time period, we will be employing Machine Learning boosted models in order to predict anomalies in the evidence and transactions. The proposed model is effective as a result of its ability to detect and forecast attacks on an early enough basis. The XGBoost algorithm was used to forecast an early time attack, which was successful. Figure 1 illustrates the performance of XGBoost in terms of early attack detection in order to maintain system security and integrity. XGBoost has demonstrated accuracy in terms of early attack detection in orders data, accounts data, and transactional data of 99.8%, 95%, and 79 percent, respectively for the early prediction of attacks in the three different types of data. Meanwhile, KMEANS has demonstrated the accuracy of confidence clustering with 98 percent, 58 percent, and 59 percent for each data set, according to the results.

References

[1] S. Li, T. Qin, and G. Min, “Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems,” IEEE Trans. Comput. Soc. Syst., vol. 6, no. 6, pp. 1433–1441, 2019, doi: 10.1109/TCSS.2019.2927431.

[2] S. Hahn, “Evidence management,” Forensic Dent. Second Ed., pp. 395–404, 2010, doi: 10.4324/9780429292767-22.

[3] A. Hamid Lone and R. Naaz Mir, “Forensic-Chain: Ethereum Blockchain Based Digital Forensics Chain of Custody,” Sci. Pract. Cyber Secur. J., vol. 1, no. 2, pp. 2587–4667, 2017.

[4] P. Agbedanu and A. D. Jurcut, “BLOFF: A Blockchain-Based Forensic Model in IoT,” Revolut. Appl. Blockchain-Enabled Priv. Access Control, pp. 59–73, 2021.

[5] J. Ricci, I. Baggili, and F. Breitinger, “Blockchain-Based Distributed Cloud Storage Digital Forensics: Where’s the Beef?,” IEEE Secur. Priv., vol. 17, no. 1, pp. 34–42, 2019, doi: 10.1109/MSEC.2018.2875877.

[6] S. M. E. Nelson, “Blockchain based Digital Forensics Investigation Framework in the Internet of Things and Social Systems,” vol. 8, no. 12, pp. 104–108, 2020.

[7] S. H. Gopalan, S. A. Suba, C. Ashmithashree, A. Gayathri, and V. Jebin Andrews, “Digital forensics using blockchain,” Int. J. Recent Technol. Eng., vol. 8, no. 2 Special Issue 11, pp. 182–184, 2019, doi: 10.35940/ijrte.B1030.0982S1119.

[8] A. Kim, M. Park, and D. H. Lee, “AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection,”

IEEE Access, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.

[9] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.

[10] Y. Zhang, S. Wu, B. Jin, and J. Du, "A blockchain-based process provenance for cloud forensics," 2017 3rd IEEE Int. Conf. Comput. Commun. ICCC 2017, vol. 2018-Janua, pp. 2470–2473, 2018, doi: 10.1109/CompComm.2017.8322979.

[11] S. Li, T. Qin, and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems," IEEE Trans. Comput. Soc. Syst., vol. 6, no. 6, pp. 1433–1441, 2019, doi: 10.1109/TCSS.2019.2927431.

[12] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture," IEEE Access, vol. 9, pp. 103637–103650, 2021, doi: 10.1109/ACCESS.2021.3099037.

[13] I. B. Senkyire and Q. A. Kester, "Validation of Forensic Crime Scene Images Using Watermarking and Cryptographic Blockchain," 2019 ICDSA Int. Conf. Comput. Data Sci. Appl. ICDSA 2019, pp. 2–5, 2019, doi: 10.1109/ICDSA46371.2019.9404235.

[14] A. Al-Nemrat, "Identity theft on e-government/e-governance & digital forensics," 2018 Int. Symp. Program. Syst., pp. 1–1, 2018, doi: 10.1109/isps.2018.8378961.

[15] P. T. Duy, H. Do Hoang, D. T. Thu Hien, N. Ba Khanh, and V. H. Pham, "SDNLog-Foren: Ensuring the integrity and tamper resistance of log files for SDN forensics using blockchain," Proc. - 2019 6th NAFOSTED Conf. Inf. Comput. Sci. NICS 2019, pp. 416–421, 2019, doi: 10.1109/NICS48868.2019.9023852.

[16] D. P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy," IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, vol. 2018-Octob, no. October, pp. 2372–2377, 2019, doi: 10.1109/TENCON.2018.8650434.

[17] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," IEEE Access, vol. 7, pp. 99573–99588, 2019, doi: 10.1109/ACCESS.2019.2930345.

[18] B. Chen, X. Huang, F. Liu, and H. Yin, "A Location-based Blockchain Evidence Preservation Wireless Communitication Scheme for HuaTaiYiMei v Tongdao Technology Development Case," Proc. - 2021 4th Int. Conf. Electron Device Mech. Eng. ICEDME 2021, pp. 38–41, 2021, doi: 10.1109/ICEDME52809.2021.00016.

[19] S. Patil, S. Kadam, and J. Katti, "Security enhancement of forensic evidences using blockchain," Proc. 3rd Int. Conf. Intell. Commun. Technol. Virtual Mob. Networks, ICICV 2021, no. Icicv, pp. 263–268, 2021, doi: 10.1109/ICICV50876.2021.9388486.

[20] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, "A forensics-by-design management framework for medical devices based on blockchain," Proc. - 2019 IEEE World Congr. Serv. Serv. 2019, vol. 2642–939X, pp. 35–40, 2019, doi: 10.1109/SERVICES.2019.00021.

[21] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh, "An Implementation of Blockchain Technology in Forensic Evidence Management," Proc. 2nd IEEE Int. Conf. Comput. Intell. Knowl. Econ. ICCIKE 2021, pp. 208–212, 2021, doi: 10.1109/ICCIKE51210.2021.9410791.

[22] J. Jemal and K. T. Kornegay, "Security Assessment of Blockchains in Heterogenous IoT Networks: Invited Presentation," 2019 53rd Annu. Conf. Inf. Sci. Syst. CISS 2019, pp. 1–4, 2019, doi: 10.1109/CISS.2019.8693034.

[23] P. Kieseberg, S. Schrittwieser, P. Fruhwirt, and E. Weippl, "Analysis of the Internals of MySQL/InnoDB B+ Tree Index Navigation from a Forensic Perspective," Proc. - 2019 Int. Conf. Softw. Secur. Assur. ICSSA 2019, pp. 46–51, 2019, doi: 10.1109/ICSSA48308.2019.00013.

[24] Y. Xiao, P. Zhang, and Y. Liu, "Secure and Efficient Multi-Signature Schemes for Fabric: An Enterprise Blockchain Platform," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 1782–1794, 2021, doi: 10.1109/TIFS.2020.3042070.

[25] K. Rani and C. Sharma, "Tampering Detection of Distributed Databases using Blockchain Technology," 2019 12th Int. Conf. Contemp. Comput. IC3 2019, pp. 1–4, 2019, doi: 10.1109/IC3.2019.8844938.

[26] M. Westerlund and M. G. Jaatun, "Tackling the cloud forensic problem while keeping your eye on the GDPR," Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 2019-Decem, pp. 418–423, 2019, doi: 10.1109/CloudCom.2019.00071.

[27] S. Brotsis et al., "Blockchain solutions for forensic evidence preservation in iot environments," Proc. 2019 IEEE Conf. Netw. Softwarization Unleashing Power Netw. Softwarization, NetSoft 2019, pp. 110–114, 2019, doi: 10.1109/NETSOFT.2019.8806675.

[28] T. Bakhshi, "Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things," 2019 4th Int. Conf. Emerg. Trends Eng. Sci. Technol. ICEEST 2019, 2019, doi: 10.1109/ICEEST48626.2019.8981675.

[29] A. Balaskas and V. N. L. Franqueira, "Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges," 2018 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2018, pp. 1–8, 2018, doi: 10.1109/CyberSecPODS.2018.8560672.

[30] A. Patil, A. Jha, M. M. Mulla, D. G. Narayan, and S.

Kengond, “Data Provenance Assurance for Cloud Storage Using Blockchain,” Proc. - 2020 Int. Conf. Adv. Comput. Commun. Mater. ICACCM 2020, pp. 443–448, 2020, doi: 10.1109/ICACCM50413.2020.9213032.

[31] A. Rapuano, G. Iovane, and M. Chinnici, “A scalable Blockchain based system for super resolution images manipulation,” Proc. - 2020 IEEE 6th Int. Conf. Dependability Sensor, Cloud Big Data Syst. Appl. DependSys 2020, pp. 8–15, 2020, doi: 10.1109/DependSys51298.2020.00011.

[32] T. Jiang, A. Sui, W. Lin, and P. Han, “Research on the Application of Blockchain in Copyright Protection,” Proc. - 2020 Int. Conf. Cult. Sci. Technol. ICCST 2020, pp. 616–621, 2020, doi: 10.1109/ICCST50977.2020.00127.

[33] G. Ahmadi-Assalemi, H. M. Al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani, and P. Pillai, “Federated Blockchain-Based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace,” Proc. 12th Int. Conf. Glob. Secur. Saf. Sustain. ICGS3 2019, pp. 1–9, 2019, doi: 10.1109/ICGS3.2019.8688297.

[34] W. T. Weilbach and Y. M. Motara, “Applying distributed ledger technology to digital evidence integrity,” SAIEE Africa Res. J., vol. 110, no. 2, pp. 77–93, 2019, doi: 10.23919/SAIEE.2019.8732798.

[35] A. Alabdullatif, K. Alajaji, N. S. Al-Serhani, R. Zagrouba, and M. Aldossary, “Improving an Identity Authentication Management Protocol in IIoT,” 2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769499.

[36] X. Li, J. Xu, X. Fan, Y. Wang, and Z. Zhang, “Puncturable Signatures and Applications in Proof-of-Stake Blockchain Protocols,” IEEE Trans. Inf. Forensics Secur., vol. 15, no. c, pp. 3872–3885, 2020, doi: 10.1109/TIFS.2020.3001738.