Title page:

The significance of Blockchain technology in preserving the digital evidence integrity in forensic investigations

Abstract

Digital forensics refers to digital evidence and IoT forensics is related to extracting evidence information from IoT devices and IoT network environments to investigate digital crimes. Both digital and IoT forensics encourage the use of forensic tools in detecting, acquiring, processing analysing and reporting as required in enforcement investigations. Due to the increase in attacks on data with the proliferation of IoT devices hackers continuously attempt to gain access to vital data to destroy or harm or for vested interests. Existing digital forensic tools lack adequate measures related to the security and integrity of evidence data. To overcome challenges in preserving evidence data blockchain technology is considered as a solution to store evidence data. This study provides qualitative research involving thematic analysis to analyse the use of blockchain to store evidence data in IoT forensics. The challenges are discussed in IoT forensics and how blockchain can support forensic investigations in terms of reliability and integrity of data. The findings from thematic analysis highlight the need for and importance of blockchain in storing digital evidence in IoT environments. This research is intended to contribute to existing research on IoT forensics and blockchain. Recommendations for organisations are also proposed for consideration.

Acknowledgements

Table of Contents

1 6

1.1 Introduction to Digital Forensics**6**

1.2 **9**

1.3 **9**

2 10

2.1 IoT Security and Forensics**11**

2.2 **16**

2.3 **22**

3 26

3.1 **26**

3.2 **27**

3.3 **28**

3.4 **29**

3.5 **29**

3.6 **30**

3.7 **30**

4 35

4.1 **35**

4.2 **35**

4.3 **36**

5 49

5.1 Discussion of Research questions**49**

5.2 **54**

5.3 **55**

6 58

List of Figures

Figure 1:1212

Figure 2:1414

List of Tables

Table 1: Codes and Themes33

1 Chapter 1: Introduction

1.1 Introduction to Digital Forensics

Digital Forensics (DF) relates to the branch of forensic science but makes use of digital technology in managing evidence available in digital form. DF has the standard processes of detection, acquisition, process, analysis and reporting of data stored electronically (Al-Khateeb, Epiphaniou and Daly, 2019). DF is important as law enforcement agencies and investigations need electronic evidence as this is allowed worldwide as authentic evidence to investigate illegal activity. Using the information in digital devices it is possible to determine how information is used stolen lost misused or disseminated, all these tasks are enabled through digital forensic tools. DF is understood as the activity or process of understanding the crimes done through digital devices. Digital crimes involve malicious activities, hacks data theft, or compromised systems that result in huge negative impacts on organisations. DF tools allow investigators to analyse and examine digital devices, and systems by tracing the source of attack or data breach for further actions and legal recourse (Holt, Bossler and Seigfried-Spellar, 2022).

DF also faces challenges related to safe keeping of digitally retrieved evidence data, security and integrity of data. The challenges are more profound in IoT network environments where multiple or a variety of heterogeneous devices are involved in data transfer thus increasing the complexities in forensic analysis and investigation. In IoT environments gathering digital evidence is done from IoT devices which can often lead to increased risks of security and integrity. The risks with IoT are unavoidable because IoT devices are unregulated and do not follow standard security practices to protect data. These drawbacks make IoT devices more vulnerable to hacks and compromise. It is understood that cybercrime investigating agencies face these problems in ensuring the integrity

and security of data especially in IoT environments. However, developments in IoT technology have significantly aimed at improving the security of data handled by IoT devices. However, challenges remain in IoT due to a lack of uniform standards (Hameed and Alomary, 2019).

The challenges in IoT devices are underlined by researchers focus on the major areas of data security, integrity and confidentiality. The advantages of blockchain include confidentiality, integrity and data security and is considered in IoT forensics and digital forensics in general. Blockchain stores data as blocks in a distributed ledger database and uses cryptographic hash functions to ensure data stored in the block is tamper-proof and maintains resistance. In view of these technology advantages, blockchain technology is considered for storing evidence data in digital forensics. Many studies in the literature highlight the need for blockchain technology to ensure data integrity and reliability in storing forensic evidence data without tampering as required by courts as authentic digital information related to crime (Mohanta et al., 2020).

There are three main types of blockchain technology namely, permissioned, permissionless and consortium blockchains. Permissioned blockchain is similar to private blockchain used by organisations with authorised access to users whereas permissionless blockchain access requires no authorisation or it is similar to public cloud services. A consortium blockchain is used by one or more organisations in an industry. In digital forensics involving IoT data breaches and compromised systems, there could be more than one player involved. For instance, the cloud provider, IoT device manufacturer, organisation and security consultants. In such situations, a private or consortium blockchain model can be ideal for storing evidence data as data is restricted to a few users and accountability for investigation and verification of evidence data is set correctly (Sheth and Dattani, 2019).

IoT devices are developed by multiple manufacturers and hence there are no standards for established wireless security protocols in the device. However, most IoT devices used make use of TCP/IP communication protocols in exchanging data with other devices or with a cloud systems infrastructure. The lack of standards makes IoT vulnerable to attacks and hacks by malicious users to gain access to main systems and data. Given these aspects, forensic analysis involving IoT devices is a challenging topic as conventional digital forensic processes may not work well with IoT forensic analysis (Karie et al., 2021). Importantly, the evidence data gathered from IoT devices must be protected and preserved without tampering or deliberate or accidental erasure. In this requirement, blockchain comes into play for its immutability, security, trust and privacy characteristics (Erdem, Yildirim and Angin, 2019).

Numerous contributions in the literature highlight the need for blockchain in digital and IoT forensic analysis. IoT forensics aims to understand the source of attack by tracing devices, retrieving and storing data from devices safely and ensuring reliability. Also, data preservation methods include digital signature, timestamp, cryptography, data hiding and data digesting as these methods are common in a digital crime scene (Akhtar and Feng, 2022). Therefore all these aspects need a mechanism to protect digital evidence obtained from cloud systems and wireless sensor networks. The evidence data must not be accessible to everyone and must be stored in a secured location away and not in the location of crime scene to ensure data is protected and tamper-proof. Almost all these requirements are fulfilled by blockchain.

In this research, the role and importance of blockchain technology in IoT forensics is analysed in preserving evidence data gathered from IoT devices in crime investigations. Blockchain is proven to provide tamper-proof security and integrity of data and is used in a variety of applications and industry areas. In digital forensics, there is a crucial need to store evidence data as data can provide

clues in solving crimes in court. Evidence data must be secured and made tamper-proof which is enabled by blockchain. The report discusses the use of blockchain to emphasis its use in preserving evidence data with a focus on IoT forensics. The report is based on qualitative research methods involving thematic analysis and discussions based on themes. The different aspects of IoT forensics and the importance of blockchain in preserving digital evidence are highlighted given the vulnerabilities found in IoT devices and the challenges in preserving evidence data.

1.2 Research aim

The aim of this research is to examine the significance of Blockchain technology in the preservation of digital evidence integrity in forensic investigation.

1.3 Research Objectives

- To study and analyse the effectiveness of blockchain in the processes of IoT forensic investigations
- To understand the importance of blockchain in improving forensic investigations in IoT environments.
- To evaluate the efficiency of blockchain technology in preserving the digital evidence integrity in forensic evidence.

2 Chapter 2: Literature Review

Data forensics (DF) technology is used to investigate computer-related crimes. This field has evolved along with Internet of Things (IoT), an emerging technology development based on ubiquitous computing devices to develop new tools, approaches and techniques (Stoyanova et al. 2020). According to Rani et al. (2021), with the increase of IoT in many applications across industries, there is a need to study data forensics in IoT as these IoT devices are vulnerable to threats and risks leading to computer-related crimes. There are many studies related to IoT and DF to highlight different solutions in the forensic investigation process (Khan, Shaikhand Laghari, 2022), (Lutta et al. 2021). The main processes in DF are to collect data, investigate and share details of investigation results. Here since IoT involves numerous devices and sensors connected to a network that exchange data DF investigation will involve scanning for data traces on all devices related to the investigation (Karie et al. 2019). The data gathered from all the participating devices are preserved (Alam and Kabir, 2023). Stoyanovaet al. (2020) mention that another major challenge with IoT devices is they do not follow a unified standard and hence data can be available in different formats or platforms which will make the investigation difficult for DF experts.

Cyber-attacks are possible because IoT technology can exchange information between two or more connected devices on the internet. IoT is widely used in agriculture, commerce, industry, and so on. Studies on IoT security explain the type of risks and attacks that lead to digital crimes (Tyagi, Rekha and Sreenath, 2020). Miloslavskaya and Tolstoy (2019) explain the problems due to specific attacks on IoT devices and applications. IoT devices are easy target for attackers and compromise easily. In IoT and related devices, users leave digital traces of information on application activities and they can be traced to obtain the source of information stored in a database. Further due to an

increase in online fraud, attackers target IoT devices as attack objects or as criminal tools due to the vulnerabilities in their architecture. To investigate security breaches or criminal activity IoT forensics (IoTF) experts make investigations to identify the main information in digital criminal incidents (Saleh et al. 2023). A literature review is presented based on secondary research to understand the role of blockchain to preserve data in IoTF investigations. Importantly IoT digital forensics is significant as specialized tools and techniques are used in crime investigation.

2.1 IoT Security and Forensics

IoT is an environment consisting of a mix of heterogeneous devices interconnected in applications. For instance, devices such as sensors, RFID, digital video recorders, etc., fall under the paradigm of IoT application networks. As mentioned earlier numerous applications of IoT range from healthcare to manufacturing to smart cities, and so on. The devices embed both hardware and software to facilitate communication in the network. Here, hardware includes sensors, actuators and communication components. Software implies the network protocols and operating environments and systems that manage sensors and exchange data. In IoT applications gather all data through sensors are transferred over the internet and usually stored on a centralized application server in a cloud infrastructure (Kollolu, 2020).

IoT due to its flexibility and specific uses in applications has become popular over the years with the potential for more real-time applications in the coming years (Hassija et al., 2019). The general architecture of IoT is made up of three basic layers namely the sensor or the perception layer, transport or network layer and the application layer. The perception layer consists of devices, usually sensors to sense the environment and gather data in response to different environmental phenomena (Qabil et al. 2019). For example, the perception layer will have temperature sensors, etc. The transport or network layer facilitates IoT to exchange data between devices. The

application layer stores support analysis and represents the sensed data to the end user. IoT devices can also be categorised into four layers namely the sensors or actuators, communications or network layer, middle-ware layer and application layers (Kamal, Hemdan and El-Fishway, 2021).

The three and four-layer architectures are illustrated in Figure 1.

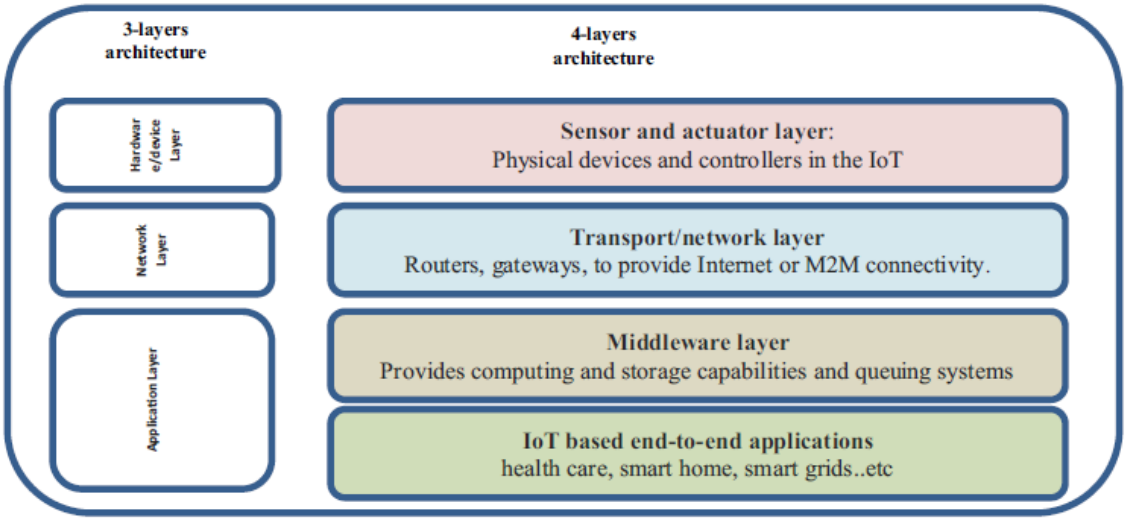

Figure 1: IoT architecture with 3 and 4 layers

(Kamal, Hemdan and El-Fishway, 2021)

Different researchers explain different layers of IoT for its architecture. The International Telecommunications Union (ITU) explain the layers of application, service support, network layer and device layer (Kamal, Hemdan and El-Fishway, 2021). Authors, Gupta and Quamara (2020) explain the architecture to have four layers such as layer for managing network, sensor or perception layer, data exchange through the transmission layer and application layers. The layers play an essential role in the functioning of IoT for the application deployed. Security is of paramount importance in IoT applications.

IoT security in general refers to the object or device that must be protected against threats to both the device or hardware and application on which it is used. Threats to hardware are usually physical damage or device theft or loss whereas software threats are possible in the form of un-authorized access, misuse of data or privacy, hacks, and malicious code that can compromise the deice or system by a malicious user (Ghazal, Afifi and Kalra, 2020). As mentioned earlier, IoT devices are vulnerable to threats and attacks for different reasons. The devices have restricted computing power, limited software resources, lower capabilities in processing complex security algorithms, and no uniform standard for architecture, the application environment makes use of many devices that generate and transmit data (de Araujo Zanella, da Silva and Albini, 2020). Therefore, the security and protection of IoT devices are highly critical for protecting important application data. Given these aspects, cyber security of IoT must ensure confidentiality, integrity and availability of information at all times.

IoTF involves gathering evidence and analyzing it to find traces of malicious activity or criminal activity against systems. Digital forensics involves the basic steps of identification of evidence in a crime scenario, preservation of data identified, analysis phase will correlate evidence to prove criminal incident, documentation of the entire process, and finally presentation with conclusions on the investigation (Nadeem, Saeed and Ahmed, 2020). The integration of digital forensics and IoT provides benefits but creates new challenges related to security and forensics. Given this understanding, IoT forensic investigation is done in three levels namely the bottom, middle and top levels. The bottom level makes up the forensic level in IoT, middle level is the cloud or internet forensics level and the top level is the application forensics level. These three levels cover the forensic investigation phases namely identification, collection, preservation, examination, analysis

and preservation (Kamal, Hemdanand El-Fishway, 2021). The IoTF investigation model will investigate crimes through the use of IoT as illustrated in Figure 2.

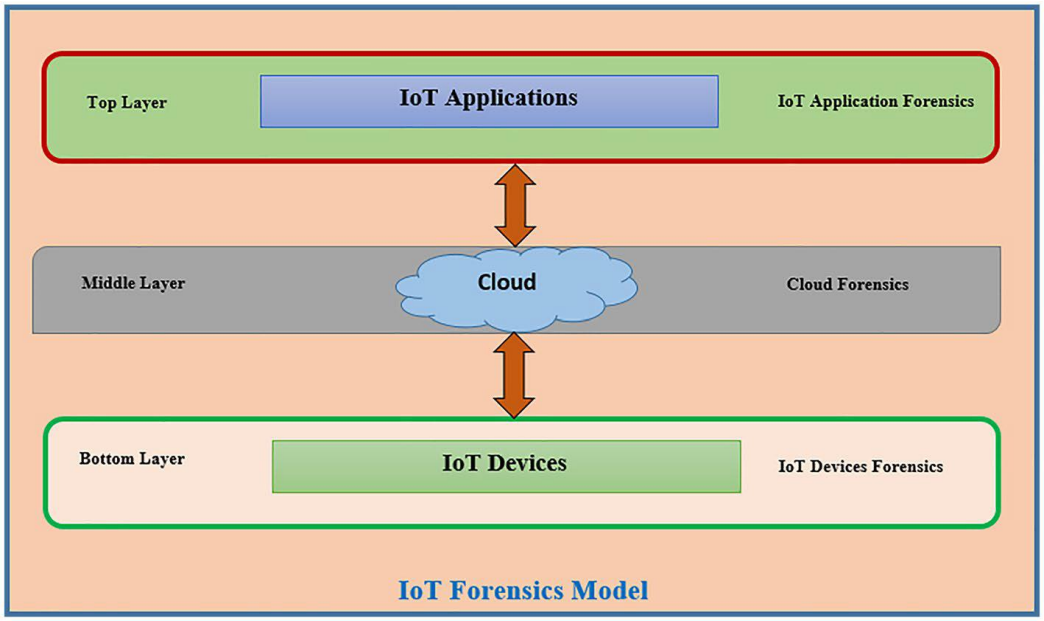

Figure 2: IoT Forensic investigation model

(Kamal, Hemdan and El-Fishway, 2021)

From Figure 2, it is noted that the model has four important phases. The phases are to find evidence in digital form, gathering and acquiring all data, the data is analysed and reported as a presentation to explain the entire forensic investigation.

Yaqoob et al. (2019)explain that a wide variety of IoT devices can create problems for data analysis. This is because IoT devices can gather sensitive user data related to passwords, personal information, bank details, etc. In such cybercrime scenarios, data is used for analysis by investigators'. Thus, the users must be aware of the data used in the investigation process. At the same time, investigators must ensure that the data is protected from unauthorized access manipulation or loss to preserve user privacy. Therefore, this needs careful management of

evidence for the investigation. Further, the data must not be mixed up with other users as this leads to complications in evidence collection.

Servida and Casey (2019) provided extensive information on challenges related to IoT in forensic investigations. The challenge is mostly related to the heterogeneity of technologies in IoT and hence the investigators must use appropriate techniques and tools to retrieve information related to crime from a variety of embedded devices. Sadineni, Pilli and Battula (2019) provided a holistic forensic aware model to support digital forensic investigation in IoT environments. As the DF solutions focus on specific application domains involving IoT devices a holistic model developed using the ISO/IEC 27043 standard can be used to eliminate ad hoc models while covering diverse digital environments. The article presents the end to end processes in IoT forensics to provide customizable and configurable environments and support diverse IoT environments. Forensics aware model for IoTF works on the levels of device, network and cloud forensics. The holistic model can be considered as a framework that must be tested thoroughly in different investigation environments to highlight its effectiveness in terms of reliable investigation outcomes.

Sharma et al. (2020) underline the challenge related to IoTF investigations in complex and heterogeneous IoT environments. It is noted that digital evidence is available in IoT devices but the problems of limited storage in small devices and detecting data in a distributed environment from devices that are compromised is a major challenge. The authors claim that this challenge area still needs development for the effective collection of digital evidence from IoT devices. Kebande et al. (2020) presented a holistic IoTF readiness framework based on ISO/IEC 27043 to qualitatively evaluate digital forensics in IoT environments. The authors conclude that due to the lack of standard approaches, the IoTF complicate digital forensic investigations. Hence the

framework was evaluated qualitatively. However, a formal evaluation of such frameworks in real time is necessary to understand their real-world usefulness.

2.2 Related work Blockchain for IoT Forensics

In today's industry products and services delivered through emerging technologies namely blockchain, IoT, and 5G (fifth generation) communications are popular for their potential in a number of application areas (Attaran, 2023). However, new technologies are easily prone to cyber threats and risks that allow cybercriminals to exploit vulnerabilities in the technologies to conduct malicious actions (Aslan et al., 2023). For instance, in IoT application environments cyber criminals can perform hacks easily as IoT devices do not have standard security measures and IoT devices exchange data with other IoT devices and with IT infrastructures through the internet. Given this scenario, cyber crimes have increased over the years and IoT due to their large interconnections makes the detection of cyber crimes difficult compared to normal hacks from the internet. Further in forensic investigations, digital evidence plays a significant role and this applies to IoT network environments(Djenna, Harous and Saidouni, 2021). There is a need to preserve evidence from hacks or tampering. To preserve evidence obtained from IoT and other digital devices blockchain is further explored.

Blockchain technology involves a distributed ledger database to store records in a decentralized manner on a peer to peer network. The data in the blockchain is stored on time-stamped blocks linked with the chain thus creating an immutable, visible and audited chain of data that is stored based on consensus and proof of trust(Rajasekaran, Azees and Al-Turjman, 2022). Data in blockchain are immutable as the blocks in data are linked as cryptographic hash of transactions. This implies new data as a block is stored on the chain only after consensus from all the members of the chain and after it is validated and approved by all members. Further, the block after

consensus by all memebrs is stored on the block is not available for changes or modifications or deletions by any members. Modification of stored data is possible, but this modified data will be stored as a new block again after consensus from all members of the blockchain. These characteristics in the blockchain ensure accountability, traceability, immutability, auditability and transparency. Blockchain is successful in many industry application areas such as supply chains, financial services, energy, pharmaceuticals, healthcare, and so on. Blockchain due to its characteristics provides a strong solution for preserving evidence from digital devices in cybercrime investigations (Sharma et al., 2020). Usually, in forensic investigations, data extracted from devices and hardware is vulnerable to hacks or theft and deliberate deletion by users. This is a major challenge, and to handle this challenge blockchain can provide the forensic examiner with self-verification of digital devices using a cryptographic functions to establish a chain of verified data blocks in the database. The cryptographic hash function will guarantee immutability, transparency and trust within the case investigation.

Ryu et al., (2019) explain forensics involves the tasks of identification, collection, storage, analysis and distribution of digital evidence are highly critical for investigating the crime. Janarthanan, Bagheri and Zargari (2021) explain that IoT forensics provides more challenges in forensic investigation due to the heterogeneous devices used in IoT networks and diverse applications with large volumes of data. The challenges in IoTF examinations must be addressed by the examiner where blockchain-enabled forensic investigation provides the promise of tracing data that will lead to criminals and their malicious activities. Further, IoTF also provides the potential to obtain insights on unauthorized actions in a cyber-environment to trace criminals. While the promise of the use of forensic tools in IoT environments is high, there are no international standards that can be made as a formal standard in IoT forensics (Kruger and Venter, 2019). Also since IoT networks

are usually linked with a cloud computing infrastructure, or in cyber-physical environments the challenges have increased for forensic examiners in existing technology scenarios (Armoogum, Khonje and Li, 2021). Some papers explain forensic investigations in cloud environments with a focus on improving trust and interaction between stakeholders in cloud forensic investigations. Likewise, studies highlight the use of blockchain in many application areas namely financial fraud detection, e-governance, and online applications. Blockchain is effective in these application areas in mitigating fraud as that ensures integrity, trust, immutability and authenticity, in un-trusted IT and software environments. Given these aspects, blockchain for IoTF is explored further, by having a thorough understanding of the challenges.

Li, Qinand Min, (2019) provided a summary of challenges in existing DF investigations involving IoT. The challenges are as follows,

Trustworthiness – implies insider threats to evidence gathered from the digital devices in an IoT environment. The challenge here is to enhance trust of evidence data in the device in DF.

Integrity – refers to continuous checks for integrity in identified digital items and the events of examination in digital investigation. In traditional investigations, there is no support for forensics activities between the items used as evidence and the tools used by examiners.

Improved provenance – helps in validating all digital evidence using a hash function and validates all findings to create a hash tree. Creating a hash is needed in an IoT environment as the hash functionality will help in examining the evidence pieces for more examination.

Scalability challenges –refers to the hash tree that has a parent node and the parent node can support up to 1000 child nodes. These many nodes in DF imply that forensic investigation must be done on 1000 events or activities or evidence items. IoT environments have the capability of

having 10^{3n} (n indicates deep-level hash tree) hash digests. Therefore, IoT forensics can easily scale up to store evidence items or events.

Availability and resiliency – Each blockchain node will contain a complete guaranteed copy of the entire hash tree, accurate and verified. This makes blockchain storage very resilient to storing events and information in forensic investigations. Here, when an evidence item is found written to the blockchain the examiner can be fully confident the evidence will be accessible and available without tampering (Cordi et al., 2022).

In view of the above challenges and the promise of blockchain, the rapid developments in IoT environments provide examiners with the need to overcome challenges in IoT ecosystems or complex networks. Also the lack of standards in IoT device manufacturing must be taken into account in IoT forensic investigation process. Dawson and Akinbi (2021) discuss that existing forensic tools and techniques do not support IoT devices as they are heterogeneous by nature. However, to address challenges related to forensics in IoT environments, different frameworks are proposed to support investigations. However, the implementation is limited to specific devices or scenarios with limited scope, for example, smart home environments. Li, Qinand Min, (2019) provide in-depth discussions on the use of blockchain by forensic examines in overcoming issues related to traceability, transparency, audibility and accountability due to its tamper proof characteristic involving a hash function that links blocks and transactions. The authors explain blockchain will guarantee transparent methods for the decentralized preservation of evidence that will mitigate the risk of evidence in place with the central arbitrator that can be arbitrarily corrupted by examines or damaged due to malicious internal users.

Brotsis et al., (2019) provided a framework using distributed hyper ledger fabric in blockchain technology to study the tasks of collection, preservation and verifying the integrity of digital evidence that are retrieved from IoT devices in a crime setting. The framework was based on a permissioned blockchain with a chain of custody in IoTF. Here, a chain of custody includes the examiners and other investigators involved in the incident. Access to blockchain data is available only with the chain of custody. Here, the evidence is stored as metadata in the form of smart contracts with multiple entities participating in the process of investigation. However, this study involves an architecture that will showcase the applicability of blockchain-based solutions to tackle challenges in preserving digitally available forensic evidence from IoT devices. The study is experimental and must be implemented and tested in a real-time IoT environment.

Mercan et al., (2020) provided a blockchain solution based on the method of proof of concept (POC). The authors using the POC blockchain framework provide an approach that is cost-efficient along with guarantees of integrity and validates provenance. The solution is based on a public blockchain and uses the concepts of proof of stake (PoS) and multi-chain blockchain technologies. The provided approach uses the methods of data provenance and data integrity in the IoT environment. The approach and solution is presented using a public blockchain network to store extracted evidence data in forensic analysis. The presented solution is evaluated with other popular blockchains namely Ethereum, EOS, and Stellar to present an analysis of security and cost. The authors claim the presented solution can provide cost savings. However since data storage is in a public blockchain, this can pose challenges as the blockchain is open for access. This can result in data compromise and integrity violation without the notice of other members of the blockchain. The issue of public blockchain can pose increased complexity as additional security measures may be required.

Tian et al., (2019) used a permissioned blockchain using a custom-made multi-chain blockchain and practical byzantine fault tolerance (PBFT) to provide a generic and scalable blockchain-based framework (Block-DEF). The framework is presented to show evidence data stored on cloud storage. The authors using this framework presented that the problems related to scalable systems, data integrity, data validity, privacy and traceability can be addressed. In this permissioned blockchain the access to digital evidence is restricted with users involved in the investigation.

In another study involving IoTF, a framework named Probe-IoT is presented based on a public blockchain platform to store evidence gathered data in an IoT environment. In this framework, the data exchanges in the system is on the blockchain after consensus from participants and an encrypted publickey for trusted third-party is used for access. The framework can be used in investigating cases that involve violations of service level agreements (SLA) in cloud service providers (CSP) (Brotsis and Kolokotronis, 2022).

The permissioned blockchain is a tamper-proof and privacy-preserving ledger that is reliable in solutions. The proposed solution is experimental and the block-DEF framework is developed to ensure the integrity and validity of evidence along with privacy and traceability. However, a prototype or a real-time implementation, its compatibility with a permissioned blockchain platform is not available to verify its effectiveness (Tian et al., 2019).

The studies reviewed provide solutions to IoTF examination as theoretical or experimental frameworks using different blockchain models for forensic examination in IoT environments. It is noted that existing studies use a mix of different blockchain platforms to include public blockchain that is vulnerable to attacks, hence the basis for preserving crime data from IoT devices is not fulfilled. Further, the growth of IoT in innovative applications has increased cyber-attacks

and threats and there is a need to extract information from IoT devices while facing limitations in existing digital forensic tools as they do not support data extraction from IoT devices. These are some of the limitations explored from reviews briefly explained above. Further, the importance of preserving digital evidence using blockchain IoTF is explored and summarized from existing research.

2.3 Related work on preserving digital evidence using blockchain in IoTF

The focus of IoT forensics involves digital devices, systems and inter-relations between different elements in IoT ecosystems. Earlier literature highlights the evidence collected in IoT devices must be protected from tampering or misuse or internal threats and IoT applications make use of many devices and hence the need for examining the entire range of devices for crime information. Horsman (2022) explains that while maintaining extracted evidence data the aspects related to privacy preservation and identity management are mandatory in the context of forensic investigations is important. Furthermore, in digital crimes, evidence is a tangible and demonstrable artefact that provides the facts and information needed for an investigation related to the incident. Hence, examiners have the essential need to maintain proper evidence to ensure the admissibility of evidence in courts and to other crime investigating agencies.

In preserving evidence an important concept named the chain of custody (CoC) is maintained in forensic examinations to have better controls and transfer for analysis sequence and protect the integrity of evidence information and mitigate breaches (Ahmadi-Assalemi et al., 2020). As reviewed in the literature blockchain technology provides a secure CoC to store evidence in an immutable platform that is reliable. Ahmad et al., (2020) provided a framework for CoC to overcome the challenge of preserving digital evidence in IoT environments. The framework is presented to support evidence gathering, storage, verification, safekeeping and access. The CoC

involves three functions namely evidence collection or the first respondent who submitted evidence, created as another unique block on blockchain that contains unique cryptographic hash. Subsequently, evidence documentation will record all information for CoC to include the name of the sample collector, name and role of the recipient in the corresponding block in the blockchain along with the date and time. Further, the storage will have a virtual key to the store medium to allow only authorized access to view evidence data (Romli, Prayudi and Sugiantoro, 2019). Hence here three important aspects namely integrity, trust confidentiality and traceability are essential. The first is data integrity which will ensure evidence integrity is maintained. The block is verified and trusted as it has the consensus of all members. The next aspect is confidentiality and trust, which implies the evidence means data cannot be accessed by users not authorised. Lastly, traceability certifies the continuity in maintaining evidence data. If the evidence is moved from one location to another or another forensic lab for analysis and investigation, these are monitored and recorded along with exhibits provided in a court of law. In all these sequences of tasks, there is a need for the immutability of data required by the court. Hence in digital forensic examinations, blockchain can provide the much-needed immutability and reliability for preserving digital evidence and artefacts (Al-Hussaeni et al., 2022).

The importance of preserving evidence information in IoTF is highlighted. Akhtar and Feng (2022) state that since DF is vulnerable to manipulation and security threats an approach to preserving integrity along with anticipating threats is essential. The authors propose a method to remove anomalies in evidence data by using machine learning (ML). This model is developed to predict attacks early thus enabling security. This study provides theoretical results using XGBoost to show promising results over 90%, however, the model evaluation in a real-time IoT environment will demonstrate its effectiveness.

From studies, it is understood that in addition to blockchain to preserve digital evidence, access must be restricted to very few users. During the DF examination, the evidence must be available only to authenticated entities to ensure privacy. Towards this approach, a cyber-trust blockchain (CTB) based on a permissioned distributed ledge is needed to store evidence and metadata (Brotsis and Kolokotronis, 2022). In this scenario, to a CoC is established to allow authorised users or entities to access digital evidence, information related to evidence is maintained chronologically. The entities that are authorized can have the ownership for forensic evidence, and issue new transactions by creating blocks. These creed blocks will have changed ownership information. The participants or entities involved in forensic evidence on the blockchain (Ahmad et al., 2020) include,

- Internet service provider: The ISP will gather evidence related to security breaches from a digital system involving IoT. The ISP is the evidence creator of the evidence and has full access to security incident information, regardless of the user or owner of data.
- Law enforcement agencies: Law enforcement will have access to evidence data that belongs to a particular ID or IoT device that has been compromised and stored in CTB during the forensic examination. Law enforcement agencies will be able to issue new transactions as new blocks in the blockchain ledger.
- Prosecutor: The prosecutor is the owner who is responsible to preserve digital forensic evidence during the entire process of investigation. This user will examine digital devices for extracting data related to crime.

In summary, the reviewed literature emphasizes the need for preserving digital evidence during forensic examination. Some studies highlight the use of decentralized mechanisms such as public or permissionless blockchain to allow for transparency, however, in the case of public blockchain

issues related to privacy can arise. In such cases the evidence CoC is subject to further scrutiny in court. The problems of privacy are overcome by the use of permissioned blockchain in IoTF examinations. In this case, the consensus is established, and only authorized users can access the evidence data. Hence, the use of permissioned blockchain is more considered in IoT forensic investigations. As blockchain maintains all data as blocks that have unique hash values, the hash value calculated for digital evidence content will be different from the hash value created for documenting the digital evidence. This implies for each digital evidence data there could be more than one block in the blockchain.

Studies highlight IoT environments make use of heterogeneous devices and hence challenges arise in evidence collection from interconnected devices. The scope of evidence gathering will be challenging as evidence gathered from IoT must be analysed, preserved and protected systematically and secured. Blockchain provides the platform to support forensic investigation in IoT application environments. Blockchain can be used to leverage high levels of security and protection for evidence data in forensic investigations. These aspects are underlined in studies as blockchain provides restricted access in permissioned blockchain models to preserve evidence data from tampering or compromise. Blockchain is ideal as it does not allow the deletion of blocks, and any existing block that is modified is added as a new block only after consensus. Due to these properties, blockchain technology is ideal to store digital forensic evidence and help examiners with confidence. Therefore, blockchain technology and digital forensics in IoT environments can work towards identifying and preserving crime-related information as useful evidence from different sources.

3 Chapter 3: Research Methodology

3.1 Introduction

The research in this topic follows the mixed research approach involving different secondary research methods. The research topic is multi-disciplinary in nature as it involves exploration of new technology and tools, cyber security aspects and digital forensic investigation. Due to the multi-disciplinary nature of the topic, a mixed research approach is followed in this study. The mixed research methods will discover and understand the best practices followed in forensic analysis and on how blockchain technology can support investigators. The study is based on secondary research methodologies that involve critical literature reviews from secondary research sources to understand the use of blockchain technology to preserve retrieved data in forensic investigation.

The literature reviews cover the main areas in forensics namely authenticity, integrity, traceability, accountability and transparency of forensic evidence. Literature was identified based on keywords such as blockchain technology in digital forensics, IoT forensic investigation, use of blockchain in digital forensics and cyber security. Secondary research is conducted and presented in literature review using research journals, online databases, technical reports and other websites.

The method of exploratory research is considered in this study to have an understanding of the existing challenges and problems identified with the chosen topic. Exploratory research will help researcher identify answers to research questions through the use of empirical data. Basically this method will help to use the ideas related to the topic by exploring the theories in more depth. In this topic, the theories of cybersecurity matters related to data protection, digital forensic investigation and blockchain concepts are involved. Hence exploratory research will explore these

concepts in depth to increase the understanding of unexplored aspects related to the topic. Exploratory research will also provide the starting point for future research on a given area or topic (Asmussen and Møller, 2019). Given these aspects, exploratory research provides the scope to examine the research questions that were not earlier explored and helps to address the research gaps and fulfill all objectives. Also, exploratory research design facilitates a sequence of steps to make inquiry, data collection and analysis thus making qualitative research more efficient.

In addition to exploratory research, descriptive research is considered because this will help to describe the situation or phenomenon related to the need to preserve extracted digital forensic data (Sundler et al., 2019). The study makes use of these research approaches and follows the mixed research methods.

Further to the exploratory and descriptive research method considered, the study will make use of thematic analysis as the overall research is based on qualitative methods. Thematic analysis method will follow a sequence of process steps outlined in the methodology. Thematic analysis is considered to identify new findings through in-depth study of the topic using data from secondary research sources, mostly academic literature.

3.2 Research approach

The research approach is deductive reasoning to discover the use of blockchain technology in preserving evidence obtained from forensic investigations. Deductive reasoning considers the methods of theoretical aspects related to blockchain and digital forensics. Towards this, a comprehensive literature review is done to understand existing studies related to the topic. Deductive reasoning helps researcher to first understand the technology implementation and concepts related to data preservation followed by arriving a specific observations. Hence deductive

reasoning is considered in this research (Casula, Rangarajan and Shields, 2021). It is noted from literature reviews, that general observations were made that provide the potential to use blockchain in preserving evidence obtained from IoT and other devices that are compromised due to breach. The literature reviews also helped to understand the benefits and limitations in using blockchain technology in preserving digital forensic data.

3.3 Research Design

The design is based on qualitative research, where a mix of different research methods is followed as mentioned earlier. Basically, the design falls in grounded theory where the research questions were not studied in depth earlier. Grounded theory is an approach to first determine what must be observed. In this case, since evidence information gathered during IoT forensic investigations is vulnerable to cyber threats insider threats, this data must be preserve using a different technology, namely blockchain. Hence, the security aspect must be observed first and in this situation, the grounded theory helps to determine the security needs for the investigation process. Based on this requirement, extensive data is gathered from existing research sources and summarized. Grounded theory is helpful as it aims to support in-depth observations based on facts.

Descriptive research is followed to understand the characteristics and categories of data preservation in a theoretical manner. Descriptive research basically explains the 'how' phenomena along with 'what' and 'when'. Here, the 'how' refers to how can the data retrieved during forensic investigations be protected from threats. Thus the use of descriptive research is justified in the study. Further, thematic analysis in qualitative methods is followed in this research design because this approach will help to compare data in secondary research to identify themes that are similar to the topic. The steps followed in thematic analysis are discussed later.

Qualitative research design is followed for this topic for the following reasons:

- The process of qualitative research will help to understand the uniqueness of the given technology scenario in the context of IoT forensic investigation
- The focus of researcher is on data collection and analysis using a mix of methods involving descriptive, exploratory and thematic analysis technique
- Qualitative research emphasizes on observing the responses in natural settings, such as homes or workplaces. Here the topic relates to a workplace scenario with the need to preserve information using a different technology, to ensure integrity and security of data.
- The design of this research is deductive. The methodology is reliant on concepts, existing research literature and industry practices.

3.4 Data sources used

The secondary data sources for the study include journals and reliable data from online libraries, Scopus, Science Direct, IEEE, and so on. The data from these sources are reliable and appropriate and fits well for the scope of this research. The data collected are from established journals and online databases and methods for conducting qualitative research are either thematic analysis or grounded theory.

3.5 Analysis of data

The data is obtained from secondary sources mostly theoretical in nature with observations, words and usually non-numerical data. Thematic analysis supports in organising the data o easily recognise the context of implementing blockchain in digital IoT forensics (Sundler et al., 2019).

The subjective experience of researcher helps to identify themes and meaning within the data. Thematic analysis approaches involve inductive thematic analysis, deductive thematic analysis,

and semantic and latent thematic analysis. The inductive thematic analysis will derive meaning and identify themes from data. The data is analysed without expected results. Alternatively, deductive thematic analysis will analyse data within a set of expected themes. In this method, prior knowledge of existing theory and research is needed to analyse this data. Semantic thematic analysis will consider the themes by ignoring the underlying data. Lastly, the latent thematic analysis approach will focus on underlying meanings and reasons for semantic content. In view of these four types, the latent semantic analysis is considered as more ideal for this analysis as it will help to determine how other researchers have approached this topic area and interpretations are made by the researcher. The researcher makes decisions or recommendations based on the interpretations (Braun and Clarke. 2022).

3.6 Use of thematic analysis

Thematic analysis is used in situations where there are large amount of theoretical data. The data can be divided or categorised to easily organise information and to synthesise patterns of data (Terry and Hayfield, 2021). In this research, participants are not involved and no theoretical framework is used, however, new insights are generated from the themes and concepts in the data. Further given the diverse nature of this topic, the thematic analysis provides the flexibility to summarise important concepts within the given dataset. To get started with thematic analysis the research questions are developed.

3.7 Research questions

1) How can blockchain technology support digital forensic investigation, especially IoT forensic investigations?
2) How can blockchain improve the efficiency and integrity of digital evidence gathered during IoT forensic investigation process?

A systematic procedure is followed to identify, analyse and interpret secondary data. In thematic analysis the following steps are followed:

Step 1: Familiarising with data – implies the data identified from secondary sources that research on blockchain technology for its use to store evidence data and support IoTF investigations. A large number of papers were identified and reviewed in the literature.

Step 2: Generation of codes – Coding is important in thematic analysis. Coding will provide systematic categories of qualitative data with reference to the research questions. Initially, open coding is done to determine useful concepts from data and later categorized under broadly defined research questions. In the analysis stage, coding will help the researcher to compare data with the concepts related to blockchain technology usage in preserving IoT forensic investigation information. The generated codes will refer to the findings and ideas for the chosen topic. A descriptive label is assigned to identify the themes across different data. Since coding every piece of text is difficult, the data that is relevant to address the research questions was coded. Here, text lines that are interesting and related to research questions are coded.

Step 3: Search for themes – The theme refers to information that is relevant to the research question and will provide a significant meaning. The following themes are identified:

Theme 1: Blockchain is reliable and improves IoT forensic analysis to support investigation process.

Theme 2: Blockchain technology is implemented in the areas of Cybersecurity and IoT security to preserve data.

Theme 3: Blockchain-based forensic investigation process.

Theme 4: Procedures in IoT forensic investigation.

Theme 5: Performance evaluation of blockchain technology for forensic analysis in IoT environments.

Theme 6: Blockchain technology preserves integrity of data gathered as digital evidence in IoT forensics.

Theme 7: Blockchain-based IoT forensic process guarantees a chain of custody for evidence preservation.

The above are the boarder themes identified from data for thematic analysis. The themes were characterised by their significance.

Step 4: Grouping codes into themes

Themes	Codes
Theme 1: Blockchain is reliable and improves IoT forensic analysis to support investigation process.	Blockchain characteristics Digital forensic process IoT forensic investigation processes
Theme 2: Blockchain technology is implemented in the areas of Cybersecurity and IoT security to preserve data.	Application areas of blockchain Cybersecurity IoT security IoT security vulnerabilities Data protection blockchain technology advantages

	security aspects of blockchain
Theme 3: Blockchain-based forensic investigation process.	Blockchain and digital forensics Blockchain significance Role of blockchain in digital forensic processes
Theme 4: Procedures in IoT forensic investigation.	IoT digital forensic techniques Steps in forensic investigations Forensic investigation in IoT networks/applications
Theme 5: Performance evaluation of blockchain technology for forensic analysis in IoT environments.	Blockchain-based forensic investigations Performance of blockchain in digital forensics Role of Blockchain in IoT forensic investigations
Theme 6: Blockchain technology preserves integrity of data gathered as digital evidence in IoT forensics.	Characteristics of blockchain technology Blockchain security Blockchain and digital evidence-preserving
Theme 7: Blockchain-based IoT forensic process guarantees a chain of custody for evidence preservation.	Advantages of blockchain in IoT forensic processes Blockchain security aspects Immutability in blockchain Security advantages with blockchain

Table 1: Codes and Themes

Step 5: Review themes – Will verify if the themes will fit in the coded data. For instance, the themes are descriptive in nature. The themes describe patterns in data relevant to the research question. For instance, the themes 1 to 4 will answer research question 1, and the remaining themes will answer research question 2. The themes are determined based on collated findings in the literature.

Step 6: Report writing

The validity of the analysis is explained. The thematic analysis will have the report that consists of the following chapters:

- Introduction
- Methodology
- Results and findings
- Discussions
- Conclusion and Recommendations

The research is conducted based on the above methods and approaches.

4 Chapter 4: Finding and Results

4.1 Introduction

The thematic report will present the findings of themes and codes identified earlier and the focus here is the phenomenon of preserving forensic traces data using blockchain in compromised IoT network environments. The report is intended to provide instructive methods to demonstrate how theoretical concepts are introduced and validated to address the issue of protecting data using blockchain. The research intends to understand the use of blockchain technology to protect forensic trace data from IoT, as ensuring protection for data obtained from IoT is a major challenge due to cyber threats and risks. Here, blockchain technology for its immutability and robust security characteristics is considered a viable option to protect data traces obtained from IoT devices, as IoT devices are vulnerable in the areas of data protection. The thematic analysis is performed as the procedures of blockchain, IoT and digital forensic tools provide well-defined descriptions of how these technology tools function while maintaining flexibility and gaining knowledge with regard to the methods and their justifications.

4.2 Methodology

Using qualitative analysis from existing literature different themes were identified and coded as shown in Table 1. The data for generating themes and codes were obtained from existing literature related to the topics of digital IoT forensics, blockchain and the use of blockchain to preserve digital traces from IoT devices. The data is based on the conceptualisation of different technology areas involved in the research. Basically, the focus on generating themes and codes was based on the grouping of issues in preserving forensic traces, IoT forensics, and blockchain technology. The findings related to each theme are discussed further.

4.3 Thematic Reports

Theme 1: **Blockchain is a reliable solution for the IoT forensic investigation process**

In current networked application scenarios, IoT has become a de facto standard to capture data from ambient environments. IoT devices gather data and send them to remote systems thus enabling their use in a wide range of applications namely healthcare, energy, agriculture, and so on. Data from IoT devices are gathered to perform analytics and further support informed decisions. In certain areas like energy systems, transportation, etc. data protection is critical in IoT devices, however, the devices are vulnerable to failures or compromise mostly due to deliberate attacks or due to human error. In case of deliberate attacks, there is a need to investigate the causes of failure. Thus, a secure transmission and storage of IoT data is critical and these requirements create the need for mechanisms to store investigated data from IoT devices in a highly protected environment. Blockchain technology for its immutability and strong security characteristics is leveraged for storing forensic data traces retrieved from IoT devices.

The characteristics of blockchain are widely discussed in the literature. IoT forensics is similar to digital forensics and involves the process of collecting, analysing, storing and presenting digital evidence from IoT devices that will bind legally. Importantly in IoT applications, a variety of devices that have varying configurations interact and exchange data. Hence IoT forensics in particular focuses more on the aspects of traceability, data reliability and provenance of evidence must be maintained. Further IoT devices with resource constraints have limitations in exchanging evidence data correctly. Hence, investigators has to ensure that all the IoT devices that are involved in a case are identified. Investigators must collect, transfer and store evidence data systematically while guarding against malicious behaviours. One way is to establish a digital chain of custody in

the investigation team to ensure the evidence collection and data transfers are transparent while protecting from loss or other forms of data abuse. Importantly the devices must be delegated with trust and integrity capabilities along with privacy in the digital forensic chain.

Given these aspects, blockchain technology with characteristics of trust, anonymity and security can support IoT forensic investigations by recoding information in a distributed ledger where the investigators can change ownership of data without an intermediary. Blockchain allows traceability and supervision of all gathered data while ensuring no single party has control of the entire evidence data. Further blockchain is a decentralized platform, which implies the team of digital forensic investigators maintain the chain of custody and any evidence data once recorded cannot be chanted. In addition, blockchain has the following characteristics that make it more ideal in IoT forensics,

Anonymity -refers to the anonymity of devices in the blockchain, where their true identity is not available to everybody engaged in the case.

Autonomy -the investigators have full autonomy to interact with each other on the blockchain without the involvement of servers.

Security -Blockchain enables secure data exchange with no scope for unauthorised data access or loss. Security is ensured through appropriate encryption-decryption keys that are available only to authorised users.

Non-repudiation -ensures transactions in the blockchain are validated. Further implies if data is stored in the distributed ledger it cannot be deleted or modified. Any modifications are stored as a new data block after approval from all the users in the blockchain.

Resiliency -blockchain data cannot be erased even in case of hardware failure. The ledger is fully available in other nodes, so the possibility of data loss is less.

Audit -Blockchain will record the time stamp of all parties involved, ownership of devices, and other relevant information. In IoT, this is important as the device information can be recorded along with gathered evidence data.

Immutability -Refers to no changes are allowed to data blocks after it is verified and recorded in the ledger.

Therefore, based on the above characteristics blockchain provides a reliable platform to store digital evidence gathered from IoT devices.

Theme 2: Blockchain technology is useful for preserving data

The tremendous expansion of IoT across different application areas starting from industry to entertainment, mobile applications, healthcare, etc. IoT applications need a high security platform to handle data breaches, and to prevent security and privacy issues. Blockchain provides the ideal solution as it is used in a wide range of application areas. For instance, healthcare, finance and insurance, industrial applications, smart homes, smart grid, information storage, and so on are some of the areas where blockchain platform is widely used.

In the application area of IoT forensics blockchain will help as it is an encrypted ledger database and can be managed using a centralised system. For instance, the forensic investigation team consisting of users can be understood as one node for each user in the team. All the nodes will connect to the encrypted ledger where the information retrieved from digital devices will be stored on the distributed ledger database. Each user will have to approve to store. When the information is stored as a block in an encrypted ledger cannot be modified or deleted, as blockchain does not allow. Further, the ledger is decentralised and users with a valid password or encryption-decryption keys will be able to view information on the block. Therefore, the architecture of blockchain

supports preserving retrieved data from compromised IoT devices and preserving it from external or internal threats or attacks.

Cybersecurity through blockchain technology is improved because in data security the weakness in devices or systems is due to the existence of a single point of failure or compromise that results in data theft or modification. Blockchain technology ensures data security from cyber attacks due to its strong infrastructure. Here, each data block is hashed and connected to the next block and hence it is impossible for malicious users to hack or steal data or manipulate it. Blockchain makes use of network security and allows only authorised users to view data in blocks thus preventing unauthorised access and communications. Given these findings from existing research, blockchain technology has the capability to strengthen cybersecurity management practices.

The IoT architecture is the same as TCP/IP architecture, hence the devices have the characteristics of interoperability, reliability, scalability and quality of service. The IoT architecture is made up of the perception layer that has sensors to perceive and collect data from the environment. The transport layer will exchange data collected by sensors in the network, made up of network or cellular technologies. The processing layer will store, analyse and process large amounts of data. This layer involves cloud computing or a large IT infrastructure. The application layer will deliver application-specific services to users and lastly, the business layer will manage applications, the IoT system and user privacy.

While exploring research on IoT security many papers highlighted the challenges that must be considered in IoT applications some of the common vulnerabilities in IoT devices include issues related to interoperability, privacy and security, standards, rights issues, and developmental issues. It is noted that vulnerabilities in IoT are a result of inherent weaknesses in the device design, configuration, implementation and management of the network or system application that is

susceptible to threats. Security challenges in IoT can be attributed to the design and lack of standards or security protocols built into the devices. For instance, as many devices participate in IoT applications a compromise of one device can result in the attacker controlling the more number of connected devices. Therefore security requirements and design must need the aspects of confidentiality, integrity and availability (CIA).

Further, the privacy issues are more profound in IoT as there are no fixed rules to guard users and the data collected by the devices are not protected. Hence there are chances for data theft and the devices can be monitored or tracked easily by external users on the internet. Other factors that make IoT devices vulnerable are inadequate standards for device manufacturers, no standard protocols for security, lack of regulatory mechanisms and lack of data protection mechanisms. These aspects make IoT devices vulnerable to cyberattacks easily by malicious users.

Blockchain to secure IoT is much needed as there are billions of IoT devices globally that participate in applications to exchange data. As security configurations are weak in devices, data theft and hacks have become common. Hence blockchain security focuses on data storage security in the form of blocks that are encrypted using cryptographic techniques. Blockchain has proved to resist hackers and hence security for data storage using blockchain is much focus in studies. There are areas such as user and device authentication methods in existing WPA encryption methods as this method can compromise easily. The blockchain authentication scheme is found to be more secure as users are approved by existing users to access blocks and hence have better control.

In IoT forensic investigations, blockchain can prevent unauthorised access to have better control of IoT devices. Further blockchain security ensures access control and data sharing in all IoT devices are easily done to determine reliable user identification, authentication and data exchange. For instance, if the IoT device is an IP camera in a smart home application, the access to camera

is granted only with trusted devices in the smart home. In this manner significant number of connections are secured and each device is verified in forensic investigations. In this manner, the security of digital evidence traces obtained from IoT can be secured from tampering or compromise to support investigations.

Theme 3: Blockchain and Forensic Process

Digital forensics involves multiple technologies, a variety of systems and devices and expertise in cybersecurity management. Legal proceedings involving digital crimes depend on digital information as an acceptable form of evidence and are often mandatory to determine the grounds for crime activity. The purpose of DF is to conduct technical investigations within the boundaries of the legal system in response to criminal activity involving digital devices. DF investigations support both civil and criminal cases. Hence, due to disputes between the parties involved, there is a need to perform forensic tools such as eDiscovery in the given context. Trained investigators collect, analyse and reconstruct events and actions to support prosecution.

With the increase in IoT devices, the scope of digital investigation has also increased. Hence an effective team is needed with expertise in mobile technologies, onsite investigations, data networks, forensic readiness planning and data recovery and evidence preservation. Therefore, DF investigations can be understood as an attractive approach for technical users as a storage medium and devices involved in the network are thoroughly analysed to identify digital traces.

Blockchain due to its characteristics of immutability and links through cryptographic algorithms prevents modification of existing data blocks and forensic data retrieved and stored as data blocks. The blocks that contain evidence information will be available permanently and accessible only by authorised users. These are some of the reasons that have influenced the use of blockchain in

financial institutions, especially banking and insurance. Also, the blockchain holds accountable the participating users for their blocks as each recorded transaction as a block is registered in the distributed ledger only after all the users have approved. These characteristics make blockchain stronger to attacks or modifications.

In forensic investigations, provenance tracking is an important requirement as it records the origin and movement of crime-related data and seized hardware devices. The challenge is when the devices can be tampered with and important evidence data stored on them could be erased accidentally or deliberately or stolen. With blockchain, a chain of custody (COC) can be created to store digital evidence compared to a paper-based solution that can be easily destroyed. Hence, in this case, if an electronic device is seized a virtual token is created to ensure the certificate of authenticity for the item during the time of investigations. Given the above aspects, the role of blockchain is significant in DF investigations involving IoT devices.

The role of blockchain cannot be ignored in DF processes for the following reasons,

- Support investigations in IoT device misuse or attacks
- The evidence identified is preserved and protected from modification or theft
- Investigators can easily find the person who has handled the evidence from the blockchain ledger
- The actions performed on evidence can be described easily
- each block has a time stamp and hence investigation is easy to document
- To develop new solutions using new technologies

Theme 4: IoT forensic procedures

Digital forensics involves the procedures of identifying, preserving, analysing and documenting

digital evidence to solve digital crimes. The above procedures are followed in investigations and presented in a court of law to support in solving the case. IoT forensics is similar to digital forensics but the process deals with IoT infrastructure and investigations are performed in an IoT environment. A number of devices such as IT hardware, motion detectors, cameras, and sensors are investigated for evidence data. Hence, conventional tools used in digital forensics cannot be employed directly to investigate IoT environments. The other issues include detecting IoT devices, storing detected evidence information, jurisdiction, inappropriate evidence management, blurry boundaries and securing a chain of custody in an inadequate standard. In these environments, there is a set of procedures to follow in IoT forensic environments. The procedures include,

- Identification- refers to the identification of devices that are compromised or needed for investigation and analysis
- Collection- involves evidence data collection
- Preservation- refers to the storage of evidence information, here the role of blockchain is essential. The evidence data collected is stored as blocks
- Examination- implies the evidence is examined for its relevance in the case
- Analysis- the collected data is analysed to understand the chain of events that led to the crime
- Presentation- the evidence gathered and analysed is presented as a report to support legal proceedings.

The above procedures are also the steps in IoT forensic investigations, mostly followed in the same sequence as provided.

Forensic investigations in IoT networks and applications can be performed after an attack is identified on the devices. The existing procedures followed in digital forensics may not work correctly in IoT forensics and it is not suitable. This is due to the limited storage capacity of IoT devices which often leads to data getting over-written or destroyed. Basically, a dynamic mode is followed to retrieve data from live IoT devices as there are running processes, network logs and device memory. The running processes will provide more relevant evidence in the investigation.

The forensic investigation in IoT must be done in three layers namely the device, network and cloud levels. The device-level forensics will gather data from the local memory of the physical device and further analyse it. The network-level forensic will gather data related to traffic logs, sources, and destinations or can even provide the identification of a suspect or attacker. IoT environments involve a variety of networks namely LAN, WAN, body area networks (BAN), and Metropolitan area networks (MAN). Each network provides varying degrees of data to support in investigation process. Lastly, cloud forensics is difficult as IoT devices exchange data with cloud servers for storage and processing and hence these data must be identified and traced to gather evidence information. Further clouds are distributed in other countries/continents and hence this is another challenge to overcome in forensic investigations.

Theme 5: Blockchain performance in IoT forensic investigation

The important aspect of the problem in DF is to preserve and manage evidence data. Digital proof is very crucial in crime investigations and legal proceedings as digital evidence links a person with malicious activity. Therefore, it is important to guarantee integrity, authenticity and audit of digital evidence. All these aspects emphasize the need for a chain of custody as evidence data is usually distributed information that must be maintained as a tamper-proof arrangement that can store

individual transactions. In order to ensure these aspects the performance of blockchain comes into play. Blockchain supports forensic investigation in terms of data integrity, security and trust. In addition, the following performance aspects in blockchain are noted that make it ideal for IoT forensic investigation.

- The tamper-proof timestamps in each block that holds evidence data will help to preserve the integrity and availability of information as and when needed.
- The decentralised nature of blockchain allows the investigation team members to include new users or nodes as and when needed. Further, there is no central authority and hence all verified blocks are available to all the users to view. Users can create new blocks with new evidence data that will be verified and stored permanently in the distributed ledger.
- All transactions are verified by all authorised users and stored as a block. Once a block is stored it cannot be modified or deleted. This is much needed to protect evidence data from malicious users, both internal and external.
- The security and integrity of blocks is ensured with strong cryptographic function. Further, the use of a digital signature preserves the data from attacks and integrity is maintained.

In view of these performance areas in blockchain technology IoT forensics will become effective in view of the restrictions and challenges found in IoT devices.

Further, the role of blockchain in IoT forensic investigations cannot be undermined for the following reasons,

- Blockchain supports storing evidence data obtained from heterogeneous networks and devices. For instance, as each physical device will have a unique ID in the network, the evidence data can be stored with proper reference for easy identification of the device.

- The network will control the flow of data and establish short routes using IoT nodes. Here investigators can easily identify devices that interact based on their unique ID, instead of verifying a large number of devices.
- Usually, all data in IoT applications are stored on a cloud infrastructure the blockchain transactions are secured in the IoT network.

The performance of blockchain plays an essential role in storing evidence data and ensuring data is secured.

Theme 6: Blockchain preserves the integrity of digital evidence in IoT forensic investigations

Blockchain integrated with IoT forensics provides a lot of opportunities as it opens new doors for data security and evidence protection. Blockchain helps to build trust between parties in the organisation along with ensuring trust between different devices due to its security characteristics. Blockchain allows only verified devices to participate in the investigation process and allows devices to communicate in the network, further, the transaction blocks are verified by authorised personnel and stored in the distributed ledger. Blockchain reduces costs for the investigating organisation as there is no centralised entity or authority or a third party. In this case, the cost is reduced as the forensic investigation team will be able to record all types of transactions that can support the criminal case. Time is reduced as opposed to other conventional digital forensic investigations because the transactions are recorded immediately and verified by the users. In addition, improved security and privacy for data is a major advantage that ensures evidence data is protected, and the blocks created by the users will have details of the user, thus ensuring privacy and accountability. Lastly, blockchain is failsafe, this implies that even if the ledger database is lost in one node, it is available on the other nodes due to its distributed ledger characteristic, hence

failure rate is almost nil.

Blockchain is used for the preservation, storage and analysis of evidence and is most suited for securing data from common attacks and hacks. However, since IoT devices work autonomously a reliable method to gather residual evidence from digital devices is still a challenge. The utilisation of intrusion detection systems (IDS) helps to identify malicious activity on the network and prevent future occurrences is one of the options. However, in IoT environments, crime scene boundaries are difficult to accomplish as interactions between devices occur in real-time. Hence, the majority of IoT devices make use of privacy to record personal information that will be useful for forensics investigations.

Further, the evidence must not be modified or tampered when data is transferred between authorised users or entities. Here, blockchain certifies the major requirements related to authenticity of information transfer, legitimacy of procedures along with reliability. These aspects help in gathering and storing digital evidence and all interactions are provided with the COC. Hence, the COC members will have access to read and write new blocks in the digital ledger that are further verified and stored based on consensus. Given these aspects, blockchain records actions taken by forensic investigators and allows interactions for verification and creation of new information. Such evidence information is helpful in discovering criminal events that can be used as evidence in courts. In this manner, blockchain ensures digital evidence preservation.

Theme 7: Blockchain provides guarantee in IoT forensic process

IoT forensics is an important area where security is essential to preserve evidence data. In DF the evidence is related to identifying how the attack has happened and who is responsible for the incident. Whereas, in IoT environments digital forensic investigations will involve gathering

evidence data from different locations where traceability and integrity are highly important. Further data obtained from multiple sources must be done in a transparent manner, secured and maintained in a tamper-proof system. Blockchain technology has the capacity to fulfil all IoT forensic requirements as it can provide better performance in the IoT environment along with supporting traceability and integrity at high levels.

Blockchain benefits are highlighted in discussions. It is important to note that due to its immutability characteristic blockchain allows permission only to authorised members such as the forensic investigation team. In addition, blockchain enables improved security, transparency and traceability in addition to cost reduction and efficiency along with automation. Since blockchain will restrict the number of nodes or users in private and federated blockchain solutions, it significantly reduces overhead and ensures evidence is preserved as each user or node accountability is established after digital evidence is verified by all users.

5 Chapter 5: Discussion and Conclusion

5.1 Discussion of Research questions

The thematic analysis provided the findings to emphasise the need for blockchain as a reliable technology solution for IoT forensics in view of the challenges and vulnerabilities in IoT devices. It is noted that blockchain provides the potential for preserving the integrity of digital evidence from tampering and from threats, both internal and external. In addition, the analysis based on themes highlights the importance of forensic procedures and the guarantees provided by blockchain in IoT forensic investigations. Further, the research questions are addressed based on literature and thematic analysis.

RQ1: How can blockchain technology support digital forensic investigation, especially IoT forensic investigations?

As explored in literature IoT forensics or IoTF involves evidence gathering in devices and systems along with elements in the IoT network environment. The challenge of preserving evidence from IoT systems is underlined in studies. This implies there is a need for protecting IoT devices by examining the range of devices and protection from tampering or misuse from internal or external threats. Thus, there is an essential need in the organisation to maintain the extracted evidence data and ensure privacy is preserved along with identity management. These are important in forensic investigations as highlighted for studies as explained in studies by Horsman (2022).

As explained by (Ahmadi-Assalemi et al., 2020), blockchain with its potential for preserving privacy, data integrity and confidentiality can play a significant role in evidence preservation while mitigating breaches and not allowing data for misuse or erasure or data. In addition, blockchain

due to its reliability can support a COC for IoTF as recommended in studies. Ahmad et al., (2020) explain that CoC can help to resolve challenges in preserving evidence data retrieved from IoT devices that are compromised. CoC explains the need to support evidence gathering, storage, verification and restricted access to evidence data. Blockchain can fit in these requirements because the digital ledger platform allows the storage of data that is verified as correct. This implies the evidence data must be verified by all the investigating team members to store and record data on the blockchain database. Further access is not allowed for all users. There are different blockchain models namely consortium, permissioned and permissionless blockchain. Also, there are types such as private blockchain and public blockchain. In the case of consortium blockchain the users with access to evidence data on the blockchain can consist of a small team to include the management and investigators. Further, if the blockchain model is permission, only those users with permissions can access and view data on the blockchain. In this manner, blockchain will support ensuring the reliability, integrity and privacy of data stored on the digital ledger database. Therefore these aspects ensure the role of blockchain in supporting forensic investigation in IoT environments.

As explained by Romli, Prayudi and Sugiantoro (2019) in IoTF investigations authorised access to evidence data is important. Hence, there are a few important steps namely trust, confidentiality, integrity and traceability are very important. For instance, the integrity of evidence is maintained by blockchain as the authorised users are themselves not allowed to modify or erase existing data. Any modifications are stored as a separate block verified by other members of the team. Further, the data blocks created by authorised users are stored with time stamps and other details that are easy to identify, thus ensuring traceability. Therefore, these characteristics in blockchain technology will ensure data availability and continuity of possession of evidence. Further, if

evidence is shifted from one location to another, blockchain allows access from any location as the distributed ledger database is easily available on networks and services. Al-Hussaeni et al. (2022) explain that evidence data is easy to monitor thus supporting exhibits to present in court. Also, courts require data integrity and confidentiality that is easily made available by immutability and reliability thus ensuring digital evidence and artefacts are preserved in a highly secured environment supported by blockchain technology.

Blockchain and IoTF integrate fully as blockchain can provide support in the preservation of data extracted from IoT devices and connected elements. While DF provides the basic steps of identifying evidence, using blockchain to store data from extracted compromised devices can be further analysed to prove a digital crime as the data will serve as evidence for the crime scene. Importantly, DF in IoT environments face challenges as explained in the literature (Nadeem, Saeed and Ahmed, 2020). Yaqoob et al. (2019) explain that due to the variety and number of IoT devices problems could arise in analysis. Hence, to overcome the problems for investigators all the data retrieved from IoT devices must be protected from any kind of tampering, misuse or loss. Blockchain technology supports these areas of data integrity and prevents unauthorised access manipulation or loss. A large number of studies emphasise the need for blockchain in IoTF investigations.

Given these aspects of digital crimes in IoT environments, evidence is highly critical for investigations by examiners. Investigators can derive support from blockchain by storing all evidence data from IoT devices on the blockchain's ledger database that provides immutable security and ensures the evidence is admissible in court and/or with other crime investigating agencies. Importantly access to blockchain databases must be restricted to a few users to mitigate the risks to information.

RQ2: How can blockchain improve the efficiency and integrity of digital evidence gathered during the IoT forensic investigation process?

Blockchain technology is important for preserving evidence data and is ideal for IoTF environments. The integrity and performance of gathering digital evidence are further ratified by blockchain by the creation of an immutable, and audited chain of data stored based on consensus and proof of trust thus establishing protection (Rajasekaran, Azees and Al-Turjman, 2022). The integrity of data is ensured because each block of data is verified before it is stored on the ledger database, and a block stored cannot be deleted or modified. Further, any modification or deletion of blocks is stored as a new block and further verified by all the members in the chain. In this manner, the integrity and reliability of digital evidence are maintained in blockchain.

Further blockchain ensures accountability, transparency and auditibility as its inherent characteristics in addition to immutability. Sharma et al. (2020) explain that these characteristics emphasise blockchain as a technology solution to store digital evidence gathered from IoT devices in cybercrime investigations. It is noted that in DF investigations, data extracted from devices is vulnerable to theft or erasure of data from the device, and this is a major challenge. The investigation process for the investigators is strengthened in blockchain as it uses the cryptographic hash function that will help investigators to self-verify the device and to establish an effective verifiable chain. From the literature, Janarthanan, Bagheri and Zargari (2021) state that the guarantees related to trust, immutability and transparency are provided by the cryptographic hash function.

IoTF investigations aim to identify data traces in IoT devices that will eventually lead to malicious activities by cybercriminals. This is required by the investigators as unauthorised actions in the

IoT environment can provide insights related to the source of malicious activity and the devices compromised. While these are needed, (Kruger and Venter, 2019) explain there are challenges related to unregulated IoT environments where there are no formal security standards for devices followed by device manufacturers which leads to IoTF investigations not having formal standards. The challenge is further compounded as IoT networks usually are connected with cloud systems as cyber-physical infrastructure thus increasing the problems in existing forensic investigation scenarios (Armoogum, Khonje and Li, 2021).

However, a large number of research papers highlight the use of IoT forensic investigations in cloud environments where trust is improved between cloud stakeholders and forensic investigations. A study by Li, Qinand Min, (2019) states that blockchain can become effective in these areas to mitigate fraud as it ensures authenticity and trust along with integrity and immutability in untrusted cloud environments. The use of blockchain in IoTF is highlighted by improvements in trust in evidence data and preservation. In this manner, the trustworthiness of evidence gathered in IoT environments is ensured. Further forensic activities are supported by blockchain by ensuring the integrity of evidence items and information used by examiners. Likewise, provenance is improved by validation of digital evidence in blockchain as the creation of cryptographic hash functionality will help investigators with evidence data and support further examination, especially in IoT environments. Further blockchain efficiency can be experienced as it provides scalability thus ensuring storage of a large number of evidence data in an organised manner. In another study, Cordi et al. (2022) explain that blockchain is highly resilient thus supporting investigators with confidence as the data stored on the blockchain is accessible and accountable to all the forensic investigation team. This is in addition to preserving data from tampering.

Given the above, blockchain provides the promise of a secured IoT forensic investigation platform as it can support overcoming challenges usually faced in conventional digital forensic processes. Blockchain technology is efficient thus improving the performance and reliability of forensic investigations as IoT devices are unregulated and networks are usually heterogeneous in nature. Further, blockchain technology and IoTF integrate well to identify data breaches through traceability and preserve crime-related information as the most important evidence required by the court. Thus the above aspects highlight and emphasise the need for blockchain technology in IoT digital forensic evidence preservation.

5.2 Recommendations

In view of the above thematic analysis and discussions, the following recommendations are presented for consideration of blockchain in IoTF.

Recommendations

- In the area of evidence storage, blockchain provides timestamps, information on the evidence, proof, hash and reference to the previous block. All these data are further approved by all users authorised to use the digital evidence on blockchain thus determining consensus. In view of these advantages, blockchain technology is ideal for storing evidence information in forensic analysis and investigations.

- Blockchain technology ensures all blocks are visible to other blocks and with each node or user in the blockchain network. Further, evidence from investigators is added to the blockchain and each block will have a unique ID, these advantages of blockchain ensure transparency and accountability while storing forensic evidence data.

- All blocks of data that are approved are synchronised in the blockchain network, and hence each authorised user viewing information is always current and updated. Modified blocks or cancelled blocks will remain in the network, and will not be erased physically, thus providing a trail of activity in IoT forensic investigations.

- The CoC in IoT forensics will be helpful in investigations as it provides the whole chain of evidence starting with the first evidence to the last evidence. This will also help in reporting and documentation.

- Blockchain provides transparency, authenticity, security and auditability along with preserving integrity. All these characteristics make blockchain an ideal technology solution for storing digital crime data.

- The blockchain network is unregulated and hence the investigation team can treat it as a trusted network without the need for validation. However, global standards have to ratify this recommendation for use in IoT forensic analysis to solve digital crimes.

- Other benefits include tracking the forensic chain of custody and data is stored and shared only with trusted participants.

In view of the above findings from research blockchain technology is highly recommended for digital and IoT forensic investigations to store evidence data.

5.3 Conclusion

The report provides detailed discussions related to digital and IoT forensics and the use of blockchain technology in storing evidence information. The main concepts related to digital forensics, IoT security and forensics are discussed in detail. A comprehensive literature review is

presented to highlight existing studies related to blockchain and IoT forensics. The IoT architecture and layers are discussed and presented to gain an understanding of security and working principles in IoT devices. It is noted that IoT devices are unregulated in the areas of security and trust and do not follow standard security protocols in their work. These drawbacks make IoT forensics vulnerable to attacks and risks. All these aspects are discussed along with challenges identified in IoT from existing literature.

Literature reviews also discuss the IoT forensic model to highlight the differences in forensic processes found in IoT and in conventional digital forensics. IoT forensics have unique challenges of their own that are provided in literature discussions. The role of blockchain in IoT forensics as a technology to preserve evidence data is highlighted as identified from existing research. It is noted that blockchain due to its robust security and trust is ideal for IoTF analysis and in storing evidence information protected from tampering or misuse. Studies related to preserving digital evidence using blockchain in IoT forensics were identified, reviewed and presented in literature review sections.

The research methodology followed is qualitative research along with mixed methods. The methods used are explained and justified for their choice and selection in the report. Thematic analysis methodology is chosen for this research as a large number of studies highlight the use of blockchain for evidence data storage in IoT forensics and digital forensic investigations. The themes were derived from existing studies and codes generated. The themes and codes are presented in the methodology sections along with justifications. The steps followed in the thematic analysis are explained along with a presentation of the thematic report to address in detail the objectives and research questions presented in earlier sections. The thematic report also emphasises the need for blockchain technology for evidence preservation in IoT forensics.

Discussions in general are provided along with recommendations. It is noted that blockchain is here to stay and will play a significant role in evidence data preservation to overcome most of the existing challenges related to security and trust in digital forensics in IoT environments.

Future work on this topic will involve practical work on preserving evidence data gathered from IoT devices to demonstrate the use of blockchain technology as an ideal security solution for preserving evidence data thus determining trust and reliability in solving digital crimes

6 References

1. Akhtar, M.S. and Feng, T., 2022. Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment. *EAI Endorsed Transactions on Creative Technologies*, *9*(31), pp.e2-e2.

2. Ahmad, L., Khanji, S., Iqbal, F. and Kamoun, F., 2020, August. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In *Proceedings of the 15th international conference on availability, reliability and security* (pp. 1-8).

3. Ahmadi-Assalemi, G., Al-Khateeb, H.M., Epiphaniou, G., Cosson, J., Jahankhani, H. and Pillai, P., 2019. Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 1-9). IEEE.

4. Alam, M.N. and Kabir, M.S., 2023. Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions. In *2023 4th International Conference for Emerging Technology (INCET)* (pp. 1-6). IEEE.

5. Al-Hussaeni, K., Brits, J., Praveen, M., Yaqoob, A. and Karamitsos, I., 2022. A Review of Internet of Things (IoT) Forensics Frameworks and Models. In *European, Mediterranean, and Middle Eastern Conference on Information Systems* (pp. 515-533). Cham: Springer Nature Switzerland.

6. Al-Khateeb, H., Epiphaniou, G. and Daly, H., 2019. Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. *Blockchain and Clinical Trial: Securing Patient Data*, pp.149-168.

7. Asmussen, C.B. and Møller, C., 2019. Smart literature review: a practical topic modelling approach to exploratory literature review. *Journal of Big Data*, *6*(1), pp.1-18.

8. Asmussen, C.B. and Møller, C., 2019. Smart literature review: a practical topic modelling approach to exploratory literature review. *Journal of Big Data*, *6*(1), pp.1-18.

9. Armoogum, S., Khonje, P. and Li, X., 2021. Digital Forensics of Cyber Physical Systems and the Internet of Things. In *Crime Science and Digital Forensics: A Holistic View* (pp. 117-148). CRC Press.

10. Aslan, O., Aktug, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), p.1333.

11. Attaran, M., 2023. The impact of 5G on the evolution of intelligent automation and industry digitization. *Journal of ambient intelligence and humanized computing*, *14*(5), pp.5977-5993.

12. Braun, V. and Clarke, V., 2022. Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, *9*(1), p.3.

13. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E. and Pavué, C., 2019, June. Blockchain solutions for forensic evidence preservation in IoT environments. In *2019 IEEE conference on network softwarization (NetSoft)* (pp. 110-114). IEEE.

14. Brotsis, S. and Kolokotronis, N., 2022. Blockchain-Enabled digital forensics for the IoT: challenges, features, and current frameworks. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 131-137). IEEE.

15. Casula, M., Rangarajan, N. and Shields, P., 2021. The potential of working hypotheses for deductive exploratory research. *Quality & Quantity*, *55*(5), pp.1703-1725.

16. Cordi, C., Frank, M.P., Gabert, K., Helinski, C., Kao, R.C., Kolesnikov, V., Ladha, A. and Pattengale, N., 2022. Auditable, available and resilient private computation on the blockchain via MPC. In *International Symposium on Cyber Security, Cryptology, and Machine Learning* (pp. 281-299). Cham: Springer International Publishing.

17. Dawson, L. and Akinbi, A., 2021. Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study. *Forensic Science International: Reports*, *3*, p.100198.

18. de Araujo Zanella, A.R., da Silva, E. and Albini, L.C.P., 2020. Security challenges to smart agriculture: Current state, key issues, and future directions. *Array*, *8*.

19. Djenna, A., Harous, S. and Saidouni, D.E., 2021. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), p.4580.

20. Erdem, A., Yildirim, S.O. and Angin, P., 2019. Blockchain for ensuring security, privacy, and trust in IoT environments: the state of the art. *Security, privacy and trust in the IoT environment*, pp.97-122.

21. Ghazal, T.M., Afifi, M.A.M. and Kalra, D., 2020. Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technology*, *63*(1s).

22. Gupta, B.B. and Quamara, M., 2020. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, *32*(21).

23. Hameed, A. and Alomary, A., 2019. Security issues in IoT: A survey. In *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)* (pp. 1-5). IEEE.

24. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A survey on iot security: application areas, security threats, and solution architectures. IEEE Access 7, 82721–82743.

25. Janarthanan, T., Bagheri, M. and Zargari, S., 2021. IoT Forensics: An Overview of the Current Issues and Challenges. In: Montasari, R., Jahankhani, H., Hill, R., Parkinson, S. (eds) Digital Forensic Investigation of Internet of Things (IoT) Devices. Advanced Sciences and Technologies for Security Applications. Springer, Cham

26. Kamal, R., Hemdan, E.E.D. and El-Fishway, N., 2021. A review study on blockchain-based IoT security and forensics. *Multimedia Tools and Applications*, *80*(30), pp.36183-36214.

27. Karie, N.M., Kebande, V.R., Venter, H.S. and Choo, K.K.R., 2019. On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, *1*, p.100008.

28. Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R., 2021. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, *9*, pp.121975-121995.

29. Kebande, V.R., Mudau, P.P., Ikuesan, R.A., Venter, H.S. and Choo, K.K.R., 2020. Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Science International: Reports*, *2*, p.100117.

30. Khan, A.A., Shaikh, A.A. and Laghari, A.A., 2022. IoT with multimedia investigation: A secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth. *Arabian Journal for Science and Engineering*, pp.1-16.

31. Kollolu, R., 2020. A Review on wide variety and heterogeneity of iot platforms. *The International journal of analytical and experimental modal analysis*, *analysis*, *12*, pp.3753-3760.

32. Kruger, J.L. and Venter, H., 2019. Requirements for IoT forensics. In *2019 Conference on Next Generation Computing Applications (NextComp)* (pp. 1-7). IEEE.

33. Li, S., Qin, T. and Min, G., 2019. Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Transactions on Computational Social Systems*, *6*(6), pp.1433-1441.

34. Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U. and Bastaki, B.B., 2021. The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*.
35. Mercan, S., Cebe, M., Tekiner, E., Akkaya, K., Chang, M. and Uluagac, S., 2020, May. A cost-efficient iot forensics framework with blockchain. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-5). IEEE.

36. Miloslavskaya, N. and Tolstoy, A., 2019. Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*, pp.103-119.

37. Mohanta, B.K., Jena, D., Ramasubbareddy, S., Daneshmand, M. and Gandomi, A.H., 2020. Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), pp.881-888.

38. Nadeem, K., Saeed, N. and Ahmed, N., 2020. A Comparative Study of Digital Forensics and Cybercrime Investigation. *Comput. Appl. Sci. www. erjsciences. info*, *2*, pp.161-171.

39. Qabil, S., Waheed, U., Awan, S.M., Mansoor, Y. and Khan, M.A., 2019, March. A survey on emerging integration of cloud computing and internet of things. In *2019 International Conference on Information Science and Communication Technology (ICISCT)* (pp. 1-7). IEEE.

40. Rajasekaran, A.S., Azees, M. and Al-Turjman, F., 2022. A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, p.102039.

41. Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K. and Choi, C., 2021. Threats and corrective measures for IoT security with observance of cybercrime: A survey. *Wireless communications and mobile computing*, *2021*, pp.1-30.

42. Romli, M.A., Prayudi, Y. and Sugiantoro, B., 2019. Storage Area Network Architecture to support the Flexibility of Digital Evidence Storage. *International Journal of Computer Applications*, *975*, p.8887.

43. Ryu, J.H., Sharma, P.K., Jo, J.H. and Park, J.H., 2019. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The Journal of Supercomputing*, *75*, pp.4372-4387.

44. Sadineni, L., Pilli, E. and Battula, R.B., 2019. A holistic forensic model for the internet of things. In *Advances in Digital Forensics XV: 15th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 28–29, 2019, Revised Selected Papers 15* (pp. 3-18). Springer International Publishing.

45. Sadique, K.M., Rahmani, R. and Johannesson, P., 2018. Towards security on internet of things: applications and challenges in technology. *Procedia Computer Science*, *141*, pp.199-206.

46. Saleh, M., Othman, S.H., Driss, M., Al-dhaqm, A., Ali, A., Yafooz, W.M. and Emara, A.H.M., 2023. A Metamodeling Approach for IoT Forensic Investigation. *Electronics*, *12*(3), p.524.

47. Sharma, D.K., Pant, S., Sharma, M. and Brahmachari, S., 2020. Cryptocurrency mechanisms for blockchains: models, characteristics, challenges, and applications. *Handbook of research on blockchain technology*, pp.323-348.

48. Servida, F. and Casey, E., 2019. IoT forensic challenges and opportunities for digital traces. *Digital Investigations, 28, pp.S22–S29.*

49. Sharma, B.K., Hachem, M., Mishra, V.P. and Kaur, M.J., 2020. Internet of Things in forensics investigation in comparison to digital forensics. *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, pp.672-684.\

50. Sheth, H. and Dattani, J., 2019. Overview of blockchain technology. *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146*.

51. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K., 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), pp.1191-1221.

52. Sundler, A.J., Lindberg, E., Nilsson, C. and Palmér, L., 2019. Qualitative thematic analysis based on descriptive phenomenology. *Nursing open*, *6*(3), pp.733-739.

53. Terry, G. and Hayfield, N., 2021. *Essentials of thematic analysis*. American Psychological Association.

54. Tian, Z., Li, M., Qiu, M., Sun, Y. and Su, S., 2019. Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences, 491,* pp.151-165.

55. Tyagi, A.K., Rekha, G. and Sreenath, N., 2020. Beyond the hype: Internet of things concepts, security and privacy concerns. In *Advances in Decision Sciences, Image Processing, Security and Computer Vision: International Conference on Emerging Trends in Engineering (ICETE), Vol. 1* (pp. 393-407). Springer International Publishing.

56. Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.A. and Hong, C.S., 2019. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, *92*, pp.265-275.