The Journal of Supercomputing
https://doi.org/10.1007/s11227-019-02779-9

A blockchain-based decentralized efficient investigation framework for IoT digital forensics

Jung Hyun Ryu[1] · Pradip Kumar Sharma[1] · Jeong Hoon Jo[1] · Jong Hyuk Park[1]

Abstract
Until now, there has been little research on digital forensics in the IoT (Internet of Things)-based infrastructure. Current digital forensic tools, investigation frameworks, and processes cannot meet the heterogeneity and distribution characteristics of the IoT environment. These characteristics are a challenge for digital forensic investigators and law enforcement agencies. To solve these problems, this paper proposes a digital forensics framework for the IoT environment based on the blockchain technology. In the proposed framework, all communications of IoT devices are stored in the blockchain as transactions, thus making the existing chain of custody process easier and more powerful. By using the blockchain technology, the integrity of the data to be analyzed is ensured and security is strengthened, and the preservation of integrity is made more reliable by a decentralized method of integrity preservation. In addition, since the public distributed ledger is provided, participants in the forensic investigation—such as device users, manufacturers, investigators, and service providers—can confirm the investigation process transparently. We simulated the proposed model to support the proof of concept.

Keywords Digital forensics · Internet of Things · Blockchain · Decentralization

✉ Jong Hyuk Park
jhpark1@snut.ac.kr; jhpark1@seoultech.ac.kr

Jung Hyun Ryu
jh.ryu@seoultech.ac.kr

Pradip Kumar Sharma
pradip@seoultech.ac.kr

Jeong Hoon Jo
Jojeong3766@seoultech.ac.kr

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul 01811, Republic of Korea

Published online: 15 February 2019

1 Introduction

As the penetration rate of the Internet has increased and devices have become ever smaller, society has become increasingly digitalized, devices have become more generalized, and more efficient electronic devices have been developed [1]. These achievements have also led to the creation of the IoT (Internet of Things), an environment in which many devices interact with each other. The complexity of the IoT system and the lack of an integrated standard interfere with the digital surveillance process and make it difficult for security and law enforcement agencies to collect forensic evidence forensically [2]. Nonetheless, national security agencies and organizations recognize that the development of acceptable IoT survey standards and strong security measures could ensure the success of their investigations. In addition, current digital forensic procedures, tools, and communication standards cannot deal with the highly heterogeneous nature of the IoT and the distributed infrastructure. The explosive growth of the IoT has led to an increasing likelihood of crime, which could lead to unexpected damage to the vast majority of cyber-criminals. In complex physical systems, sensor-sensitive data can be vulnerable or exposed because it travels through other networks, user devices, and communication paths.

However, in 2009, Nakamoto Satoshi proposed the blockchain technology [3]. This makes individual transactions safe and transparent and completely eliminates the need for traditional centralized methods. Originally, transactions between customers were recorded and managed within a central authority such as a bank. This centralized system, however, cannot be freed from threats by malicious attackers. On the other hand, the blockchain-based cryptocurrency can be traded without a central authority like a bank by sharing a common distributed ledger for all customers. This is because all transactions are made with the consensus of more than half of all customers. The integrity of each ledger is ensured by proving transaction details through Proof of Work (POW) every 10 min. Currently, the various types of blockchains are categorized into public, private, and consortium depending on whether the ledger is open or not. In the public blockchain, all participants can share and manage their ledgers. In the private blockchain, however, only a certain central authority can manage and share ledgers, while in the consortium blockchain, only verified participants can manage and share ledgers. This study applies the blockchain to the data integrity preservation method in the digital forensics process by considering the fact that the blockchain discloses the ledger and internal information to all participants, in order to verify and preserve the integrity of the information. Current data integrity verification methods in digital forensics are generally a way for investigators to collect digital evidence in accordance with legal procedures and to image the disk through professional digital forensic tools. In this process, digital evidence is verified by a central authority. However, this centralized method of integrity preservation carries the risk that evidence may be damaged by malicious insiders or attackers. Therefore, this paper proposes a method of integrity preservation in which the blockchain is applied to the digital forensic investigation process based on ledger transparency.

The main contributions of this research are as follows:

- It presents a discussion of the problems and limitations of digital forensics in the IoT environment.
- It proposes a framework for digital forensics in the IoT environment using blockchain technology.
- We simulated the proposed model to support the proof of concept and discussed future research direction.

In this paper, we discuss blockchain, existing digital forensics investigation process, digital forensics in IoT, existing research, and requirements of Sect. 2. And in Sect. 3, we propose main framework, block structure, workflow for IoT environment. Finally, we conclude this paper in Sect. 5.

2 Related works

Existing financial transactions are managed by a central authority for all customers. In this process, the ledger is the only way of ensuring the integrity of customers' financial information. However, cryptocurrency uses blockchain technology for the integrity preservation mechanism without a central authority such as a bank. The blockchain technology first appeared as a core technology of cryptocurrency. By using the blockchain, transactions between customers do not need a central authority. In cryptocurrency, the ledgers of all participants are shared and managed by other participants to ensure the transparency of the ledgers. Transactions between participants are guaranteed to be transparent by other participants. Since the storage of information is decentralized, it is impossible for malicious attackers or insiders to conduct information deception or a tampering attack. Furthermore, all transactions are performed with the consent of the other participants, which essentially prevents malicious participants from duplicating or denying transactions [3]. All participants are managers and supervisors. In general, blockchain technology is categorized into public, private, and consortium blockchains depending on the degree of disclosure of the ledger. In the public blockchain, all participants share and manage their ledgers. In this type of blockchain, all participants are subjects that supervise and verify the ledgers. In the public blockchain, participants can record and search ledgers, share common distributed ledgers, and receive incentives whenever they block to maintain the network. However, in this case, it is very difficult to change or update the blockchain system because this type of blockchain has no central authority. It is also inefficient because the process of verifying transactions is very long. In the private blockchain, the central authority manages the ledgers of all participants. Participation in a private blockchain network is possible only if the central authority allows it. In the case of this type of blockchain, it is easy to change or update the blockchain system because a central authority exists. As for the consortium blockchain, it is a combination of public and private. Transactions in this type of blockchain are made among previously authorized participants. These three types of blockchains can be applied according to the requirements of the field in which the blockchain technique

is required. The public blockchain can be used for transactions in a cryptocurrency system such as Bitcoin or Etherium, while the private blockchain can be used in cases where the central authority controls many participants, and consortium blockchains can be used for relatively small transactions between trusted partners.

Table 1 shows the general type of blockchain. The blockchain is divided as shown in the table below and applied differently depending on the purpose.

2.1 Existing digital forensic process

The digital forensic investigation process for existing traditional systems, such as personal computers and servers, consists of six stages: Preparation; Response; Evidence Acquisition; Transportation and Confirmation; Analysis; and Report. In the preparation stage of the investigation, preliminary work is carried out, such as checking an incident and acquiring the authority to investigate it. In the response stage, a crime scene is preserved and the media to be analyzed are acquired. In the evidence acquisition stage, the system and storage medium are acquired and the evidence is sealed. In the transportation and confirmation stage, the sealed evidence is carried to the investigation agency and the original is preserved. In the analysis stage, a copy is generated, and data are extracted, classified, and analyzed in detail. Finally, in the report stage, analysis reports are drafted and testified in court [4].

The data collected according to this procedure are sent to an analyst, who then analyzes the data according to the analysis request of the case manager. At this time, if the data source is analyzed, the data integrity may be impaired. Therefore, the data are copied to enable exactly the same analysis as that of the original data, and the data are imaged to facilitate the analysis. A write-block device is used to preserve the integrity of the original data, and duplication is performed twice to distinguish between analysis and storage. It maintains integrity by acquiring the hashes of the original data, analytical data, and archival data [4]. Preservation of the integrity of imaging operations is also performed in the same way as data replication. Thus, in Korea, the current process of obtaining data and preserving integrity in a digital forensic investigation depends on a central authority, such

Table 1 Types of blockchain technology

Features	Public	Private (consortium)
Read access	Everybody	Only authorized organizations
Transaction verification and permission	Everybody can join in network	Only authorized organizations
Transaction maker	Everybody	Only authorized organizations
Consensus algorithm	Proof of work permitting partial branching	Proof of work that does not allow partial branching
Access control	Everybody	Access control via private channel
Examples	Bitcoin, Etherium	IBM Fabric, LoopChain, R3 Corda

Applying the blockchain technology to digital forensic investigations in the IoT environment can safely preserve data integrity and simplify the chain of custody processes

as a responsible person, an analysis expert, the Supreme Prosecutor's Office, or the NIS (National Intelligence Service). The original data may be manipulated if the responsible person or expert is malicious, and their stability may be degraded because the hashing process used for integrity preservation is performed once throughout the data.

The existing digital investigation process cannot efficiently handle the heterogeneity and distribution characteristics of IoT-based infrastructures. Therefore, a digital forensic investigation in the IoT environment requires a process that has been optimized for the IoT-based infrastructure, unlike the existing digital forensic process and framework. Digital evidence exists in crime scenes with various data types. Important evidence can be found on the suspect's PC, laptop, external hard drive, USB, mobile devices (smart phone, tablet, etc.). In addition, since the capacity of digital media and storage devices varies, digital forensic investigation of each device can take a long time and a lot of resources [5]. To solve these problems, digital forensic research has been carried out for a long time. But digital forensics should be prepared to meet the new environment—the IoT. The IoT environment grows exponentially differently from the growth of the existing digital environment. Therefore, the existing digital forensic investigation method should be newly established for the IoT environment. Figure 1 shows the existing digital forensic investigation process at a real cybercrime scene.

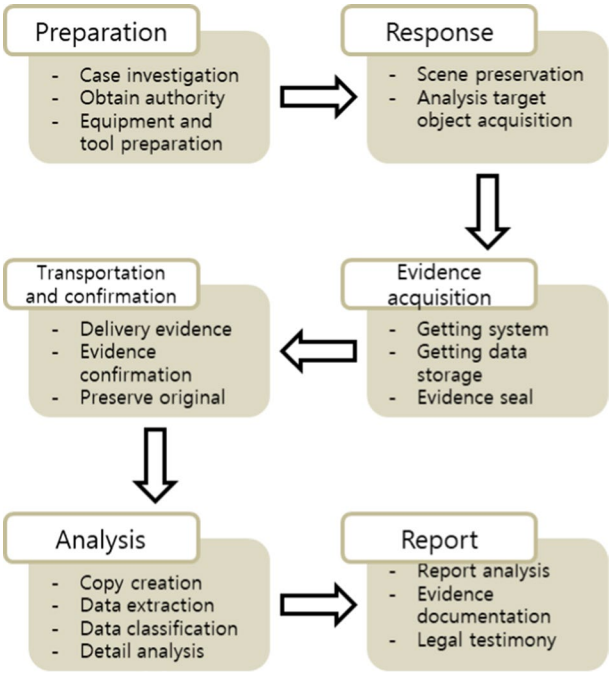

Fig. 1 Existing digital forensic process

2.2 Digital forensic in IoT

IoT forensics represents a forensic investigation of various IoT-based infrastructures that may be digitally investigated using conventional methods. It is categorized as cloud forensics, network forensics, and device-level forensics [2].

- *Cloud forensics* All IoT-based devices are integrated and shared resources in a virtualized environment to interact on the network using cloud services. Most cybercrime in the cloud-based IoT environment targets data generated in the cloud. This is due to the constantly increasing complexity of the devices that connect to the cloud and the nature of most data being centralized and dependent on the cloud.
- *Network forensics* Digital forensic investigation targeting networks is performed in an IoT environment using various types of networks. This is used to acquire abnormal attack log and perform digital forensic investigation process. This concept includes a home network, an industrial network, a LAN (local area network), a MAN (metropolitan area network), a WAN (wide area network) and so on.
- *Device forensics* Digital evidence collection of devices used in IoT environments. This forensic collects digital evidence from physical devices such as video, audio, NFC (near-field communication), memory and other IoT devices.

2.3 Existing researches

In this section, we present an overview of existing researches on digital forensics methodology in IoT environment.

- Zhang et al. [6] proposed a way to increase the reliability of the chain of custody in a forensic investigation in a cloud environment. Detailed recordings in the digital forensic process are essential for chain of custody. In this study, when data are collected during a forensic process, it suggests its source system. The source of this process increases the credibility of chain of custody.
- Kebande and Ray [2] suggested digital forensic investigation framework for Internet of Things environment. This framework presents three modules that include proactive processes, IoT forensics, and reactive processes. The proactive process represents a digital forensic preparation (DFR) process associated with activities for preparing the IoT environment forensically. The IoT forensic process represents a variety of forensic schemas that can extract evidence in an IoT environment. The reactive process represents a digital forensic investigation process that can occur after a potential security incident has been identified. Based on this framework, new digital forensic investigation procedures can be used to meet digital forensic investigation requirements for IoT's highly heterogeneous and distributed infrastructure.

- MacDermott et al. [7] discussed existing digital forensic limitations and digital forensic challenges in the IoT environment. In their paper, they presented the direction of digital forensics in IoT environments by dividing the weight of digital evidence and data sources in a smart-city environment. Also, they discussed the need for a suitable method of digital forensic investigation today, changing from IoT to IoA (Internet of Anything) era.
- Cebe et al. [8] proposed an integrated lightweight block-based forensic framework for digital forensics for smart vehicles. The goal of this forensic framework is to resolve legal disputes and prove objectively the defective vehicle in the event of a traffic accident. The evolution of smart vehicles presents new challenges for digital forensics in IoT environments. Unlike the existing forensic methodology, the sensor data produced by the decision-making entity can be used to establish an effective smart vehicle digital forensic investigation method. Manufacturer, driver, insurance company, investigator, etc. are considered as participants. They proposed and discussed an effective and reliable smart vehicle digital forensic framework.
- Oriwoh et al. [9] proposed a challenge and new approach to the digital forensic investigation process in the IoT environment. They explain that IoT is designed as a network of decision-making, self-managing systems. The impact of IoT on digital forensics is enormous in terms of the responsibility of cybercrimes caused by smart devices. The consequences of the interaction of IoT devices will have a significant impact on the practice of existing digital forensics. They predicted that digital forensics in IoT environments would be different from traditional digital forensics.
- Conti et al. [10] focused on security issues such as privacy, access control, secure communication, and secure storage of data in an explosively growing IoT environment due to the business potential. They explained that in the IoT environment, every single byte of communication data of devices could be investigated. They also presented challenges by categorizing the IoT environment into security and forensic perspectives. In particular, among the forensic challenges, evidence identification, collection and preservation explain how important it is to collect and manage digital evidence in a forensic investigation in the IoT environment. The authors argue that new digital evidence collection and management processes for forensic investigation in the IoT environment are needed in this paper.
- Kouwen et al. [11] described how digital forensic investigation methods for wireless communications technologies should be studied. They presented a survey of wireless communications equipment and services that a digital investigator could access in a crime scene or investigation. They performed forensic experiments on applications such as radio-based email, two-way radio, and push-to-talk and presented the results. They also point out that devices are increasingly being developed in an integrated direction, increasing the likelihood that wireless communications equipment will be used for cybercrime. As they said, there is a need to study forensic techniques in other areas than common system forensics.
- Sharma et al. [12] proposed distributed security SDN architecture for IoT using blockchain techniques for the limitations of IoT environments such as availability, security, and scalability as the number and variety of devices rapidly

increased. This architecture is a combination of SDN and blockchain technology, allowing untrusted members to peer-to-peer without intermediaries. In their paper, they shown that the proposed architecture allows real-time detection of security threats with low power overhead. This study is an example of applying the blockchain technology appropriately for the security element of IoT environment.

2.4 Problem statements

Today, most evidence preservation systems are based on a centralized repository structure consisting of third parties. This inevitably leads to various problems. Centralized structures always require strong safety requirements. Intrusion into a centralized storage node occasions serious problems, such as information leakage and data tampering. Like the current digital forensic methodology, the centralized structure is susceptible in terms of transparency and reliability. People are constantly questioning whether services are reliable. In addition, various IoT devices have different producers and service providers, so an integrated digital forensic framework is needed. This has a negative impact on forensic investigation and system scalability [13].

By contrast, distributed blockchained networks provide a transparent and reliable security environment where data can be protected through large-scale computing power. Trusted timestamps can be immediately attached to newly created blocks. Most importantly, it is possible to avoid trust issues by spreading the authority of the auditor. It demonstrates the integrity, accuracy, and timeliness required for preservation.

2.5 IoT forensic requirements

The following components are the requirements for a digital forensic investigation of the IoT [8].

- *Integrity* In all digital forensic investigations, the submission of evidence in court is the ultimate goal of digital forensics. Integrity is the most important factor from the beginning to the end of the forensic investigation.
- *Non-repudiation* Investigators should be accountable for the outcome of the trial by presenting objective evidence of the integrity and origin of the data.
- *Relieve single point-of-trust* The forensic investigation process in the IoT environment should mitigate the trust of a single entity and provide the reliability of each entity in a distributed method.
- *Persistence of forensic analysis* The forensic investigation process should provide access to historical data even before cybercrime occurs. A generic mechanism for crime analysis should be provided.
- *Lightweightness* Devices in the IoT environment must have a minimum overhead in the endpoints (device layer) because they operate with so many interactions.
- *Privacy* Due to the characteristics of the blockchain, all ledgers are shared to participants. In this case, invasion of privacy should be prevented in advance.

3 Blockchain-based digital forensic framework

In this section, we discuss an overview of the proposed framework, the structure of the blocks used in this framework, the participants in the blockchain, and the workflow.

3.1 Overview of proposed framework

Figure 2 illustrates the overview of proposed digital forensics framework for IoT environment. The proposed framework is divided into three layers: cloud; blockchain; and IoT devices.

Generally, in an IoT environment, devices communicate with the cloud. By 2020, the number of IoT devices is expected to increase to 26 billion [14]. In this case, it is almost impossible to investigate a large number of IoT devices using existing digital forensic methods.

Figure 2 shows an overview of proposed digital forensic framework for IoT environment in this paper. Each IoT device stores data generated in the process of communicating with other devices in the blockchain as a transaction.

The IoT environment includes all small environments using IoT devices: sensors; smart car; smart building; smart industry; smart home; smart grid. In all of these environments, cybercrime can occur at any time, and proper forensic framework for it must be established. In the IoT device category, devices have different purposes, services, manufacturers, technologies, and data types. IoT devices send and receive

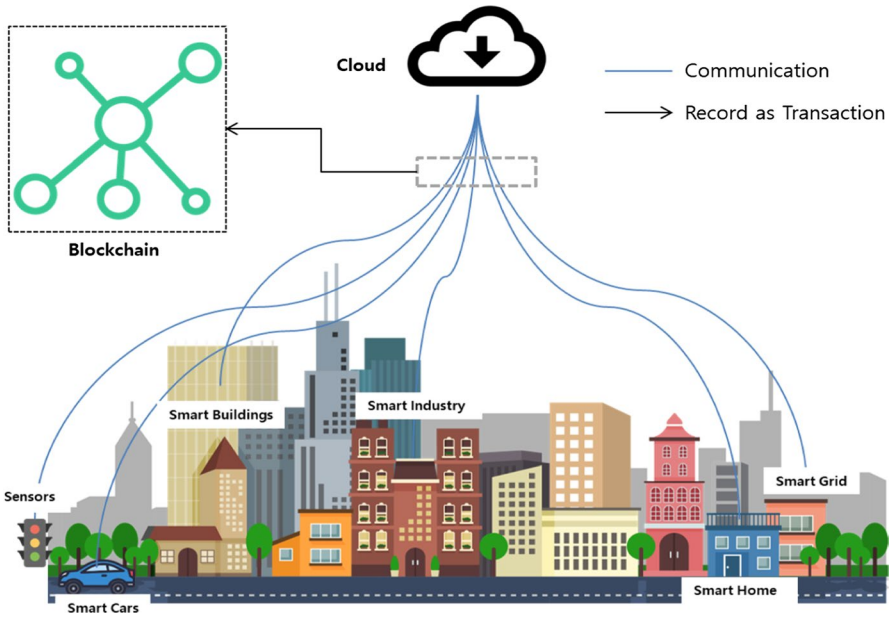

Fig. 2 An overview of proposed framework

large amounts of data regardless of device user's will. In this case, if the existing forensic method is applied to each device forming a large number of relationships, the investigation becomes very difficult. Therefore, in the proposed framework, the data generated in the process of communication of each IoT device are stored as a transaction in the blockchain. The digital forensic investigator exploits the stored integrity of blocks and the simplified chain of custody process.

3.2 Block structure of proposed framework

In this paper, we propose a block structure that is different from the existing block structure. Figure 3 shows the structure of the blocks used in the blockchain of the proposed framework. Blocks are divided into two sections: block header and transaction. The block header is divided into block number (Block #); Merkle tree hash; and timestamp. The block number is a number sequentially assigned to the generated block. The Merkle tree hash is used by investigators or other participants to locate transactions in a configured blockchain. The timestamp stores the time at which the block was generated. Transaction is divided into five sections: transaction ID (Tx id); digital signature; PUFsrc; PUFdst; and data. The transaction ID stores the result of performing the remaining sections (signature, PUFsrc, PUFdst, data) through the SHA-256 hash function. This is the unique identification number of the transaction. The signature contains digital signature generated by PUF ID and private key of sender IoT device. PUFsrc stores the PUF ID of the device that sends the data, and PUFdst stores the PUF ID of the device that receives the data. Finally, the data store data generated by communication between devices. In this paper, we propose a block structure slightly different from the existing block structure. In the proposed framework, blockchain is not used as an element of FinTech, but for ease of integrity in forensic investigation. Thus, a block is a concept of 'safe' storage of data that occurs between device and device, rather than an object that a user has to 'mining' competitively.

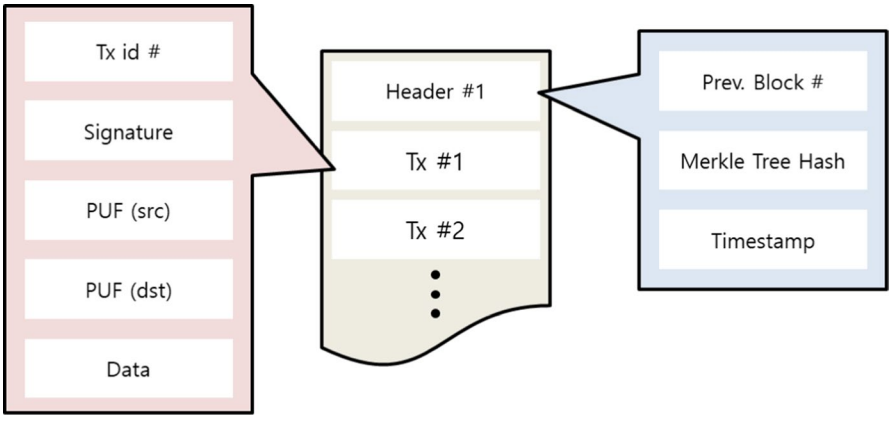

Fig. 3 Block structure for proposed framework

3.3 Participants of blockchain

The blockchain of the proposed digital forensics framework is divided into four categories: IoT device user; investigator; IoT device manufacturer; and service provider. The blockchain participants in this paper are the modified version of the blockchain participant structure proposed by Cebe et al. [8].

In a digital forensic investigation, a blockchain is used as a means of ensuring the reliability, integrity, and transparency of stored data, and provides shared ledger to all participants in order to manage information securely and efficiently. The information stored in the blockchain cannot be modified without consensus of all participants. In the cybercrime scene, the investigator may access the IoT forensic blockchain with the permission of the government authorities. At this time, participants other than the investigator can also use the blockchain information. This is because all participants in the blockchain share the same information to maintain the integrity of the information. An IoT device user may use blockchain information to cooperate with an investigator or to prove his innocence if his device is used for cybercrime. For IoT device manufacturers, blockchain information may be used to demonstrate defects in manufactured IoT products or to warrant the product. In the case of a service provider, blockchain information can be used for the guarantee of the service provided by the customer and the customer's personal information. The purpose of the content covered in this section is related to privacy issues in forensic investigation and blockchain technology. In the blockchain field, there are some solutions related to privacy such as Mixing Services, Centralized/Decentralized Mixing Services [15] or Publishing Transactions Anonymously, and Fetching Transactions Privately [16]. However, the privacy problem in the digital forensic investigation process is combined with the legal and administrative problems besides the technical perspective, so it is difficult to solve it by the technical solution alone. The main purpose of this paper is to simplify the integrity preservation process. The privacy issue in the digital forensic investigation process will be covered in a future study.

3.4 Workflow of proposed framework

Figure 4 shows a workflow of the blockchain-based digital forensic framework for the IoT environment proposed in this paper. In this proposed framework, we divide the framework into three layers: device layer (bottom layer); blockchain layer (middle layer); and participants' layer (upper layer). In this workflow, two IoT devices are used as an example. In the device layer, each IoT device communicates itself and exchanges data. Each device has a key pair and a PUF ID for digital signatures and exists in the IoT environment as many types of IoT devices. In the blockchain layer, which is the middle layer, we generate blocks using the data generated during the communication of each IoT device. The data sent from Device #1 to Device #2 is stored at the data section—bottom of the transaction. The PUF ID of the data sender Device # 1 is stored in the PUFsrc of the transaction in the block, and the PUF ID of the data receiver Device

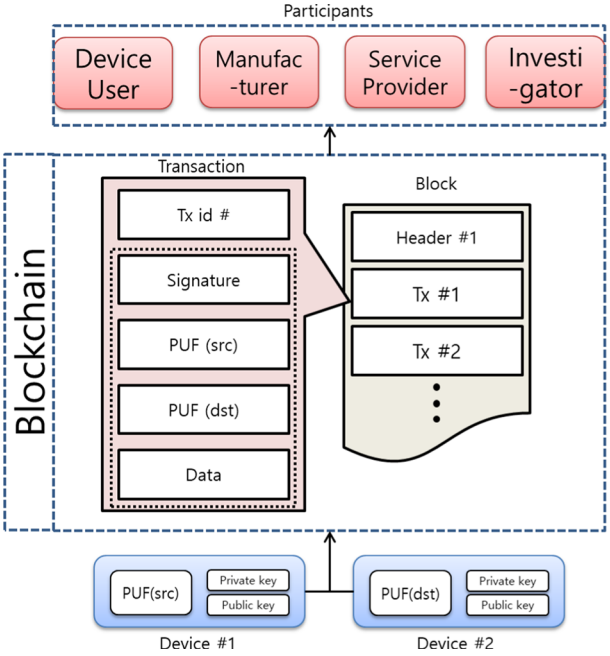

Fig. 4 Workflow of proposed framework

#2 is stored in the PUFdst. And then, generate a digital signature of the transaction using the private key and the PUF ID from the key pair of the sender Device #1. If the digital signature, PUF (src), PUF (dst), and data are all stored, it is hashed twice using SHA-256 hash function and stores the result in transaction id—Tx id section, the top of transaction. When the above-mentioned process is completed, one transaction is completed, and then, the transaction is continuously recorded for the next communication. If all transactions exceed the block size, the next block is created and linked to the previous block. In the participants' layer, which is the upper layer, when a crime occurs, each participant (device user, manufacturer, service provider, investigator) can check the open ledger of blockchain. For example, the investigator can verify that Device #1 is a legitimate sender by decrypting the digital signature of the transaction using the public key of Device #1, the data sender. Through this workflow, each participant can verify the integrity of the information transmitted by the IoT device. In particular, investigators can reduce the resources consumed by the chain of custody processes that are performed to demonstrate the integrity and transparency of data.

4 Experiments and analysis

4.1 Experimental environment

To support the proof of concept, we simulated the proposed model prototype using the Ethereum private network platform. The Etherium is a blockchain technology that is designed for smart contracts in essence, with Turing completeness and excellent scalability [17]. We refer to the Bitcoin as a blockchain technique in the introduction of the paper, but we use Ethereum as an experimental basis for reasons such as ease of experiment and visibility of results. Ethereum uses the Proof of Work (PoW) consensus as Bitcoin. In this paper, the concept of a smart contract is needed because the blockchain is not used for FinTech, but is used for recording the transmission process of the IoT device as a transaction. For simulation, we installed Geth [18] to set up a private blockchain and configured the blockchain consensus and smart contracts. Geth is a command line interface to run full Ethereum. We constructed smart contract interfaces for evidence generation, acquisition, and report generation using Mist Browser [19]. Mist Browser is a powerful tool to interact with the blockchain components like smart contracts, Ether, transactions blocks, etc. The desktop for experiment had 64 GB DDR3 RAM and an Intel i7 processor. Note that due to limited resources of our laboratory, we have currently built a prototype to evaluate the feasibility of our proposed model. We will expand the system model to build a comprehensive forensic framework model for future work.

4.2 Analysis

In addition to the results shown in Fig. 5, we measured the gas consumption with respect to the size of the blocks and number of transactions. The gas indicates the cost consumed by the proposed model to generate the evidences, while the size (bytes) represents the size of transaction blocks in our private blockchain network. The evidence generation by the transaction was simulated up to 800, which is the same in Fig. 6. The reason for limiting the number of proofs to 800 is that the performance of the experimental desktop is expected to affect the experimental results when simulating more than 800 evidences. In this simulation, as the evidences generated increased from 1 to 800, the block size due to transaction growth increased from 0.4 to 1.34 KB. At this time, gas consumption increased from 1.3 to 5.0. In this case, assuming 10 Gwei (1 Gwei is 0.000000001 Ethereum) per gas is used for fast transmission—as of September 12, 2018, 5 Gwei for standard transmission, 10 Gwei for fast transmission [18], we will pay 0.00000005 Ethereum (5.0 Gas * 10 Gwei), to cover 800 pieces of evidence. We also record the execution time of generating evidence through our smart contract. Figure 5 shows the gas consumption, with respect to execution time and number of transactions in our smart contract. The result shows that the cost of processing evidence generation (in terms of gas consumption) varies with block size and

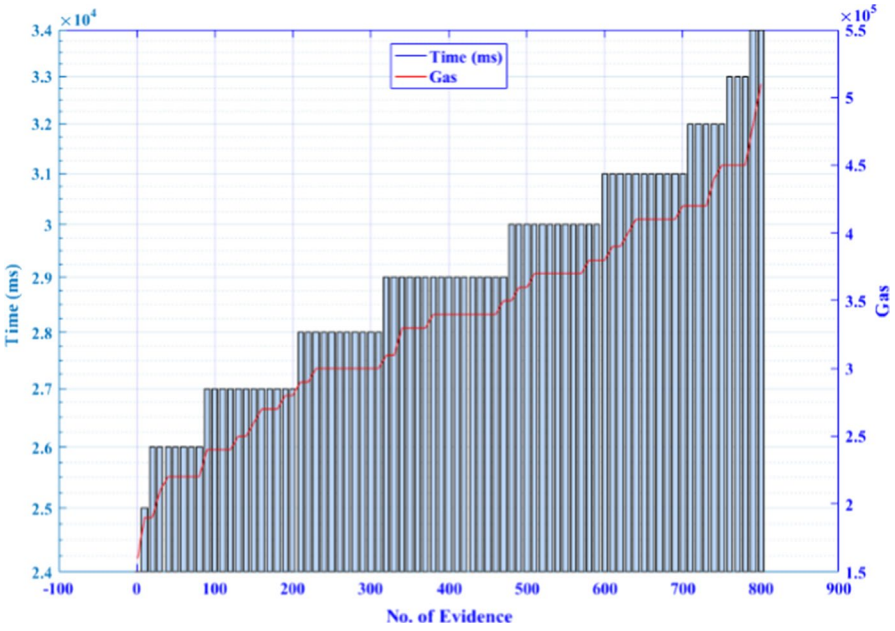

Fig. 5 Gas consumption with respect to execution time and number of transactions

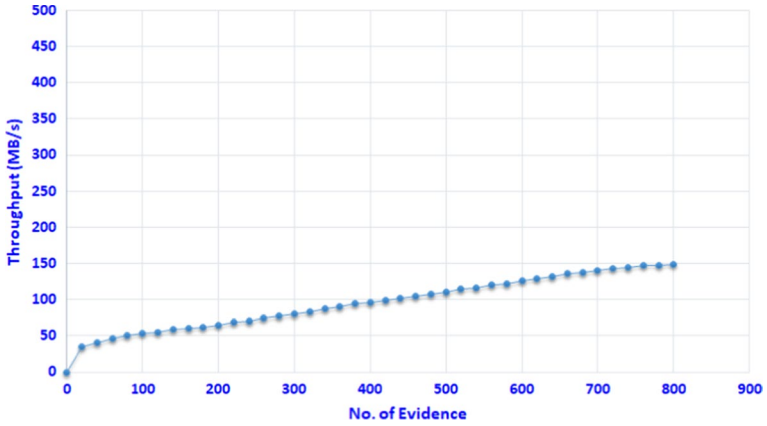

Fig. 6 Throughput with respect to the number of evidence

execution time. Currently, we have built a prototype to evaluate the feasibility of our proposed model. We will expand the system model to build a comprehensive forensic framework model for future work.

To evaluate the effectiveness of the proposed framework, we also analyzed the throughput and CPU utilization. The important factors to analyze the scalability of the proposed model are the relationship among the throughput and CPU utilization

with respect to the number of evidence generation. Figure 6 shows the relationship between throughput and the number of evidence generated. Increasing the number of participating nodes increases the throughput. Thus, an additional node could be deployed in the model, resulting in higher throughput. In addition, for performance issues, we have recoded the overall average CPU usage against the number of evidence generated. Figure 7 shows the CPU utilization varies with the number of evidence generated. The linear growth in CPU utilization as the number of evidence generation increases shows the scalability of the proposed framework.

5 Conclusions

In the current digital forensics investigation, preservation of data integrity is carried out independently by central authorities such as the Prosecutors' Office and the National Intelligence Service and Police. This has sufficient efficiency and procedural convenience, but the integrity of potential evidence may be compromised if a malicious attacker attacks the central authority. In addition, human and material resources are consumed in maintaining the chain of custody to preserve integrity in the investigation process [20]. Unlike today, in order to have proper digital forensic investigation in large-scale IoT environments, the current chain of custody process must provide a more robust integrity preservation approach and simplified procedures.

Therefore, in this paper, we propose a blockchain-based digital forensic framework for IoT environment to solve heterogeneity and distribution characteristic of the IoT environment and the centralization of existing forensic investigation. Blockchain technology is the safest and most secure technique to preserve data integrity at the present time. We also present modified block structure and workflow of proposed framework for investigation. In near future, we will study the execution time and time complexity of proposed digital forensic investigation framework and apply it to actual digital investigation.

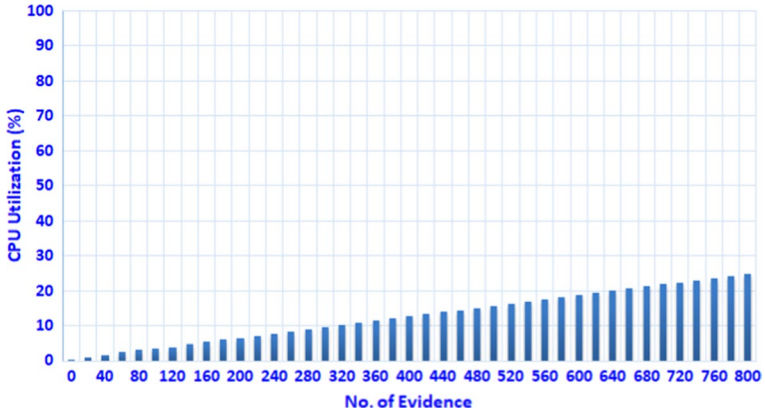

Fig. 7 CPU utilization with respect to the number of evidence

Our next goal is to test more IoT devices, use-case scenarios, and apply proposed framework to real digital forensic investigations. These goals will be evaluated in various IoT environment-based digital forensic frameworks. In addition, we plan to conduct simulations considering various IoT-based environments such as smart city, smart home, smart industry, and smart car.

Acknowledgements This work was supported by Institute for Information and communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2018-0-00644, Linux Malware Dynamic Detection and Protection Solution on Embedded Device).

References

1. Sharma PK et al (2018) Li-Fi based on security cloud framework for future IT environment. Hum Cent Comput Inf Sci 8:23
2. Kebande VR, Ray I (2016) A generic digital forensic investigation framework for Internet of Things (IoT). In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)
3. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. http://www.bitcoin.org
4. Harbawi M, Varol A (2017) An improved digital evidence acquisition model for the Internet of Things forensic I: a theoretical framework. In: 2017 5th International Symposium on Digital Forensic and Security (ISDFS)
5. Perumal S et al (2015) Internet of Things (IoT) digital forensic investigation model: top-down forensic approach methodology. In: 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)
6. Zhang Y et al (2017) A blockchain-based process provenance for cloud forensics. In: 3rd IEEE International Conference on Computer and Communications (ICCC)
7. MacDermott A et al (2018) IoT forensics: challenges for the IoA era. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)
8. Cebe M et al (2018) Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. Cornell University. arXiv preprint arXiv:1802.00561
9. Oriwoh E et al (2013) Internet of things forensics: challenges and approaches. In: 2013 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)
10. Conti M et al (2018) Internet of Things security and forensics: challenges and opportunities. Fut Gen Comput Syst 78(2):544–546
11. Kouwen A et al (2018) Digital forensic investigation of two-way radio communication equipment and services. Dig Investig 26:77–86
12. Sharma PK et al (2017) Distblocknet: a distributed blockchains-based secure SDN architecture for iot networks. IEEE Commun Mag 55(9):78–85
13. Wang M et al (2018) Lightweight and manageable digital evidence preservation system on bitcoin. J Comput Sci Technol 33(3):568–586
14. Rivera J, van der Meulen R (2013) Gartner says the internet of things installed base will grow to 26 billion units by 2020. Stamford, CT, Dec 2013
15. Feng Q et al (2018) A survey on privacy protection in blockchain system. J Netw Comput Appl 126:45–58
16. Henry R et al (2018) Blockchain access privacy: challenges and directions. IEEE Secur Priv 16(4):38–45
17. Ethereum private network platform **(online)**. https://www.ethereum.org/. Accessed date 04 Sept 2018
18. Geth (online). https://geth.ethereum.org/downloads/. Accessed date 04 Sept 2018
19. Mist browser (online). https://github.com/ethereum/mist. Accessed date 04 Sept 2018
20. Ryu JH et al (2018) Analysis of a third-party application for mobile forensic investigation. J Inf Process Syst (JIPS) 14(3):680–693