Internet-of-Forensic (IoF): A Blockchain Based Digital Forensics Framework for IoT Applications

Gulshan Kumar[a,b], Rahul Saha[a,b], Chhagan Lal[b,c] and Mauro Conti[b]

[a]School of Computer Science and Engineering, Lovely Professional University, Punjab, India
[b]Department of Mathematics, University of Padua, 35131 Padua, Italy
[c]Department of Intelligent Systems, CyberSecurity Group, TU Delft, Netherlands

ARTICLE INFO

Keywords:
IoT, Forensics, Digital, Blockchain, Custody, Security, Cloud.

ABSTRACT

Digital forensic in Internet-of-Thing (IoT) paradigm is critical due to its heterogeneity and lack of transparency of evidence processing. Moreover, cross-border legalization makes a hindrance in such process pertaining to the cloud forensic issues. This urges a forensic framework for IoT which provides distributed computing, decentralization, and transparency of forensic investigation of digital evidences in cross-border perspectives. To this end, we propose a framework for IoT forensics that addresses the above mentioned issues. The proposed solution called *Internet-of-Forensics* (IoF) considers a blockchain tailored IoT framework for digital forensics. It provides a transparent view of the investigation process that involves all the stakeholders (e.g., heterogeneous devices, and cloud service providers) in a single framework. It uses blockchain-based case chain to deal with the investigation process including chain-of-custody and evidence chain. Consensus is used for consortium to solve the problems of cross-border legalization. This is also beneficial for a transparent and ease of forensic reference. The programmable lattice-based cryptographic primitives produce reduced complexities. It shows benefits for power-aware devices and puts an add-on to the novelty of the presented idea. IoF is generic; hence, it can be used by autonomous security operation centres, cyber-forensic investigators and manually initiated evidences under chain-of-custody for man-made crimes.Security services are assured as required by the framework. IoF is experimented and compared with the other state-of-the-art frameworks. The outcomes and analysis prove the efficiency of IoF concerning complexity, time consumption, memory and CPU utilization, gas consumption, and energy analysis.

1. Introduction

The present world of technology is evolving around Internet-of-Things (IoTs) [1][2]. Wide acceptability and the advantages of IoTs have hold up a prediction of more than 20 billions of connections in near future [3]. The development of IoT infrastructure depends on its architecture. Among all, the three-layered architecture is mostly used in various applications [4] [5] as shown in Fig.1. It includes perception layer, fog layer, and cloud. Irrespective of various architectures, the basic functionalities of IoT infrastructure have been segregated in two major parts: perception and communication. Perception deals with the devices which are affiliated to an IoT network; while in communication layer the devices communicate with each other and transmit data depending upon the requirements of an IoT-based application and it also stores the data at cloud. Different intermediate layer(s) such as fog, dew, and cloudlets can exist which are used to reduce the delay of communication [6].

Along with IoT, the blockchain is also making significant market presence [7]. Initializing its journey with cryptocurrencies like Bitcoin, blockchain has now proved its advantageous significance in many fields [8][9]. Blockchain-based IoT systems improve transparency, and the distributed nature of this combination have given an overwhelming response in research fraternity [10]. The continuous development of IoT infrastructures and applications has also increased several concerns in cyber-world and security is one of them. More number of devices eventually leads to the greater number of vulnerabilities with a variety of security attacks. The sophistication of the digital crime techniques always has urged for a concrete security-forensic solution which is able to work on multinational framework. To this end, the key contributions of the proposed work are as follows.

- We propose a framework for digital forensics investigation that uses IoT as the backbone technology for evidence gathering and communications, and blockchain for digital forensic evidence management.

**Corresponding author
ORCID(s):

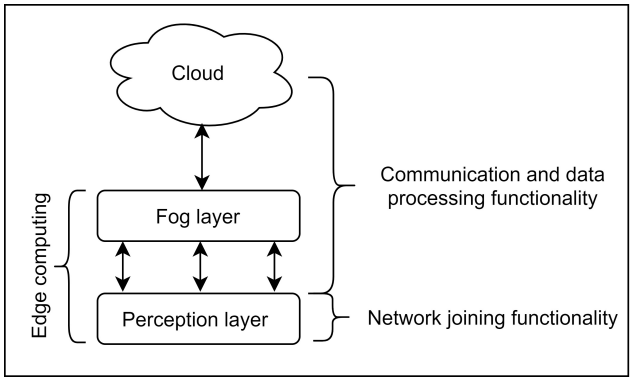

Figure 1: Basic layers of IoT

- The framework uses consortium blockchain to support a secure chain of custody through case-chain during the whole investigation process. The use of lattice based signcryption with programmable hash function makes the framework post-quantum resistant and less complex. The blockchain based case-chain provides a transparent mechanism for all the internal processes of a digital forensic investigation.
- The objective of the work is to solve the problem of transparency of investigation in the forensics of digital evidences. Digital forensics, more specifically network forensics applications are almost similar to intrusion detection; however, in the present solution not only network forensics, the suspicious devices will be under observation of memory forensics, system forensics and also cloud forensics as per the evidences perspectives.
- The experimental analysis shows the superiority of our system as compared to the existing frameworks in terms of complexity, gas consumption, energy consumption and resource utilization.

The rest of this paper is organized as follows. Section 2 reviews related work in the direction of IoT based digital forensic processes and its related blockchain applications. Section 3 explains the proposed IoF in details. Section 4 analyses the results and measures the performance, and finally, we conclude the work in Section 5.

2. Related work

In this section, we review some significant works for digital forensics directions and identify their pros and cons. This analysis establishes the present status of the digital forensics.

Authors in [11] propose Forensic-chain, a blockchain-based solution emphasizing on Chain of Custody (CoC). Proof of Concept (PoC) is developed in Hyperledger Composer. However, end-to-end complete framework is missing in this work. Digital witnessing and its privacy concerns are explained well by various researchers [12] [13] [14]. These works discuss about providing privacy features and access controls to the digital witnesses; management of the digital witnesses and the requirements are also well defined. But, the transparency of handling the privacy or access control imposition is missing. Therefore, problems still persist for a CoC against trust issues for the interaction or handling the records from all the stakeholders in cloud forensics. This has been addressed in [15]. The work shows a process provenance system with the use of Proof of Existence (PoE). Generic cryptographic group signature is used to perform the blockchain operations. However, the keys are assumed to be obtained from central nodes which may reveal the keys of the nodes. Vehicular forensic investigation has been researched in [16]. The solution is blockchain-based and provides a lightweight privacy-aware mechanism for vehicles. It eliminates the need of a trusted third party. Fragmented ledger is used with consensus; however, the integrity between the fragmented ledger and the shared ledger is not addressed. A permissioned blockchain solution for IoT forensics has been researched recently [17]. It provides a complete workflow of the evidences from gathering to disposing. Smart contracts are made for various transactions. Privacy of the identity is imposed using Merkle tree signature. Heterogeneity of the devices is not addressed in this work. Cloud forensics and forensics-as-a-service has been emphasized in [18][19]. A system-oriented design for supporting court ordered data access has been observed in [20]. It uses system-encrypted storage and per-device authorization protocols with the device manufacturer.

Forensic Investigation Framework (FIF-IoT) uses a public digital ledger to validate criminal events in an IoT-based environment [21]. It collects interactions of IoT entities as evidences and store them securely as transactions in a public, distributed and decentralized blockchain network. Thus, it eliminates a centralized control and avoids single-point failure. It also provides a mechanism to verify the integrity of the acquired evidence from the ledger. As the IoT devices are resource-constrained, the complexity of the proposed approach is a question and can be improved. We have considered this work as one of the candidates to compare our proposed solution. A secure Blockchain-based Digital Evidence Framework (Block-DEF) has been proposed by the researchers [22]. The original evidences are stored in a secured storage and evidence information is stored in blockchain. A lightweight blockchain is used and a name-based practical byzantine fault tolerance consensus is proposed. Multi-signature is used for evidence submission and retrieval. The mapping between the storage and evidence information need to be secure. This work is considered as another candidate for our comparative analysis. A simple and basic architecture of blockchain has been utilized for IoT forensics in [23]; it uses a public distributed ledger and all the IoT devices' communications are considered as transactions for storing in blockchain. Thus, maintaining CoC is easier. The complexity of the approach can be reduced further with the lattice based cryptographic protocols and therefore, it has been considered as a candidate solution for the comparison. Further, the integrity evaluation is also observed by using an open time stamp service in [24]. The method is claimed to be scalable; however, timestamp attacks and global time synchronization problem may create problem in the system. Blockchain-based Chain of Custody solution (B-CoC) is proposed for digital forensic investigation [25]. It is applicable for private and permissioned blockchain. It is comprised of Evidences DB, Evidence Log, and Front end interface, and it supports smart contract approach. The system lacks behind in latency and throughput; it can be improved; cryptographic features need to be robust and load distribution needs to be rechecked for IoT-fog interfacing.

Blockchain feasibility in cloud storage and various factors in cloud forensics are studied recently in [26]. Evidence reconstruction problem needs to be readdressed. A solution of Blockchain Assisted Secure Logging-as-a-Service (BlockSLaaS) is found in [27]. It handles multi-stakeholder collusion problem and provides integrity and confidentiality but faces privacy issues. We have considered this work as candidate for comparative analysis due to its proposed mechanism. A blockchain-based solution with integrity and spatio-temporal properties of digital evidences has been researched in [28]. This is an application that needs to be installed for a suspicious device as an evidence. Heterogeneity and compatibility are not addressed in the application. A privacy ensured blockchain-based solution for IoT forensics is shown in [29]. A preservation model for electronic devices for evidence process has been suggested recently [30]. It uses a blockchain approach to ensure backup, classification of evidence access rights, the decentralization of electronic evidence server, data security protection mechanism and guarantees information integrity traceability but, it does not confirm the IoT-based transactions. Another preservation approach for evidences has been identified [31]. It exhibits a lightweight digital evidence-preservation architecture to ensure privacy-anonymity, audit-transparency, function-scalability and operation-lightweight. The transparency is provided using an evidence audit network with Proof-of-Existence (PoE), instant timestamps. Irreversible hash functions are used for chaining process. The synchronization between evidence chain and the original blockchain of Bitcoin can be an issue in this work. The other approaches are summarized in the survey shown in [32].

The security aspects have always been considered as critical considerations for any type of networking applications. Among all the security services, encryption, hash and digital signature are the fundamental cryptographic tools that ensure the security services: confidentiality, integrity, and non-repudiation [4]. The traditional methods of "signature-then-encryption" face two problems such as low efficiency and high cost of combination. Arbitrary combinations are also questionable for security provisions. Therefore, to solve these problems signcryption has been introduced in 1997 [33]. It has been developed as a cryptographic primitive performing the digital signature and encryption functions simultaneously. Various researches are conducted to develop efficient signcryption schemes and other extensions are still in process. Significant usage of signcryption for IoT-based applications have been found in [34].

Apart from the chain-of-custody in digital forensics, there are several directions which urge for new developments. A conceptual model for planning, execution, analysis and dissemination of experiments has been shown in [35]. The model ensures reproduction of digital forensics experiments. For digital forensic experiments, the problems can arise from side-channel attacks on the security protocols and therefore, they need a solution. A significant solution in this direction is an open research problem [36]. Stitcher tool is developed for addressing the technical challenges faced by investigators [37]. These challenges are more critical for IoT-based digital forensics. Stitcher provides correlation and consistency in digital forensic evidences in such environment. Smart cities are one of the exemplary outcome of IoT developments. Being connected devices everywhere, such smart cities also require forensic applications. A review of digital forensics on biometric data for smart cities is analyzed in [38]. This review notifies future directions

of biometric-based digital forensics works. Trust aspects of the digital forensics are also in concern and need further exploration [39]. With a probability of misleading evidences or data manipulation in the evidences, various problems such as compression bombs, obfuscation, and steganography must be solved for trust validation of the digital evidences.

From the above discussion, we can observe that digital forensics opens up various pathways to enhance the present status. However, in this paper, we emphasize on the blockchain-based approaches; we notice that their completeness is missing and can be enhanced further. The advanced post-quantum resistant cryptographic methods, throughput, delay and energy consumption also provide a scope of exploration. Further, consortium-based solution is not also researched in recent times in this direction. This also urges for a complete solution to handle the cross-border issues of investigation which can also be marked as references for solving other criminal incidents. To address these problems we have come up with the solution of 'Internet-of-Forensics (IoF)' to provide a framework for digital forensic functions. The highlights of the novelty are:

- Compatible for heterogeneous devices of IoT perception layer as complexity and energy consumption is low.
- Use of consensus for consortium blockchain approach to solve the effect of cross-border legalization issues.
- Using a hierarchy of chains for Chain of Custody (CoC), Evidence chain (EC) and Case Chain(CC). It is combined as CoC-EC-CC. It provides granularity transparency of the investigation.
- Ensuring privacy-anonymity for the forensic witnesses to avoid manipulation of evidences.
- This evidence processing model can also work as intrusion detection system apart from manual evidence inclusion.

As per criticality is concern, the presented solution is more inclined to solve the forensics process transparency. The cross-border legalization is secondary part but important for the solution. It is expected that all the countries will come forward to be participant in the consortium so that crimes (digital or physical) can be minimized for sustainability. Moreover, putting the details of investigation in blockchain will also help other departments or investigation officers to follow the references and some hidden link to be identified if exists. The manipulation of evidences can also be prevented by the solution shown in the work.

3. Proposed Work

The transparent framework handling, the heterogeneous devices with their transactions, and enhancing the digital forensic investigation process with low complexity and low latency, are the essential requirements in any IoT infrastructure. Therefore, we propose IoF framework with the following assumptions: (i) national and international legalization offices are the members of the consortium blockchain, (ii) a trusted key generator-verifier is available, and (iii) perception layer is comprised of heterogeneous devices.

The proposed framework has been segregated in four layers: Edge-IoF, Fog-IoF, Consortium-IoF, and Cloud storage. Each of these modules have their own role and responsibilities, which are summarized below.

- *Edge-IoF:* In this layer, all the user devices (e.g., mobiles, laptops, smart devices, and other IoT appliances) are considered. As the framework is generic and flexible, any evidences related to manual crime can also be explicitly included with required access controls. Our solution also makes a proper synchronization between the storage information and evidence reports. As these devices have low power resources and low storage, the objective of the proposed framework is to provide low complexity. Therefore, we use a lightweight signcryption process which also provides confidentiality, integrity, and non-repudiation during data transmission of evidences in Chain of Custody (CoC) or out of CoC. Further, to protect the privacy of the devices and the officers handling the devices, we use anonymity-pseudo-identity by using lightweight cryptographic hashing technique. The original identity of the devices (Device/Hardware MAC or identification number by manufacturer) and the investigators are mapped with this hash value to avoid the chances of manipulation or any legal manipulative reaction. We can store this mapped data in fog level or cloud level. A separate privacy level maintenance can be added to decide which evidences can be put in blockchain process; however, it has been kept as future scope.
- *Fog-IoF:* Along with the fog devices (e.g., routers, switches, and gateways), we use the digital forensics applications and devices (e.g., network and memory forensic tools as required) at this layer. It is considered that the

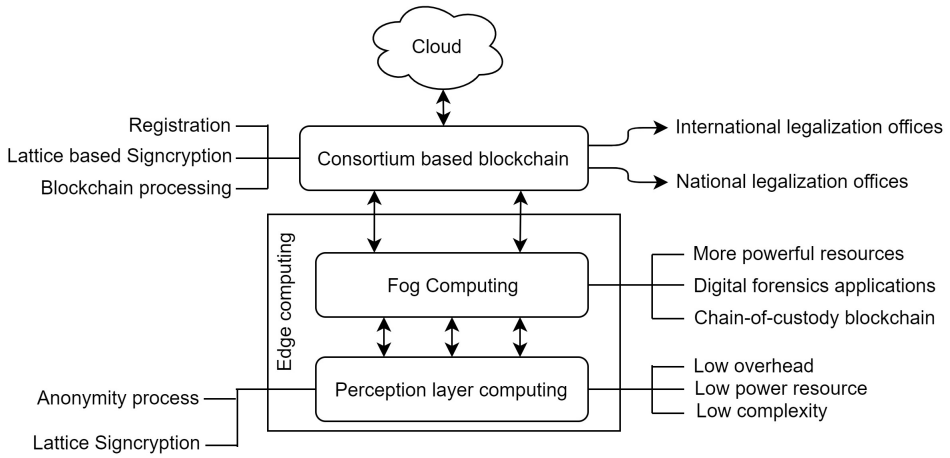

Figure 2: Proposed framework for IoF

devices at this layer are more resourceful; therefore, Fog-IoF layer can perform complex tasks of forensic analysis. It is also responsible for maintaining chain of custody of the evidences in a blockchain process to provide transparency in evidence access by investigation personnel.

- *Consortium-IoF:* This layer in the framework builds a blockchain of international and national level investigation organizations. It is obvious that, the attackers use various sophisticated tools and mechanisms for executing malicious activities; the identities of such attacks also face cross-border issues (such as IP address registration, domain names etc.) which delays the process of investigation. The consortium blockchain helps to make collaboration among the investigation organizations and provide the transparent evidence processing. Moreover, investigation trust among the personnel with cross-border countries and justified reference points of investigation enhance the importance of IoF.

- *Cloud Storage:* Generally, every investigation office can store their data in their clouds. These clouds can be connected in blockchain to provide tailor-made system for digital forensic purpose.

The functionality of each layer in the framework provides a suitable solution required for digital forensics in IoT-fog computing. The Fig.2 shows the schematic diagram of the proposed framework. In the following subsections, we have discussed about each layer of the framework and the advantages of IoF over existing frameworks. It also relates the technical aspects to achieve the properties of low complexity, anonymity, and blockchain provisions as it is shown in Fig.2. Note that, as per this figure, two blockchains are configured: one in consortium, another in fog layer for CoC; however, these two blockchains can be merged in public domain or can be used separately with some discrete access control mechanisms.

3.1. Perception layer

Perception layer consists of heterogeneous low-powered devices. Moreover, a manual entry of evidence is also considered here. Sometimes, it is also required to protect the privacy of the device and investigators till the evidence is produced in the court. Therefore, we use Programmable Hash Functions (PHFs) from lattices to provide security to the signatures, and also the identity of the user (devices and investigators) can be mapped to a pseudo-identity, and thus, IoF provides anonymity and privacy to the users [40]. PHFs are also used for signcryption process to ensure that only legitimate devices are the part of IoF. This lattice-based approach makes the IoF secure and ensures the confidentiality, authentication, non-repudiation, and integrity of the digital records in blockchain. Moreover, lattice-based cryptography can withstand quantum computing attacks with low complexity. Note that this framework is compatible for intrusion detection systems else unnecessary data storage in clouds will be occupied. In the experimentation, we also consider the devices as suspicious and have generated alerts for intrusion detection. The overall functioning in IoF is segregated into following processes.

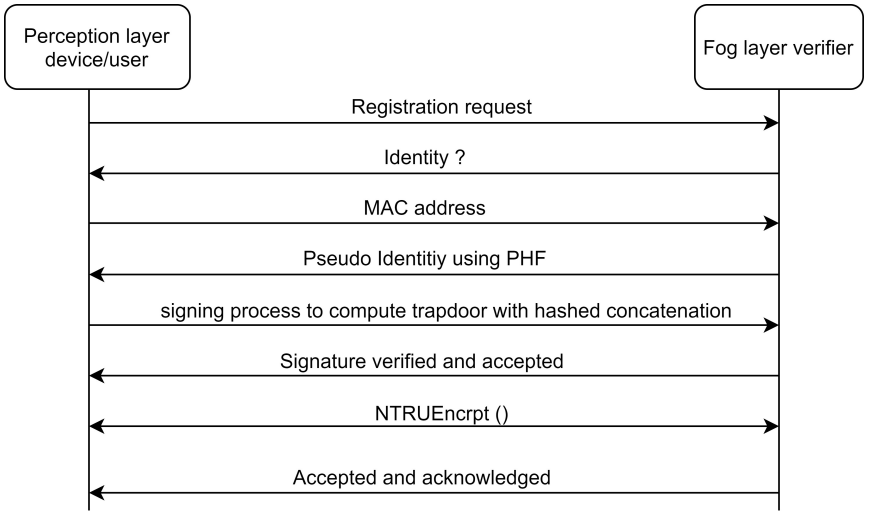

Figure 3: Interaction between evidence device and verifier

3.1.1. Pseudo identity generation

All the devices provide their corresponding hardware identity (MAC address) as an input to the hash function, and we obtain a hashed output as a pseudo-identity. The mapping can be stored on a private cloud and only pseudo-identities are published on public cloud. The investigators' identities can also be mapped following the same process. Therefore, privacy can be preserved well. We have chosen the trapdoor key mode of operation assuming that in IoT infrastructure intruders attempt to exploit the trapdoors.

The lattice-based PHF maps an input of $x \in \mathcal{X}$ to a matrix of $\mathcal{H}_K(x) = AR_x + \in BS_x \in \mathbb{Z}_q^{n \times m}$, where $\mathcal{H}_K$ is the hash function with key K; n, m and q are the positive integers, and $\in \mathbb{Z},$ is the set of integers; R_x *and* S_x matrices are computationally feasible with a trapdoor value td. A *and* B matrices are user defined generators that belong to $\mathbb{Z}^{n \times m_q}$ *and* $\mathbb{Z}^{n \times m'_q}$. To start the process of pseudo-identity, the MAC addresses are converted to the polynomials of degree d, these polynomials are then converted to polynomial ring G which is given as the input to $\mathcal{H}_K(x)$. Then, we calculate the hash as:

$$\mathcal{H}_K(x) = A + \sum_{z \in CF_x} A_z. \tag{1}$$

Here, CF_x are cover-free sets which construct lattice-based PHFs, A_z is calculated by a function with parameters of K, binary decomposition of z and index i. The process of generating hash is summarized in Algorithm 1.

The calculated complexity of Algorithm 1 is $O(N\ logN)$. N is the number of elements in the ring G.

3.1.2. Short signature and confidentiality processing

The devices at perception layer are resource constrained; therefore, the objective is to make the security process simple and effective with less computational complexity. To this end, we use the short signature process with lattice based PHFs as shown in [40].

Using the lattice-based PHF $\mathcal{H}_K(\,)$ with some positive integers $\overline{m}$, m', l, q, n, and B be the compatible trapdoor matrix as shown before, the verification key for the PHF based signature scheme uses $K_{ver} = (A, r, K_r)$ where, A is a trapdoor matrix $A \in \mathbb{Z}_q^{n \times \overline{m}}$, r is a uniformly random vector $r \in \mathbb{Z}_q^n$, and K_r is a random key. The signing key consists of a trapdoor $\mathcal{T}$ of A such that $Ae = v$, where $v \in \mathbb{Z}_q^n$, and e is the sample short vector.

For any message transmission M, the device uses the signing process to compute trapdoor with hashed concatenation as:

$$A_{\mathcal{H}} = (A||\mathcal{H}_K(M)). \tag{2}$$

It uses the trapdoor $\mathcal{T}$ to generate the sample short vector e satisfying the signing condition: $A_{\mathcal{H}}e = v$. We have used the sampling algorithm as shown in [41]. Finally, it returns $s = e$ as signature. The verifier verifies the signature

Algorithm 1 Pseudo identity generation

INPUT: polynomial ring G generated from devices' MAC addresses
OUTPUT: Pseudo Identity $\mathcal{I}$

Initialize A , R, S.
Convert MAC addresses into Polynomial group $G = I \otimes g_t \in \mathbb{Z}_q^{n \times nk}$, $k = log_2 q$ *and* $g = \left(1, 2, ..2^{k-1}\right)^t$
Create a trapdoor matrix $B = G$.
$K = (A, \{A_i\})_{i=0,1,..\mu-1}$ where, $\mu = log_2 N$
$\forall x \in \mathbb{Z}$, $x \rightarrow \mathcal{CF}_x$
$\forall z \in \mathcal{CF}_x \subseteq N$, *calculate* $A_z = f(K, z, 0)$ *from* K *and the binary decomposition of* $z = (b_0, ..b_{\mu-1})$
$f(K, z, i) = \begin{cases} A_{\mu-1} - b_{\mu-1} G, & if\ i = \mu - 1 \\ (A_i - b_i G).G^{-1}(f(K, z, i) + 1), & \\ otherwise & \end{cases}$
$\mathcal{H}_K(x) = A + \sum_{z \in CF_x} A_z$
$\mathcal{I} = \mathcal{H}_K(x)$
Return $\mathcal{I}$

as correct, and validates iff e is short with the threshold value of l and $A_{\mathcal{H}} e = v$. Once the signing is done, we use NTRUEncrypt to provide confidentiality to the evidence transmission [42]. The overall process is summarized in Algorithm 2.

Algorithm 2 Signature and confidentiality processing

INPUT: Message M, A, r, K_r , $\mathcal{H}_K$
OUTPUT: *Generation and verification of* s *and encryption*

$\left(K_{ver} = (A, r, K_r)\right)$
Select $\mathcal{T}$ of A
$A_{\mathcal{H}} = (A || \mathcal{H}_K(M))$
$A_{\mathcal{H}} e = v$
Calculate $e\ of\ \mathcal{T}$
Sign with $s = e$
Verify s with K_{ver}
If $if\ (A_{\mathcal{H}} e = v)$
if Accept signature **then**
    Call NTRUEncrypt()
else
    Discard and abort session
    Return NULL
end if

We can see from the above explanation that the devices consisting the evidences belong to perception layer, but the verifier is at the fog layer. This requires for secure transmission of messages from perception to fog layer. Moreover, it is known that the perception layer is resource constrained, so the verifier at perception layer would be a bottleneck for the proposed framework; therefore, we have placed the verifier at fog layer. The interaction between a device at perception layer and the verifier at fog layer is shown in Fig. 3. The interaction between the device and the verifier also helps the fog layer to record the basic status of the device under consideration for the forensic purpose.

3.2. Fog layer

We put resource extensive devices such as routers, switches, gateways, and local or private servers in this layer to assist in the forensic applications purpose. The signature data as mentioned in previous subsection is verified by the fog layer and stored and updated periodically by itself. Apart from the signature-encryption task, we have enabled

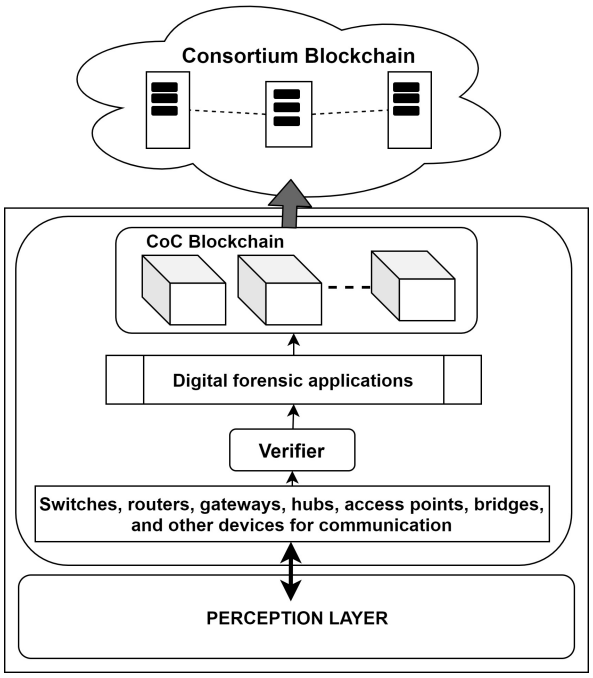

Figure 4: Proposed model for the fog layer in IoF

this layer with some digital forensic applications and chain of custody blockchain. Each time a device is handed over with users or even location, the digital forensic applications record the data of that device and create a transaction in blockchain for that device. For the digital forensic applications, we have used autopsy applications, localization tracing, and Nmap applications for the experiment. The access to the blockchain is granted on the successful verification of a signature. The fog layer structure in the presented framework is shown in Fig.4. The devices in the perception layer communicate via the devices of the fog layer. Once these devices receive messages from any device of perception layer, it verifies the signature and decrypt the message. It has been assumed that the verifier is trusted enough and non-forgeable. Once the devices are authenticated, digital forensic applications such as network and memory forensics tools are run on these devices to gather the present working features from them. The data are saved in blockchain to further access by the investigator(s) in CoC. Finally, this blockchain for CoC is extended to the consortium blockchain for transparency worldwide.

The blockchain aspect of the presented framework is shown in Fig.5. The colours in the figure represent an evidence at different time interval. The connections among the coloured boxes represent the connection of evidences for a case; thus, creating a chain of evidences. Once the issuer of the evidence (device or investigator) is verified, fog layer allows the framework to run the digital forensic applications. We also consider that multiple investigators are using this framework from different locations and including the evidences in the blockchain (transaction in form of evidence information and state); thus making it decentralized and distributed. It then outputs the digital forensic applications data i.e. services running on the device, memory status, and port status along with the pseudo-identity, and generates a block for a particular evidence. The block is then inserted in the blockchain with smart contract execution. The CoC blockchain derives an Evidence Chain (EC) in the process for a single case. Extending the EC with all the digital forensic stages finally gives the Case Chain (CC) as shown in Fig.5. We have named this combination as CoC-EC-CC. The process is initiated with the granularity of an evidence. Moreover, for the manual inclusion of the evidences needs to be stored in the secure storage (assuming the storage location is trusted). Proper synchronization is provided by this CoC-EC-CC as all the access information of an evidence is maintained in CoC which can be connected further with EC as required. For multiple evidences, the same can be connected as EC. Following Fig.6, we connect these evidences for a single case and also for multiple cases in the investigation process. Each stage in the investigation may be coordinated by multiple investigators at times and thus, it is required to connect those chains. This leads to CC. All these chain

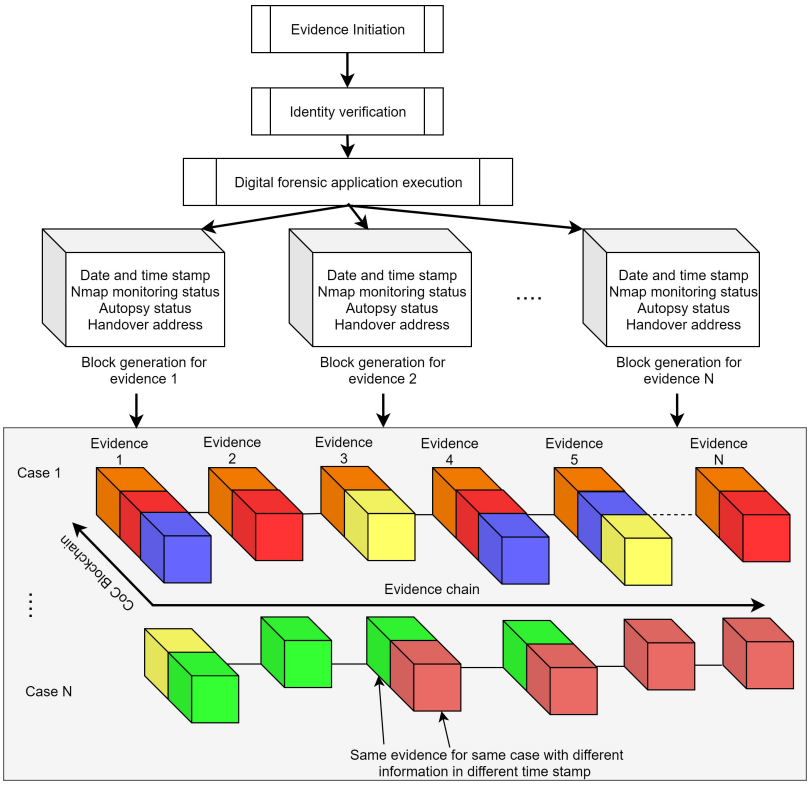

Figure 5: Blockchain perspective of IoF

information are stored in the consortium blockchain. To make the framework adaptable with the existing systems, if the local investigation departments are storing their data in local cloud, those clouds can be connected in a consortium blockchain representing as nodes of blockchain. Moreover, smart contracts are applied to execute some conditional functions in the consideration of consortium to have the transparent analysis of those functions' outputs. We have applied the smart contract in solidity for compatibility with Caliper evaluation framework and Hyperledger composer. Such a blockchain application for evidence management enhances non-repudiation, integrity, and availability of the evidence information. Note that as IoTs deal with huge number of devices, the blockchain length increases significantly; the reduction of blockchain length in the present scenario is hold for future work.

3.3. Consortium Blockchain

We assume for the legalization offices to be the part of a consortium. These consortium modules connect with each other to form a decentralized permissioned blockchain framework. The control over a consortium blockchain is granted by a group of approved individuals such as police departments, advisory committee, and CBI-FBI personnel; thus, decentralization takes place. The consensus process in this consortium blockchain differs from that of the public blockchain as the participants of this blockchain belong to a group of pre-approved nodes (users) on the network. Thus, consortium blockchain enhance the inherited blockchain security features with a higher degree of control.

We use Hyperledger to implement consortium blockchain concept. CoC-EC-CC are stored at cloud servers which are distributed. These servers are under the decentralized control of the consortium members. To participate in the consortium blockchain and access data from the CoC-EC-CC, the department (user or investigator) requires to provide signature of a transaction of CoC-EC-CC access. This distributed consortium is beneficial for tracing a cross-border online criminal activity. The consensus process of the consortium blockchain is based upon the legalization aspects with some pre-defined set of conditions. As different countries have different investigation processes, such pre-defined legalization agreement is important in IoF. Moreover, such distributed framework is considered to be helpful for referencing any case from other investigation body of any country which may speed up the process of investigation.

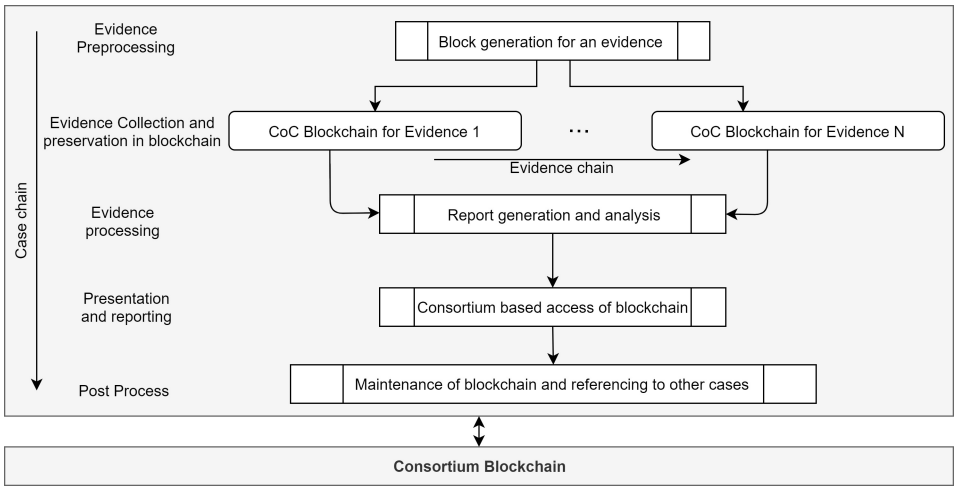

Figure 6: Connection of chains in the proposed framework

3.4. Cloud Layer

To make a distributed framework with the help of blockchain cloud is necessary for storage and also for data access, IoF maintains the cloud locally (department basis or country basis) and goes for synchronization with consortium blockchain periodically. The connection of such cloud entities in consortium blockchain increases the data availability. In an IoT environment the participating devices are concern as malicious devices or users (attackers) may try to manipulate the data. Therefore, in perception layer we have used the cryptographic approach for the process. However, in the upper layers of the presented framework it is considered to be comprised of pre-defined systems and collaborations among them to make it secure.

3.5. IoF advantages

Our proposed IoF opens up the new dimension of research in digital forensics by using the lattice-based cryptographic methods. Moreover, the research gaps identified in Section 2, are addressed in the presented solution. The IoF shown in this paper uses heterogeneous devices in IoT which is an advantage of the framework. Besides, the consideration of consortium blockchain in digital forensics is also a path breaking significance of IoF that shows the potentialities over the existing solutions. The granularity of transparency is also ensured here which is another advantage of IoF and is not been observed in literature. The assurance of privacy-anonymity for the forensic witnesses to avoid manipulation of evidences is another important advantage that IoF ensures.

4. Experiments and performance analysis

IoF is simulated by creating a network environment and with the help of Ethereum Virtual Machine (EVM) and Hyperledger fabric. The details of the experimental setup, parameters for evaluation and the obtained results are discussed in the following subsections.

4.1. Experimental setup

We have simulated the IoF prototype using Ethereum private network platform. We include smart contract to record the transmission processes of evidences and its various parameters' state as blockchain transactions. For simulation, we have installed Geth to setup a blockchain and configured the blockchain consensus and smart contract. The smart contract construction is shown in Fig.8. We have constructed smart contract interfaces for evidence generation, acquisition, and report generation using Mist Browser. The system for experiment have 64 GB DDR3 RAM and an Intel i7 processor. Transaction validations in the blockchain are done in Ethereum base only. The step-by-step experimental setup is as follows.

- Step 1: Pre-installation of Homebrew and Node/npm.

- Step 2: Installation of Ethereum, Solidity, Remix IDE, Mist Browser, and Microsoft LatticeCrypto Library for PHFs.
- Step 3: Genesis blocks are initialized with *bootnode* tool.
- Step 4: Configure the set of validators with the genesis block.
- Step 5: Blockchain is initialized with two blocks and three virtual organization accounts with wallets.
- Step 6: A folder is created to store the blockchain.
- Step 7: Private Ethereum Blockchain is initiated and run.
- Step 8: Geth console is used to connect to the private Ethereum blockchain.
- Step 9: Accounts has been created and dummy Ethers are mined.
- Step 10: Smart contract condition is created in solidity with Mist and included in Ethereum.
- Step 11: Remix IDE is initialized to deploy the generated smart contract.
- Step 12: Remix IDE is updated with wallet account of an organization and blockchain network details.
- Step 13: Smart contract is executed on Ethereum blockchain.

Moreover, we have used the Caliper's framework for the evaluation. We use Caliper's 2-organization-1-peer and 3-organization-1-peer network models with 6 clients. The experiments are done mainly with two functions of the case chain, i.e., evidence collection and evidence processing, as they have the direct impact on the blockchain states. The results are averaged on 12 rounds of tests to avoid measurement errors. In real life implementation these rounds depends on the precision and accuracy requirements of the applications. The finality of the transaction is used as per the Ethereum reference for the simplicity of the transaction. In general, some specific finality condition can also be used with smart contract explicitly. The network model used for this experiment includes four mobile phones and three laptops. These devices work as perception layer nodes and are connected with four different data servers which form a peer-to-peer network for blockchain. Internally, all these four data servers are connected with some forensic application processing units. Installation of CISCO router gateway is included as fog layer. For the data storage and blockchain operations we have used workstation with the previously mentioned blockchain settings. The abstract view of experimental configuration is shown in Fig.7.

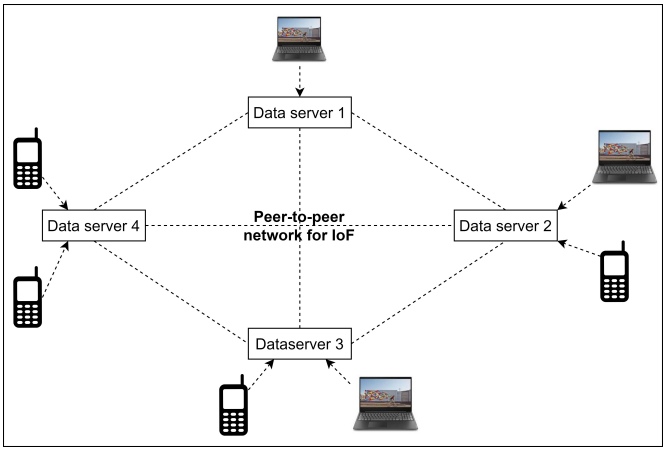

Figure 7: Abstract view of experimental configuration: internally forensic application units are connected with the data servers

```
1 pragma solidity ^0.4.22;
2 contract ChainOfCustody {
3     struct Evidence {
4           bytes32 PseudoID();
5           nmap_service();
6           nmap_port();
7           nmap_IPaddress();
8           ID_access();
9           ttime () ;
10   }
```

Figure 8: Solidity smart contract construct for the IoF framework

4.2. Performance metrics

The simulation of IoF framework has been analysed based on the performance parameters: latency, throughput, CPU utilization, memory utilization, gas, complexity and energy consumption.

- *Latency:* Latency (or transaction latency) is the time gap between initiating a transaction with "send" button, and the inclusion of the transaction in the blockchain [25]. The transaction latency is the sum of the block inclusion latency and consensus latency, and it is given as:

$$L\,(tx) = L_B\,(tx) + \; L_C\,(b)\,, \tag{3}$$

where $L_B\,(tx)$ is block inclusion latency, i.e., the time taken for a transaction tx to be included in a block b and $L_C\,(b)$ is the consensus time for agreed upon decision on block b and its inclusion in blockchain. Moreover, $L_B\,(tx)$ is calculated as:

$$L_B\,(tx) = time\,(block\,(tx)) + T - time(tx), \tag{4}$$

where $block\,(tx)$ is the block in which the transaction tx is included, T is the block period, $time(tx)$ is the time when transaction tx issued, and $time\,(block\,(tx))$ is time when the block for tx is generated. Block inclusion latency have impacts on T, gas limit G, and the number of transactions per unit time (tps).

- *Throughput*: This metric is measured as the number of blocks which are appended to the blockchain per second [42]. More accurately, the number of transactions in unit time is defined as throughput of the blockchain. It depends on the applicable consensus algorithm, which specifies how nodes communicate to ensure the validity of the appended transaction and the consistency of each of their copies on the shared ledger. It is given as:

$$Throughput\;(tps) \;=\; \frac{Total\;committed\;transactions}{Total\;time\;for\;committed\;nodes}. \tag{5}$$

- *CPU and memory utilization*: For an IoT-based system, the utilization of memory and CPU gives a glimpse of efficiency of the system. This utilization ratio is represented in percentage, i.e., how much percentage of CPU processing units and system memory are busy in processing the blockchain related to some certain parameter.

- *Gas*: Every transaction or smart contract executed on the Ethereum blockchain requires gas [44]. It is a fraction of an Ethereum token and used by the contract to pay the miners for securing that transaction on the blockchain for their efforts. We have measured the gas consumption with respect to the size of the blocks and number of transactions. In this simulation, as the evidences generated are increased from 1 to 1000, the block size is increased from 0.5 KB to 3.34 KB. At this time, gas consumption is increased from 1.0 to 4.8. We have assumed the denomination of Gwei as 1 Gwei is equivalent to 0.000000001 Ethereum. In this way, 10 Gwei per gas is used for fast transmission, we have to pay 0.00000048 Ethereum (4.8 Gas * 10 Gwei) to cover 800 pieces of evidences.

Table 1
Performance measurement with 2-organization 1-peer network model

Round	Send rate (tps)	Max. L. (s)	Min. L.(s)	Avg. L. (s)	Throughput (tps)
1	7	0.73	0.53	0.63	6
2	12	0.97	0.59	0.78	8
3	17	1.23	0.67	0.95	13
4	22	2.73	0.78	1.75	17
5	27	3.12	1.33	2.23	20
6	32	5.33	1.87	3.60	22
7	37	7.07	2.01	4.54	24
8	43	11.67	4.33	8.00	27
9	49	13.22	6.50	9.86	30
10	52	15.33	7.66	11.49	34
11	57	16.01	7.89	11.95	20
12	62	18.11	8.01	13.06	12

Table 2
Performance measurement with 3-organization 1-peer network model

Round	Send rate (tps)	Max. L. (s)	Min. L.(s)	Avg. L. (s)	Throughput (tps)
1	7	1.03	0.89	0.96	5
2	12	1.17	1.03	1.10	7
3	17	4.33	1.67	3.00	9
4	22	6.00	2.33	4.17	12
5	27	11.12	2.87	6.99	14
6	32	12.33	3.50	7.91	17
7	37	13.07	5.11	9.09	20
8	43	15.67	6.67	11.17	23
9	49	16.22	8.33	12.27	27
10	52	17.33	9.03	13.18	32
11	57	19.01	10.33	14.67	22
12	62	21.33	11.66	16.495	10

4.3. Results and discussion

We measure the above metrics for IoF and the other frameworks in the literature [21] [22] [23] [26] [27]. Note that, these measurements are more inclined for CoC-EC-CC; consortium is more emphasized for a global framework and contains CoC-EC-CC.

4.3.1. Latency comparison

We have measured the latency in both 2-organization 1-peer network model and 3-organization 1-peer network model with 12 rounds as it is shown in Table 1 and Table 2, respectively. For each round, the tps, maximum (Max. L.), minimum (Min. L.), and average latency (Avg. L.), and throughput have been observed to analyse the system behaviour. The latency is measured in seconds (s).

The measurements shown in tables 1 and 2 depict that with the increasing transaction sending rate, the average latency increases gradually with an average increasing factor of 24.3% for 2-organization 1-peer model and 25.7% for 3-organization 1-peer model. This effect in latency is caused by the number of message communication by the peers. The results also show that after 10^{th} round the system performance degrades, it denotes the failure point where the throughput drastically decreases by 32.1% in average. As, the round increases, the send rate increases, due to increasing

number of messages and evidence transactions, the system degrades its throughput. This throughput can be further optimized in future using some optimization framework. In real-life implementation the number of iterations can be experimentally decided depending upon the requirement of the system and application. We have also measured the other algorithms' average latency (average of all rounds and irrespective of 2-organization or 3-organization 1-peer network model) and plotted a comparison graph against the send rate of transaction in tps as shown in Fig.9.

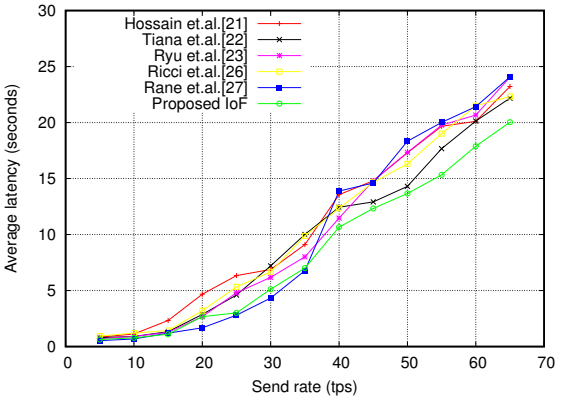

Figure 9: Comparison of average latencies

We have varied the send rate of transaction from 5 tps to 65 tps to compare the average latency of the approaches as shown in Fig.9. It has been observed that the proposed approach has average latency of 7.07 seconds irrespective of all rounds and irrespective of network model under consideration (i.e. 2-organization or 3-organization). It is significantly 34.2%, 27.7%, 30.7%, 31.8%, and 29.8% less as compared to the approaches mentioned in [21] [22] [23] [26] and [27], respectively. The use of PHFs and fog-based method in the presented framework is therefore advantageous for IoF.

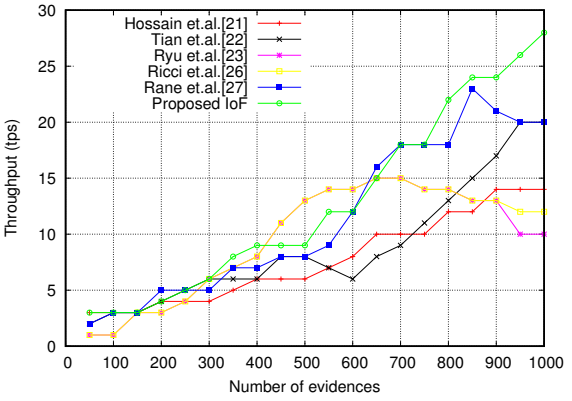

Figure 10: Comparison of throughput

4.3.2. Throughput comparison

The experiments for throughput have been executed in terms of number of evidences processed in unit time. We have measured the evidences from 100 to 1000 considering 50 perception layer device evidences including from laptops and smartphones. The other algorithms are also measured with the same experimental setup and the comparison is shown in Fig.10. We have assumed that each transaction is comprised of 10 evidence information in average. The output is shown in tps.

Fig.10 shows that almost all the approaches in the comparison start with approximately same measurement of throughput. The works in [23] and [26] show similar kind of throughput in all the evidence scenarios; however, after 900 evidences the approach shown in [23] degrades by 37.9%. Overall, with the increasing number of evidences, the

Table 3
Comparative analysis of blockchain-based approaches for digital forensics

	Number of perception layer devices	Number of concurrent transactions capacity	Average transaction throughput (tps)	Overall commit time of all the transactions (minutes)
Hossain et al. [21]	10	780	4	37.83
	20	1200	9	51.88
	30	1970	14	65.30
	40	2100	20	79.78
Tian et al. [22]	10	1100	10	30.23
	20	1650	13	45.50
	30	1900	17	50.23
	40	2300	21	62.90
Ryu et al. [23]	10	1600	14	29.40
	20	2000	21	42.54
	30	3450	23	51.89
	40	5600	29	68.23
Ricci et al. [26]	10	1430	5	35.77
	20	1790	8	43.90
	30	2000	13	56.44
	40	2600	18	63.11
Rane et al. [27]	10	1700	11	27.87
	20	2180	18	46.90
	30	4300	23	51.90
	40	6400	38	62.18
Proposed IoF	10	2500	17	23.33
	20	3200	27	34.67
	30	4000	36	43.02
	40	7100	47	51.33

comparative approaches degrade their throughput by 23.67% on average, whereas our IoF maintains the throughput with average increasing factor of 4.5%. This signifies that IoF is beneficial in terms of throughput. To enhance this result and check the capacity of the systems, we have measured the failure points in terms of concurrent transactions handling. The comparative results are shown in Table 3.

The measurements in the above Table 3 shows that IoF is able to handle a greater number of concurrent transactions with the increasing number of transnational nodes or devices, which is 36.8% more than other frameworks. The ease of computational feasibility through less complex cryptographic measures is the reason for this benefit. Another benefit is also observable in Table 3 is the overall commit time, which actually enhances the latency experimentation discussed previously. It shows that the overall commit time for all the transactions, irrespective of the number of nodes, is less as compared to other frameworks by 23.4% in average.

4.3.3. CPU and memory utilization

The overall memory consumption and CPU utilization of IoF are shown in Table 4. We have measured these metrics for all rounds, irrespective of 2-organization 1-peer network model and 3-organization 1-peer network model of Caliper framework.

Table 4 shows that with the increasing number of rounds, the memory utilization increases by 11.7% in average in both network models. 3-organization 1-peer network model consumes more memory as a greater number of evidences are handled, while, the CPU utilization is less in this network model for IoF. The results show the usage strategy of the network model; if memory is not large enough, we can use 2-organization 1-peer network model, and if CPU efficiency is less then we can use 3-organization 1-peer network model. To extend this result for the comparison with the other existing frameworks, we have used Fig.11.

Fig.11 shows that the proposed framework consumes less CPU resources as compared to others; whereas, the memory utilization is more as compared to some of the frameworks in comparison. It is due to the use of two blockchains in the framework. Though the memory utilization is high, the transparency and chain of custody is beneficial for IoF.

Table 4
Memory consumption and CPU utilization for the proposed IoF

Round	2-organization 1-peer network model		3-organization 1-peer network model	
	Memory utilization	CPU utilization	Memory utilization	CPU utilization
1	20.3%	23.2%	22.6%	15.5%
2	21.0%	23.4%	24.9%	19.7%
3	25.2%	32.5%	28.3%	21.8%
4	28.7%	35.9%	31.8%	26.9%
5	34.3%	38.7%	33.5%	30.4%
6	37.5%	40.6%	37.4%	37.8%
7	41.8%	45.8%	42.2%	41.3%
8	45.1%	50.1%	47.1%	43.6%
9	49.0%	57.5%	50.8%	49.8%
10	53.3%	63.5%	56.2%	59.5%

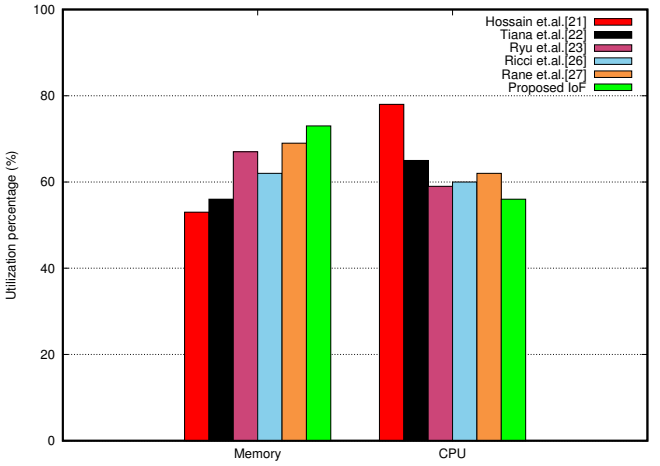

Figure 11: Comparison of memory and CPU utilization

4.3.4. Gas consumption

The block inclusion latency, which is a part of overall transaction latency and commit time, is affected by three parameters: block period parameter T, the gas limit G, and the workload. The workload is the rate of transactions issued to the system in unit of time, and it is generally expressed as tps. Suppose, we are able to precisely characterize the workload the system is subject to, and to set G such that every issued transaction is included in the block of the current proposer. In such ideal condition, the latency of the block inclusion is within the interval of 0 and T. However, if in such condition, we set $G = \infty$, then it may affect adversely to the consensus timing due to the large number of blocks. We have considered three gas limits $G1 = 21800$ (without ICO), $G2 = 100000$ ($medium$) and $G3 = 200000$, and we have conducted the experiments in 10 rounds. We have observed the timing of latency for each gas limit and found that for *G3* the latency is the most as a greater number of blocks are transacted. The latency time comparison for the our work for the three gas limits is shown in Fig.12.

We have also compared the gas consumption of other existing frameworks as shown in Fig.13. All the existing frameworks are either based on distributed ledger or on blockchain. Therefore, we have experimented in Ethereum framework. Fig.13 depicts that IoF provides lower gas consumption than other existing frameworks by 32.16% in average. Generally, gas consumption depends on the line of codes that needs to be executed for processing a smart contract.

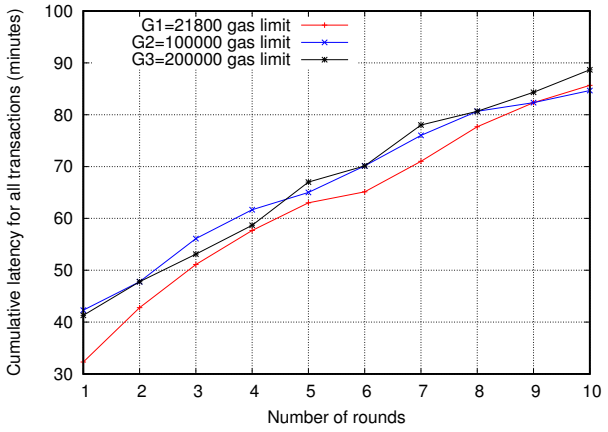

Figure 12: Cumulative latency for different gas limits

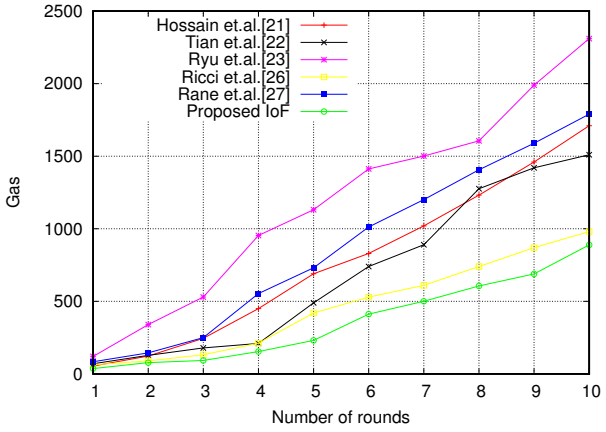

Figure 13: Comparison of gas consumption

Table 5
Cost Analysis

Computation cost					
Hossain et al. [21]	Tian et al. [22]	Ryu et al. [23]	Ricci et al. [26]	Rane et al. [27]	Proposed IoF
O(N logn)	O(N logn)	O(N logn)	O(N + logn)	O(N logn)	O(N) + O(n)
Communication cost					
Hossain et al. [21]	Tian et al. [22]	Ryu et al. [23]	Ricci et al. [26]	Rane et al. [27]	Proposed IoF
O(log N)	$O(N^2)$	O(N logn)	O(log N)	O(N) + O(log N)	O(N logN)
N is the number of nodes (devices) and n is the number of transactions					

In this respect, it is observable from the comparison that the framework is suitable for IoT-based infrastructures as they are resource-constrained.

4.3.5. Computational cost

We analyze the cost in two parts: computation cost and communication cost. Computation cost signifies the complexity of the proposed framework's computational tasks and communication cost endeavours the complexity of communication. The comparison of cost analysis is shown in Table 5. It shows that the computational complexity of IoF is less as compared to the other frameworks but, the communication cost is on the higher side as it includes more communication at the initial stage as shown from Fig.3. However, to optimize the communication cost with minimization function or protocol optimization is considered as a future extension.

4.3.6. Energy consumption

IoF is useful for IoT-based forensic processes. In such scenarios, energy of the devices may become a severe constraint to evaluate the evidences' properties. Therefore, we have evaluated the residual energy of the overall network after n number of successful evidence transactions. The formula used for this metric is:

$$E_{res}(average\ percentage) = \sum_{i=1}^{n} \frac{(E_{i_{T+\Delta}} - E_{i_T})}{E_{i_T}} \times 100. \tag{6}$$

The same formula is used for the other existing frameworks and significant improvement has been noticed for IoF. The comparative analysis is shown in Fig.14. The lightweight encryption and hash-based cryptographic operations are the main reasons for this fact. Moreover, the analysis of evidences in the fog layer makes it less exhaustive for computational aspects. Therefore, the average energy consumption in the present solution is reduced significantly. It has been observed that IoF uses 31.6%, 35.8%, 43.8%, 33.5% and 38.5% less energy consumption as compared to Hossain et al. [21], Tian et al. [22], Ryu et al. [23], Ricci et al. [26] and Rane et al. [27] respectively; overall 36.6% better in this parameter.

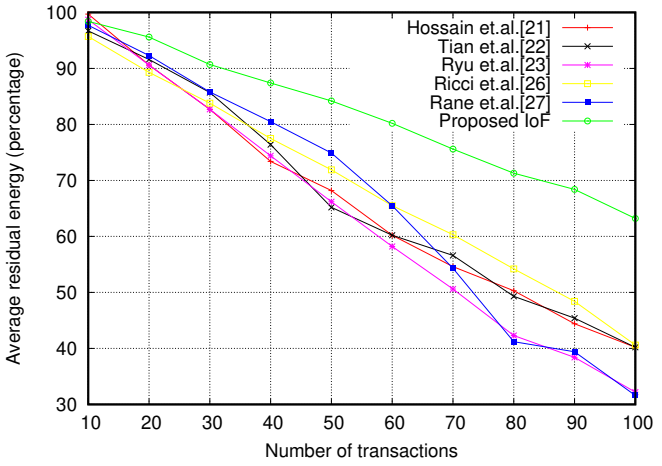

Figure 14: Comparison of average residual energy consumption

4.3.7. Security analysis

The blockchain-based applications are inherently considered to be secure for preserving confidentiality, integrity and non-repudiation. The same have been ensured in the proposed IoF by using NTRUEncrypt() and PHF. Moreover, the data is tamper-resistant as the digital forensic operations are performed in fog layer without any manual intervention. Manual intervention is only required for a collection of evidences from the crime scene if it is a physical attack such as murder, kidnapping and others. However, this point is not considered in the present work and the reliability of evidence collection process is assumed. The chain of custody is making the influence of coordination and monitoring process of the overall forensic framework. Privacy-anonymity in the forensic is required to maintain the social dignity of a suspect till the evidences and its analysis are confirmed. Besides, it also helps to protect the identity of the investigators for avoiding manipulation. The device identities use hashing for this. This privacy-anonymity is also required so that the manipulation of the evidences under influential circumstances can be avoided. Pseudo-identities are used for blockchain, whereas the original identity mapping process is stored locally. However, it is admitted the traceability of evidences in the forensic process does not confirm the privacy issues, we attempt to provide a basic level of understanding for the same; a separate privacy model can be researched further to enhance this issue.

5. Conclusion

Blockchain technology implicitly provides integrity, transparency, accounting, availability, and access control, and confidentiality. Thus, it shows potential and becomes a suitable candidate to improve digital forensics investigation in IoT domain. The futuristic increasing number of devices poses a concern of increasing number of threats and attacks in IoT. A number of research efforts have been made in past, but each of them have limitations. In this paper, we have proposed a solution for applications of digital forensics in IoT.The use of Programmable Hash Functions (PHFs) is a novel idea for providing security features in blockchain and is attempted in the presented solution. Moreover, a chain-of-custody solution along with the use of consortium blockchain for cross border forensic data has been also considered. Smart contracts are applied for gathering forensics data. Forensics applications are featured within the edge computing, specifically, the fog layer utilizing its processing capacity. The framework has been evaluated based on latency, throughput, gas consumption, energy and resource utilization, and the failure points are also identified. The comparative analysis of the results shows that the proposed IoF is efficient in IoT infrastructures. In future, we aim to address the optimization of the concurrent transaction capability of the chain, and explore some smart contract based view structure of the blockchain.

References

[1] Jeretta Horn Nord, Alex Koohang, Joanna Paliszkiewicz, The Internet of Things: Review and theoretical framework, Expert Systems with Applications, Volume 133, 2019, Pages 97-108.

[2] Ambrosin M., Conti M., Ibrahim A., Sadeghi AR., Schunter M, SCIoT: A Secure and sCalable End-to-End Management Framework for IoT Devices, In: Lopez J., Zhou J., Soriano M. (eds) Computer Security (ESORICS 2018), Lecture Notes in Computer Science, vol 11098. Springer, Cham, 2018.

[3] Digital 2019: Global Digital Overview, 2019, available at:https://datareportal.com/reports/digital-2019-global-digital-overview, accessed on 10^{th}September, 2019.

[4] Ayesha Altaf, Haider Abbas, Faiza Iqbal, AbdelouahidDerhab, Trust models of internet of smart things: A survey, open issues, and future directions, Journal of Network and Computer Applications, Volume 137, 2019, Pages 93-111.

[5] In Lee, The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model, Internet of Things, Volume 7, 2019, 100078.

[6] Paolo Bellavista, Javier Berrocal, Antonio Corradi, Sajal K. Das, Luca Foschini, Alessandro Zanni, A survey on fog computing for the Internet of Things, Pervasive and Mobile Computing, Volume 52, 2019, Pages 71-99.

[7] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, XinxinNiu, Kangfeng Zheng, Survey on blockchain for Internet of Things, Computer Communications, Volume 136, 2019, Pages 10-29.

[8] Muneeb Ul Hassan, Mubashir Husain Rehmani, Jinjun Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Generation Computer Systems, Volume 97, 2019, Pages 512-529

[9] Hany F. Atlam, Gary B. Wills, Technical aspects of blockchain and IoT, Advances in Computers, Elsevier, in press, 2018.

[10] Rekha Goyat, Gulshan Kumar, Rahul Saha, Mauro Conti, Mritunjay Rai, Reji Thomas, Mamoun Alazab, Tai-hoon Kim, Blockchain-based Data Storage with Privacy and Authentication in Internet-of-Things. IEEE Internet of Things Journal, in press, 2020.

[11] Auqib Hamid Lone, RoohieNaaz Mir,Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer,Digital Investigation,Volume 28,2019,Pages 44-55.

[12] A. Nieto, R. Roman and J. Lopez, Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices, IEEE Network, vol. 30, no. 6, 2016, Pages 34-41.

[13] A. Nieto, R. Rios and J. Lopez, Digital Witness and Privacy in IoT: Anonymous Witnessing Approach, 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, 2017, pp. 642-649.

[14] A. Nieto, R. Rios and J. Lopez, A Methodology for Privacy-Aware IoT-Forensics,2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, 2017, pp. 626-633.

[15] Y. Zhang, S. Wu, B. Jin, and J. Du, "A blockchain-based process provenance for cloud forensics," *2017 3rd IEEE Int. Conf. Comput. Commun. ICCC 2017*, vol. 2018-January, pp. 2470–2473, 2018

[16] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles, IEEE Communication Magazine, vol. 56, no. 10, pp. 50–57, 2018.

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

[18] Bharat Manral, Gaurav Somani, Kim-Kwang Raymond Choo, Mauro Conti, Manoj Singh Gaur, A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions, (ACM) Computing Surveys, vol. 52, no.6, pp. 1–38, 2019.

[19] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges,Futur. Gener. Comput. Syst., vol. 92, no. May 2018, pp. 265–275, 2019.

[20] S. Savage, Lawful Device Access without Mass Surveillance Risk: A Technical Deisgn Discussion,CCS'18,October 15-19, 2018, Toronto, ON, Canada, pp. 1761–1774.

[21] M. Hossain, Y. Karim, and R. Hasan, FIF-IoT: A forensic investigation framework for IoT using a public digital ledger, Proc. - 2018 IEEE Int. Congr. Internet Things, ICIOT 2018 - Part 2018 IEEE World Congr. Serv., pp. 33–40, 2018.

[22] Zhihong Tiana, Mohan Lia, MeikangQiub,_, YanbinSuna,_, Shen Sua, Block-DEF: A Secure Digital Evidence Framework using Blockchain, Procedia Computer Science, 2019, Pages:1–16.

[23] Jung Hyun Ryu · Pradip Kumar Sharma, JeongHoon Jo · Jong Hyuk Park, A blockchain-based decentralized efficient investigationframework for IoT digital forensicsThe Journal of Supercomputing (2019) 75: 4372.

[24] W. T. Weilbach and Y. M. Motara, Applying distributed ledger technology to digital evidence integrity, in SAIEE Africa Research Journal, vol. 110, no. 2, pp. 77-93, June 2019.

[25] Bonomi, Silvia &Casini, Marco &Ciccotelli, Claudio. (2018). B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics, arXiv:1807.10359.

[26] J. Ricci, I. Baggili and F. Breitinger, Blockchain-Based Distributed Cloud Storage Digital Forensics: Where's the Beef?,IEEE Security & Privacy, vol. 17, no. 1, pp. 34-42, Jan.-Feb. 2019.

[27] Rane S., Dixit A. (2019) BlockSLaaS: Blockchain Assisted Secure Logging-as-a-Service for Cloud Forensics. In: Nandi S., Jinwala D., Singh V., Laxmi V., Gaur M., Faruki P. (eds) Security and Privacy. ISEA-ISAP 2019. Communications in Computer and Information Science, vol 939. Springer, Singapore.

[28] Priyanka Samanta and Shweta Jain. 2018. E-Witness: Preserve and Prove Forensic Soundness of Digital Evidence. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18). ACM, New York, NY, USA, 832-834.

[29] Billard D., Bartolomei B. (2019) Digital Forensics and Privacy-by-Design: Example in a Blockchain-Based Dynamic Navigation System. In: Naldi M., Italiano G., Rannenberg K., Medina M., Bourka A. (eds) Privacy Technologies and Policy. APF 2019. Lecture Notes in Computer Science, vol 11498. Springer.

[30] Yu Xiong and Jiang Du. 2019. Electronic evidence preservation model based on blockchain. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP '19). ACM, New York, NY, USA, 1-5.

[31] Wang, M., Wu, Q., Qin, B. et al. J. Comput. Sci. Technol. (2018) 33: 568.
[32] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, EvangelosPallis, and Evangelos K. Markakis, A Survey on Internet of Things (IoT) Digital Forensics: Challenges, Approaches and Open Issues, IEEE Communications Surveys and Tutorials, 2019.
[33] Guillaume Endignoux. Design and implementation of a post-quantum hash-based cryptographic signature scheme. Master's thesis, École polytechnique fédérale de Lausanne, 2017.
[34] Yuliang Zheng, Signcryption and Its Applications in Efficient Public Key Solutions, In Proceedings of the First International Workshop on Information Security (ISW '97), Springer-Verlag, Berlin, Heidelberg, 1997, Pages 291–312.
[35] Edson OliveiraJr, Avelino F. Zorzo, Charles Varlei Neu, Towards a conceptual model for promoting digital forensics experiments, Forensic Science International: Digital Investigation, Volume 35, 2020.
[36] Asanka Sayakkara, Nhien-An Le-Khac, Mark Scanlon, A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics, Digital Investigation, Volume 29, 2019, Pages 43-54.
[37] Yee Ching Tok, Chundong Wang, Sudipta Chattopadhyay, Stitcher: Correlating digital forensic evidence on internet-of-things devices, Forensic Science International: Digital Investigation, Volume 35, 2020.
[38] Arun Ross, Sudipta Banerjee, Anurag Chowdhury, Security in smart cities: A brief review of digital forensic schemes for biometric data, Pattern Recognition Letters, Volume 138, 2020, Pages 346-354.
[39] Wasim Ahmad Bhat, Ali AlZahrani, Mohamad Ahtisham Wani, Can computer forensic tools be trusted in digital investigations?, Science Justice, 2020.
[40] Zhang J., Chen Y., Zhang Z. (2016) Programmable Hash Functions from Lattices: Short Signatures and IBEs with Small Key Sizes. In: Robshaw M., Katz J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9816. Springer, Berlin, Heidelberg.
[41] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and newcryptographic constructions. In: STOC 2008. pp. 197{206. ACM (2008).
[42] Security Innovation's NTRUEncrypt Adopted as X9 Standard for Data Protection. April 11, 2011.
[43] Hyperledger blockchain performance metrics, white paper, Hyperledger Performance and Scale Working Group, available at: https://www.hyperledger.org/resources/publications/blockchain-performance-metrics, accessed on 15^{th} October, 2019.
[44] https://support.blockchain.com/hc/en-us/articles/360027772571-What-is-gas- , accessed on 17^{th} October, 2019.