IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 30, 2019, accepted July 7, 2019, date of publication July 22, 2019, date of current version August 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2930345

An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology

MEHRAN POURVAHAB[1], (Member, IEEE), AND GHOLAMHOSSEIN EKBATANIFARD[2]
[1]Department of Computer Engineering, Rasht Branch, Islamic Azad University, Rasht, Iran
[2]Department of Computer Engineering, Lahijan Branch, Islamic Azad University, Lahijan, Iran

Corresponding author: Gholamhossein Ekbatanifard (ekbatanifard@liau.ac.ir)

This work was supported by the MehranNet ISP (Internet Service Provider), Langarud, Guilan, Iran, supervised by the Rasht Branch, Islamic Azad University, Rasht, Iran.

ABSTRACT A Potential solution for solving forensic is the use of blockchain in software-defined networking (SDN). The blockchain is a distributed peer-to-peer network that can be utilized on SDN-based Internet of Things (IoT) environments for security provisioning. Hence, to meet some challenges in digital forensics such as data integrity, evidence deletion or alteration, blockchain is used. However, some problems such as poor attack detection and slow processing existed in previous works. To address these issues, an efficient forensics architecture is proposed in SDN-IoT that establishes the Chain of Custody (CoC) in blockchain technology. The proposed SDN-based IoT architecture is initiated with flow table rules on switches for the three different traffics Voice over Internet Protocol (VoIP), File Transfer Protocol (FTP), and Hyper Text Transfer Protocol (HTTP). In this work, overloaded switches migrate the packets to nearby switches to balance the packet flow. The packets disobeying flow rules will be discarded by switches. The blockchain-based distributed controller in this forensic architecture is designed to use the Linear Homomorphic Signature (LHS) algorithm for validating users. Each controller is fed with a classifier that uses the Neuro Multi-fuzzy to classify malicious packets based on packet features. The logs of events are used and stored on the blockchain in the proposed SDN-IoT architecture. We evaluated the performance of our forensic architecture and compared it to the existing model using various performance measures. Our evaluation results demonstrate performance improvement by reducing delay, response time and processing time, increasing throughput, accuracy, and security parameters.

INDEX TERMS Software-defined networking, the Internet of Things, forensics, security, blockchain.

I. INTRODUCTION

The increased demand for different data traffics has become complex to manage with the conventional network infrastructure. For management, a distributed Software Defined Networking (SDN) architecture is introduced to assist recent emerging technologies with the mitigation hardness. SDN is composed of a data layer, control layer and application layer that supports IoT applications [1]–[3]. SDN assists smart applications in Machine-to-Machine communication, vehicular communication, smart grid (vehicle-to-grid, home and industrial energy management, Microgrid energy management) and others [4]. In SDN, security is incorporated as authorization/authentication in the control plane and mitigation of data modification/leakage in the data plane. Blockchain is being the solution for a decentralized security provisioning system that is incorporated on a smart grid application for security and privacy protection [5]. Security is a significant issue handled by SDN based IoT architectures. Although security is a major problem in fundamental design, it is suggested with solutions in the blockchain [6], [7].

The blockchain is structured in accordance with the number of transactions. Peers connected in blockchain are enabled to discard any invalid transactions that enter into the network. IoT using blockchain is assured for security provisioning.

Blockchain technology is applicable for data sharing using the Paillier cryptosystem. Hash keys in blockchain are generated for security and stored in the form of the Merkle tree [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenyu Zhou.

SDN based IoT using blockchain technology achieves security and scalability. Transactions in blockchain are performed to prove security with minimized overhead [9]. Merkle Patricia tree is assisted for matching the root hash values. The correct path is validated before performing transactions. Security in blockchain also has some challenges such as data privacy, delegating trust, access control, authenticating device and trust model [10]. Security with blockchain is the best whereas using a third party for the purpose of authentication. The issue of security is absolutely resolved in IoT devices by using this technology. The IoT devices participating in the environment can be registered into blockchain for the need for security [11]. This blockchain technology is efficiently used for exchanging resources. The security is also achieved by providing privacy policies based on blockchain in the IoT environment [12]. These policies can be defined according to the user's preferences.

BeeKeeper is a protocol proposed on blockchain based IoT service system [13]. The recorded data on the blockchain can neither be deleted nor modified. Homomorphic computations are performed for securing the data with encryption. The blockchain is also tested on sensitive healthcare remote patient monitoring system [14]. Blockchain technology in SDN enabled IoT is applied on Microgrid applications [15] that ensures to have the properties coping with cyber-attacks.

Cryptographic techniques are studied for providing confidentiality using blockchain [16]. This blockchain is flexible to design trust models and the establishment of protocols. Blockchain works effectively with multiple parties' involvement [17]. The ability to create security between two parties is assured to be a trusted ecosystem.

Authentication is also attained using virtual identity, nonce value and a signature that are defined as Blockchain-based ID as a Service (BIDaaS) [18]. In BIDaaS, the blockchain is responsible for storing virtual ID, public key and signature of the user. Peer to peer networking is built on blockchain which does not require any centralized entity to be trusted. All the nodes connected with each other are supposed to be trusted due to the management of blocks in the blockchain.

Data transmission is also assisted by using blockchain which detects the node failure and establishes transmission using the constructed tree [19]. A response threshold is pre-determined for identifying the failed node which is presented in the blockchain network. Failure is predicted for enriching network performance. Cyber-physical infrastructure model requires blockchain for provisioning security [20].

The significant features supported in blockchain are decentralized, asymmetric encryption, distributed and storage efficiencies. Public sector services have also benefited from the utilization of blockchain [21]. User's unique identities are required to meet authentication. In recent studies, it is defined that IoT devices are manageable on the blockchain platform [22]. Hence the public key and signature of an individual device play a vital role in solving security problems. The need for security in SDN based IoT is increased; hence, to meet the security requirements, blockchain is an effective solution that supports large scale infrastructure.

Blockchain technology is defined for the purpose of managing data. In simple words, it is a digital idea for data storage. Based on the selection of transactions, new blocks are created by the miners. In our proposed work, miners are the IoT device holders. Only the registered users can access the block of transactions that are aggregated in the blockchain. A signature is essential for the purpose of identifying the blocks. The signature is unique and considered to be proof of work.

A. MOTIVATION

Security is becoming one of the essential constraints in any type of applications due to the increase in the utilization of hand-held remote devices as IoT devices. The major challenge in these devices is providing security for the data, since these devices are easier to steal and hack. Few poor investigations of security have introduced forensics as a solution to detect serious causes in the environment. In order to predict the criminal activities and prove proper examinations, the proof is mandatory. Collecting evidence play a key role in forensics for identifying and grab crime. Hence our major focus is forensics is modeled with authentication of IoT devices under blockchain technology to detect/predict the participation of malicious packets and collect useful evidence. A previous work of SDN-Fog architecture was developed to address the security issue using blockchain technology [23]. In this work, packets are analyzed to detect malicious activity, which is specified by the administrator, i.e., controller. Our proposed architecture is equipped with blockchain technology to provide security based on the transactions of users. The proposed forensics architecture is designed with the use of IoT devices, data plane and control plane. Each plane is responsible for validating users. Then the request enters blockchain which is presented in controllers. Our motivation in forensics with blockchain technology has introduced algorithms in IoT devices authentication, identifying malicious packet and maintaining CoC into the modeled system.

B. OUR CONTRIBUTIONS

- Forensic is a criminal investigation for capturing criminal activities. A novel forensic architecture is incorporated in Software Defined Network integrated with IoT environment, where security is achieved by applying blockchain technology. Security is ensured from the proposed forensic architecture that ensures security from the beginning of the packet entry. This forensic architecture overwhelms any type of attacker.
- Blockchain technology is built on the control layer in SDN for authenticating all IoT devices to ensure secure access. IoT devices are supportable for different traffic, so this work takes account of three different traffics.
- The blockchain is built with LHS algorithm for authenticating devices that uses unique identity and a point for recognizing the user.

- Neuro Multi-Fuzzy model is presented for classification which takes account of six significant packet features. The features include source IP address, destination IP address, flow duration, packet size, sequence number and service type. Finally, the evidence is collected into the SDN-controllers and then in the blockchain to maintain CoC that can be further used by the forensic team.
- The most significant achievements of the proposed work are minimized delay, response time, processing time and increased throughput, accuracy with the efficiency of security using the blockchain technology.

C. ORGANIZATION

The rest of this paper is organized into the following sections: Section II is composed of previous research works handled based on blockchain technology. Section III summarizes the problems defined in existing works. Section IV elaborates the proposed environment in SDN based IoT using blockchain technology. Section V illustrates the significant achievements of the proposed work along with a comparative study and finally, section VI concludes this paper with future directions.

II. LITERATURE REVIEW

In this section, the blockchain security on SDN and SDN based IoT environment are discussed. Blockchain-IoT was involved in different applications for distributed storage as healthcare systems, vehicular-fifth generation (5G) and smart city [24], [25]. Each application using blockchain concentrated on the providence of security with attribute access schemes, trust values and cryptography techniques.

A hybrid blockchain was presented for preventing attackers by using the computation of credibility score [26]. This credibility was mathematically formulated based on the number of parties that are entered into a contract. Proof-of-stake was used instead of the Proof-of-work method. More than 51% of the devices have a high fake credibility score which identified as attackers. The credibility score was involved in order to identify fake contract but it was challenging to predict the illegitimate user. For resolving such security challenges on SDN, blockchain was used [27]. The blockchain also details on the two types of ledgers such as (1) Centralized ledger and (2) Distributed ledger.

Privacy and availability based on blockchain security were designed in SDN infrastructure [28]. In this work, a private blockchain network was constructed by building 5 hosts. Each host was comprised of a pair the public and private keys for encrypting the file and then delivered it as a signed transaction. The cryptography algorithm used in this paper was the Secure Hash Algorithm (SHA)-256 algorithm which has high time complexity. SHA-256 was commonly used in many of the work, from which few works are discussed here. A blockchain-based approach for providing data accountability was proposed by the SHA-256 algorithm [29]. In this approach, a Data subject, Data controller and Data Processor are the three entities that are majorly involved in the design. However, security was attained, it failed to process faster that tends to intolerability of the huge number of users. Blockchain in 5G-VANET was presented for avoiding unauthorized vehicle's access [30]. SHA-256 algorithm creates hashes for secure access. The credibility of the vehicle was predicted from the trust score that depends on the road section and the distance between vehicles. A pre-defined trust score threshold was set based on which access is granted. Here the vehicles are fast moving, hence a better lightweight algorithm is required.

In [31], lightweight digital evidence preservation architecture was proposed in blockchain technology. The evidence chain was constructed using the Elliptic Curve Digital Signature Algorithm. The evidence from the server or blockchain was monitored. Lightweight blockchain was developed for assisting the IoT environment [32]. This work was enabled to minimize overhead on blockchain and so the providence of security was poor. In accordance with the major issues in previous research works on using blockchain is resolved in our proposed architecture.

Security in blockchain-IoT was also presented with access control policies and signature schemes based on which the user is either allowed to access or denied. Access control in the Internet of Things was performed using Blockchain technology [33]. This work involved two different policies as general and special for owner and user respectively. A transaction consists of an identifier which was a random number and input that specifies the type of transaction to be held. The owner including an identifier, public key, resource address, URL link, and digital signature. Digital Signature was used for authenticating the owner and lastly, an acknowledgment was sent from a smart contract. This process undergoes multiple mathematical computations that make the system lengthier and time-consuming.

A distributed secure SDN architecture for IoT using blockchain technology was presented in [34]. This facilitates to update flow rules and adapt automatic security against threats. Also, a distributed peer-to-peer network was designed for blockchain to verify node based on the generated flow table rules. This architecture was operated in the absence of a centralized controller. Each requesting node was verified based on the hash values, and then the flow rules table was updated to the recent version. Topological information and status information plays a major role in identifying attackers. This work was modeled to detect the attackers and then the flow tables will be updated; hence the malicious packets are allowed into the network. This causes degradation of the system and even within a short period of participation of malicious packets can corrupt the system.

In order to solve the malicious packets issues, a Chainguard for the providence of security in the blockchain [35] was proposed. The filtering of network traffic was majorly performed in this Chainguard which was designed for SDN. This process was defined to effectively mitigate two attacks such as Denial of Service (DoS) and Distributed Denial of Service (DDoS). A periodical replenishing was performed using a token bucket which initializes the number of tokens.

The Packets are processed only when the gray list becomes empty, therefore it has more waiting time. A distributed peer-to-peer applications and a secure validation method, pricing strategy were proposed in [36]. The pricing strategy was involved to prevent selfish users and mitigates other attackers. This process majorly includes the generation of a pair of a public key, private key, hash function, and a signature. In this process, the cryptographic algorithm remains as a limitation. However, security provisions using blockchain a stronger cryptography technique was also required.

A blockchain based Data Preservation System (DPS) was proposed for securing sensitive medical data [37]. In DPS, initially, the raw data was uploaded by the user directly into the system, which was preserved by converting it into transactions for blockchain processing. This work was applicable for both text and multimedia files. SHA-256 algorithm was involved for computing hash values followed by the use of Elliptic Curve Cryptography (ECC) for generating asymmetric keys. Also, the Advanced Encryption Standard (AES) algorithm was also involved to encrypt data. The use of three different security algorithms makes the system more complex. An Anti-Quantum transaction authentication scheme was proposed over blockchain [38]. This authentication was defined based on multiple spaces for achieving complete security. The transactions were verified and either it was accepted or rejected. The requirement of security using cryptography is satisfied but using multiple complex mathematical computations is tedious to assists a massive number of requests.

Privacy using blockchain was applied to the health care environment. Blockchain-based security mechanisms have presented a key management scheme [39]. This scheme uses the AES algorithm, which gave a chance for adversaries to decrypt the data. In [40], an attribute-based signature scheme consisting of multiple authorities. Electronic Health Records (EHRs) system was involved to use blockchain using cryptography. This work presents setup, authority setup, key generation, signing, and verification. The major parties participating in this EHR system are servers, data verifiers, authorities, and patients. The involvement of multiple authorities leads to tedious system design. ModelChain was proposed by using blockchain for privacy [41]. This work integrates machine learning with the blockchain network. This ModelChain has additionally included process of Initialize, Update, Evaluate and Transfer on each block. EHR systems have combined the Attribute-Based Encryption (ABE) and Identity Based Encryption (IBE) with signature algorithm [42]. Signature-based verification was performed for verifying the encrypted data and provide access permission. The security operation is usually required to be maintained with the limited number of external parties, here more than one entity is present where the security can be leaked easily. An attribute-based access control scheme in IoT was designed with blockchain technology to manage the records in a decentralized manner [24]. The lightweight computations have addressed single point failure and data tampering. Individuals were pre-defined with a set of attributes which were based on their identities. The attributes that are taken into account are matched to access, if not the access was denied. The involved set of attributes is required to be stronger security concerns.

III. PROBLEM STATEMENT

In this section, the major problems handled on blockchain technology are discussed. SDN architecture was designed for efficient mitigation of Distributed Denial-of-Service (DDoS) attack [43]. IP addresses were considered as a significant constraint in this work, here the whitelisted or blacklisted IP addresses were sent to the blockchain via smart contracts. The smart contract is responsible for verifies whether the received request was received from owner IP, if not then the request will be ignored. Attackers are identified only using the IP address, it is impossible to identify the attack if any registered user performs packet flooding i.e. DDoS attack. IoT based blockchain involves the participation of multiple entities into the environment [44]. Keys for IoT devices are generated by smart contracts, only for registered devices. The major issue was the required device for performing the registration which changes in every location.

A distributed cloud-based SDN architecture was comprised of the device layer, fog layer and cloud layer [23] i.e. SDN-Fog. The fog layer consists of a blockchain based SDN controller distributed network. An SDN controller includes packets parser, flow topology graph builder and several components. Packet parser identifies the packet features and then the parsed data set was constructed and then verified. The verifier operates for generating path conditions and generating reactive rules.

Then, in the migration agent, the missing packets were migrated to data plan cache, followed by updating the new rules. Flooding attack was identified in the controller only after migrating packets to data plane cache. Zero-knowledge proof function for preventing the attack to account details was presented [45]. This majorly dealt with a smart grid, hence it consists of consumer and prosumer who generate electricity and other types of prosumer were sellers. A public key was generated by the client and stored it along with ID and the password which was fed into the server. In this work, the original data was stored on the server and blockchain stores only the public key. As a result, when the client requests, the blockchain verifies and approves with authentication. User Identity and password are very simple and easy entities that can be extracted by attackers.

In [46], the authors have concentrated on verifying and trusting IoT services by proposing a Trust list. The trust list maintains a service profile and device profile for the devices. A 2-step trust development was performed which validates the service profile and then the controller was provided with device profile for validation. Here the validator requires verifying each device and the packets are dropped while the servers are unknown to controllers. A verifiable identity for reliable authentication process was proposed i.e. VeidBlock [47]. The concept of blockchain ledger was used

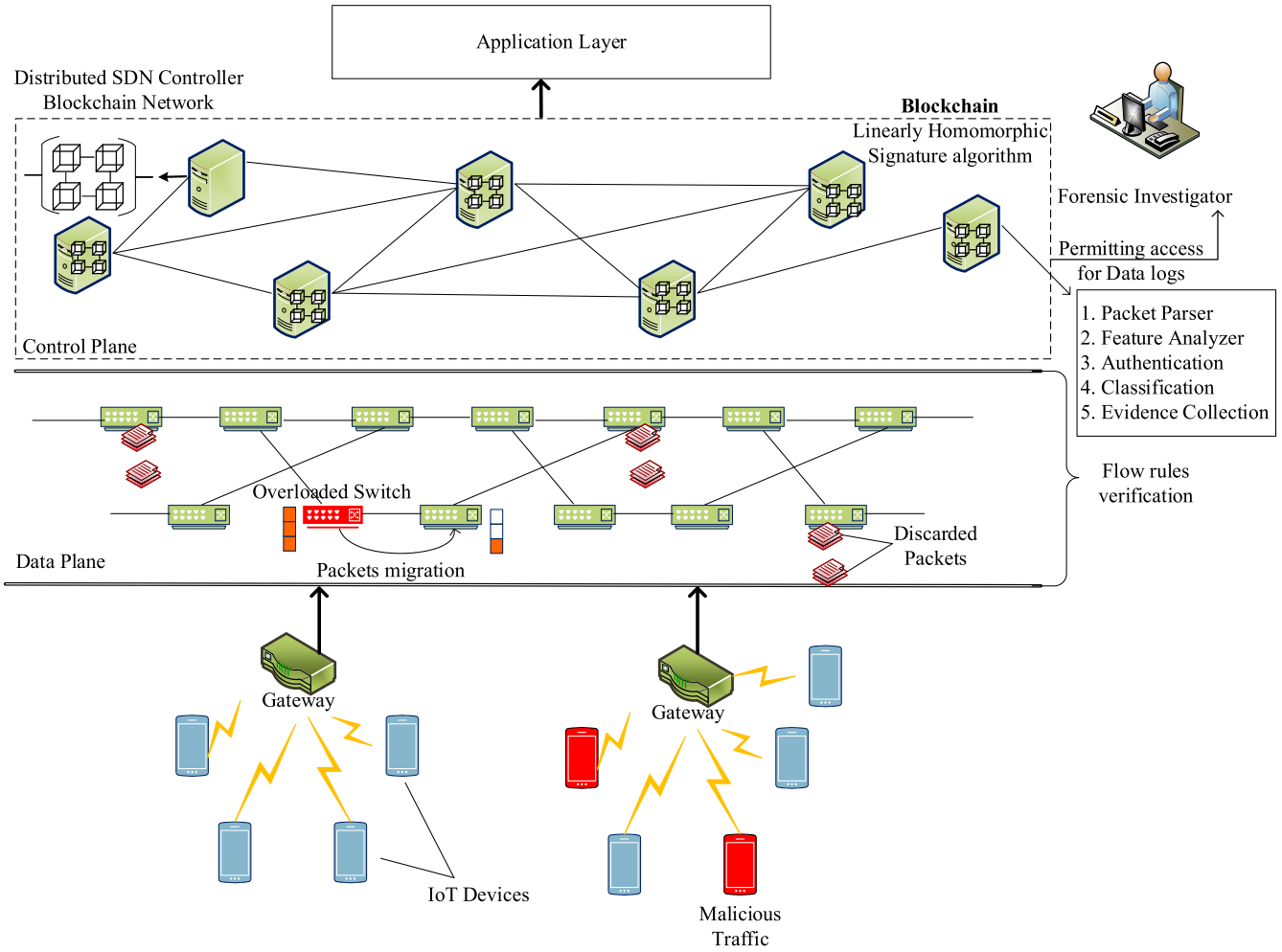


FIGURE 1. The proposed forensic SDN-IoT architecture.

to protect against tampering. Controllers are registered to Identity Provider and Validator which play a major role in this proposed system. During verification, the identity was predicted and verified to reject impersonation attacks and authenticate the requester. Identity was only used for authentication; even some attackers participate with legitimate identities. Therefore, the major problems stated on the blockchain are security using a few inappropriate entities, which are overwhelmed in this proposed Forensic architecture on SDN based IoT environment.

IV. FORENSIC ARCHITECTURE IN SDN-IOT

In this section, proposed forensic architecture in SDN-IoT is elaborated in data plane and control plane with details and necessary algorithms.

A. SYSTEM MODEL

The proposed forensic architecture in SDN-IoT environment is involved to solve the aforementioned problems. Blockchain technology is presented on the control plane for assuring security. The overall architecture guarantees the achievement of a forensic environment by analyzing the devices at each transmission.

The developed forensic architecture is comprised of n number of IoT devices that are represented as $i_1, i_2, i_3, \ldots\ldots, i_n$, these IoT devices are connected to a gateway denoted as Gw. The data packets $dp_1, dp_2, dp_3, \ldots,$ are forwarded to data plane that is comprised of switches and then the packets reach control plane. The controllers and switches in control plane and data plane are $C_1, C_2, C_3, \ldots,$ and $S_1, S_2, S_3, \ldots,$ respectively. The proposed forensic architecture in SDN based IoT is depicted in Fig. 1. The data packets from IoT devices are received at gateway node and further, it is forwarded to switches. In this work, three different traffics are taken into accounts such as VoIP, FTP, and HTTP. Switches are responsible to ignore packets if they do not obey the flow rules. The initial verification at switches assists to attain a perfect forensic architecture by ignoring unnecessary illegitimate traffic into the network. In according with the flow rules, the data packets are permitted into the control plane. The control plane presents blockchain technology that is distributed in peer to peer network structure. The packets received at control

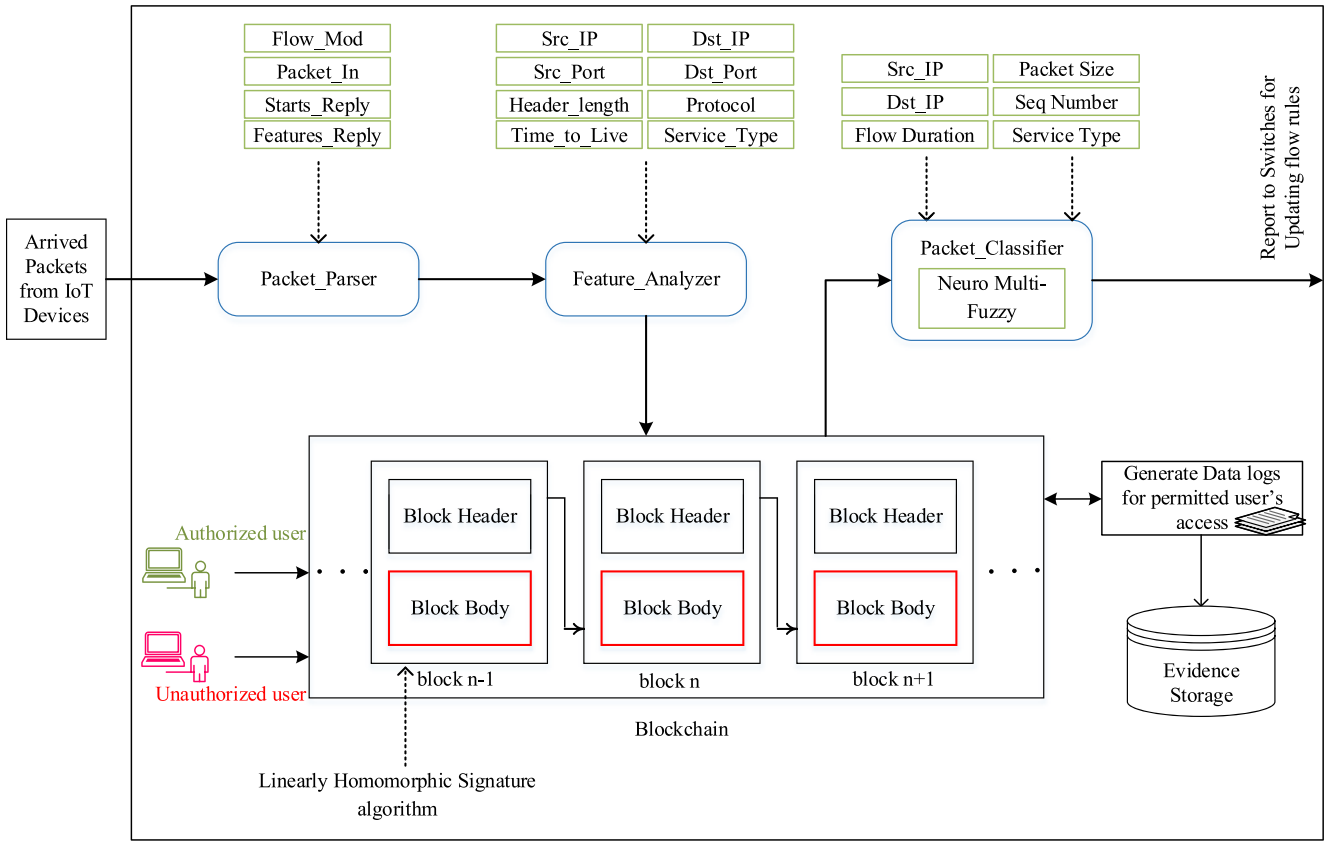


FIGURE 2. SDN-controller for SDN-IoT architecture.

plane perform the LHS algorithm which authenticates the IoT device using the unique identity and Elliptic curve point. If the device is not authenticated, then the packet is discarded.

Further, the data packets are classified using Neuro Multi-fuzzy that is required to the device with a faked identity. The one aim of forensic architecture design is to achieve SDN-IoT by validating the packets and the corresponding device individuality in each plane to ensure permission for legitimate users.

Here SDN architecture involves the processing of two separate layers as data plane and control plane, whereas it is enabled to support IoT devices that are connected via gateway towards the switches.

The establishment of CoC ensures that the collected evidence i.e. packet does not alter until it is verified by the blockchain. Major requirements of CoC are integrity, authentication and verification.

Fig. 2, depicts the proposed design of the SDN controller that includes Packet_In, Packet_Parser, Feature_Analyzer, Packet_Classifier, LHS algorithm using a unique identity and the elliptic point through the blockchain and also the controller is responsible in collecting data logs. Also, the controllers in control plane store the evidence locally into the blockchain. The conventional blockchain is used for the purpose of ensuring a forensic environment. Blockchain technology executes the LHS algorithm. A well composed SDN controller is enabled to manage the arrived number of packets from switches. In accordance with the number of IoT devices, the number of incoming packets is increased.

B. VERIFICATION ON SWITCHES

The data packets from IoT devices are not always secure into the network. Switches present on data plane are fed with certain flow rules that are generated based on the type of traffic, protocol, and port numbers. In this proposed forensic architecture, the devices are allowed with three different traffics such as VoIP, FTP and HTTP.

Flow table rules in this forensic architecture are depicted in Table 1. These rules are majorly defined from the port numbers for each traffic. The data packet that does not match this rule is discarded by the switches in the data plane. The data plane with switches migrates the data packet if the flow entries exceed the limit. Migration of packets between switches also resolves the occurrence of flow table overloading attack in the data plane. Every switch built in the data plane is supposed to have a specified number of flow entries. In many cases, the data packets are discarded without verification, due to the issue of overloading in switches.

To solve this problem the packets from the overloaded switch are migrated to a nearby switch whose flow entries are available. Data plane in the proposed forensic architecture

TABLE 1. Flow table rules.

Traffic	Protocol	Port number	Action
VoIP	UDP	5060, 5061, 5062, 5063, 5064 & 5065	Allow
		Other port number excluding above	Deny
FTP	TCP, UDP	20 & 21	Allow
		Other port number excluding above	Deny
HTTP	TCP	80 & 443	Allow
		Other port number excluding above	Deny

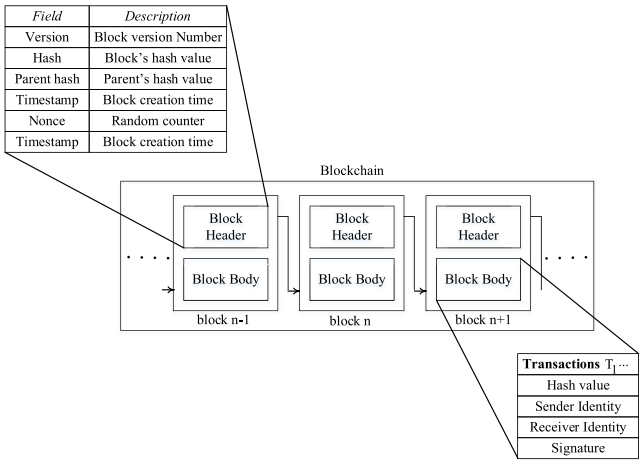


FIGURE 3. Blockchain structure.

verifies the packets from devices and also it migrates the data packets in case of overload.

The entire process followed on switches is demonstrated in pseudo code 1 which begins with the initialization of IoT devices. Traffic T_v, T_f and T_h represent the VoIP, FTP and HTTP respectively in forensic architecture. The action for each traffic is taken based on the port numbers *PNs* and validated. Further, the switch S_h exceeding maximum flow entries e_{max} will migrate the packets to another switch whose flow entries are available.

The three traffics and the corresponding port numbers are verified by individual switch before processing. The invalid traffic with the mismatched port number will be discarded by the switch. The three different traffics are validated by port numbers since illegitimate users enter the network via invalid port number. Based on this procedure, the data packets from IoT devices will reach controllers via switches and gateway.

C. DISTRIBUTED SDN CONTROL PLANE

The control plane in forensic architecture is accountable for authenticating device using the LHS algorithm and then the validated devices are classified using packet features in Neuro Multi-Fuzzy. The controllers in this forensic SDN-IoT collect the data logs and provide access to a forensic investigator. Each user log includes address, time and packet features that created provenance and records the events.

The LHS algorithm is handled on blockchain that validates the signature which is generated by using device identity and elliptic curve point. Elliptic curve point is included for enhancing security. Usually, many works have discussed signature generated using a unique identity which can be easily predicted by attackers. To overwhelm this limitation, the elliptic curve point is included for each device during authentication in the blockchain.

Blockchain technology is an efficient idea presented to achieve security. The blockchain is comprised of the number of blocks with header and body. The blockchain structure is illustrated in Fig. 3. T is the transactions that are held on each block in the blockchain that guarantee to provide security. Here identity-based signature algorithm is used for authenticating the device with respect to the identity. The controller in this forensic architecture consists of packet parser, feature analyzer and classifier. Then the evidence is collected and maintained as data logs are preserved with integrity in controllers. CoC ensures the originally acquired evidence which is not altered priorly in the blockchain.

1) PACKET PARSER

This entity in the controller is responsible for predicting the irregular behavior of devices in the network. The packets from devices are dynamically monitored by packet parser.

The OpenFlow messages are involved in SDN, which exchanges messages between switch-to-controller and controller-to-switch. The message field includes Flow_Mod, Packet_In, Stats_Reply and other necessary packet features. In this place, the packets are transmitted into the next entity of the feature analyzer.

2) FEATURE ANALYZER

The feature analyzer is responsible for extracting the packet features from each arrived packet. The significant features present in a packet are extracted. The packet features include source_port_number, source_IP, destination_port_number, destination_IP, header_length, protocol, time_to_live, service_type and more. This entity is required for extracting the packet features for classification.

3) AUTHENTICATION

Authentication is performed using LHS algorithm in which a unique identity and the elliptic point is considered to authenticate individual IoT device. The signature present in each block is verified with the corresponding IoT user. The packet parser and feature analyzer extract the packet features and then the IoT is authenticated using the proposed algorithm.

4) PACKET CLASSIFICATION

The proposed Neuro Multi-Fuzzy is used for classifying the packets based on their packet features. A device may produce

fake identity to cheat the network, but the packet features are too complex to be changed and so classification is performed by using packet features.

5) EVIDENCE COLLECTIONS

The controllers designed in this architecture are enabled to collect evidence which is utilized for diagnosing forensics. In this proposed design, the controllers classify the packets and later they are gathered and stored as data logs. The data logs stored in SDN controllers are facilitated to be accessed by a forensic investigator who is responsible for detecting forensics. The controllers also store hash of the evidence for ensuring secure access in blockchain. Hereby, the data logs collected in accordance with user's transactions require updating which will be periodically updated into new logs in controllers.

The data packets entering into the controller are verified by signature in the blockchain and then it is classified. Before computing the signature, each device is required to choose a unique elliptic curve point P. For determining a point P, consider the following curve equation,

$$y^2 = x^3 + ax + b \tag{1}$$

The terms x and y are the standard variables and a, b are the constant coefficient respectively. Let (x_M, y_M) and (x_L, y_L) be two non-symmetric points from the elliptic curve. From the two points determined point P as follows,

$$P = \frac{y_M - y_L}{x_M - x_L} \tag{2}$$

This point P is taken into account for estimating the signature for authentication. This LHS algorithm uses unique identity and the elliptic point is secured and assured to be against forgery of data [48]. This LHS algorithm is supported with bilinear pairings. Consider G_1 and G_2 as two bilinear groups which are $|G_1| = |G_2| = p$, where p is the prime number. Further, define hash function H_1 and H_2 respectively. Let the secret key be sk and public key be pk. Then using the device identity and P the signature is generated.

Select a random number R from Z_q^* i.e. random number having prime order of q, and define a value w from G^R, where G is the generator. Let the generated signature be expressed as,

$$St = (H_1(ID), H_2(P), w) \tag{3}$$

The generated Signature St being verified by the blockchain and it permits authenticated users for transactions after classification. In general, the blockchain technology uses the conventional signature algorithm which is not supportable in forensic design, so LHS algorithm using unique identity and the elliptic point is proposed. The elliptic point is unique and hence the forgery of user is impossible in this proposed Forensic SDN-IoT.

Neuro Multi-Fuzzy model in forensic architecture is present for classifying the legitimate user that has involved in the network. Once the device is authenticated from the blockchain, they are analyzed on the neuro multi-fuzzy model. This model works as a combination of neural network and fuzzy logic systems. Parallel processing of fuzzy logic tends to mitigate the processing time of classification. Fuzzy take into account of six significant packet features for classification.

Pseudo Code 1 Process Followed in Switches

Let traffic be T_v, T_f *and* T_h

begin // *start the process*
initialize $i_1, i_2, i_3, \ldots\ldots, i_n$ // *total IoT devices*
$i_1, i_2, i_3, \ldots\ldots, i_n \rightarrow$ packet forwarding
if ($i_1 \rightarrow T_v$ or T_f or T_h) // *identifying traffic*
{
S_h check PN valid // *verify port numbers from the flow table*
forward packet
else
discard packet
}
end if // *end of traffic validation*
repeat step 4 upto i_n
S_h monitor f_e
if ($f_e > e_{max}$)
{
migrate packets // *packets are shifted to nearby switch*
else
continue processing
}
end if
end // *finish the process*

Multi-fuzzy is designed with the participation of more than one fuzzy in which each has three inputs. A set of three features in deployed in one fuzzy and the other set in another fuzzy as shown in Fig. 4. The output from two fuzzy is given as input into a decision making fuzzy for authenticating packets. However authentication is performed, the packets are verified with their features to achieve a better design of forensic architecture in SDN enabled IoT environment.

Fuzzy rules on each fuzzy block are illustrated in Table 2, based on that the decision on each packet is made. The major features that are considered in multi-fuzzy design are source IP address, destination IP address, flow duration, packet size, sequence number and service type.

- *Source IP address* – This source IP address plays a significant role among all the other features. This address represents the particular device and fake IP address could be identified.
- *Destination IP address* – This packet feature denotes the destination to which the requested packet needs to be reached.
- *Flow duration* – flow duration represents the time consumed by the packet to reach the control plane. If the flow duration is very high or very low, it is suspected to be suspicious.

TABLE 2. Multi-fuzzy rules.

FUZZY LOGIC 1 (FL_1)			
Source IP	***Destination IP***	***Flow Duration***	***Output 1***
High	High	High	High
High	High	Low	Low
High	Low	High	Low
High	Low	Low	Low
Low	High	High	Low
Low	High	Low	Low
Low	Low	High	Very Low
Low	Low	Low	Very Low
FUZZY LOGIC 2 (FL_2)			
Packet Size	***Sequence Number***	***Service type***	***Output 2***
High	High	High	High
High	High	Low	Low
High	Low	High	Low
High	Low	Low	Low
Low	High	High	Low
Low	High	Low	Low
Low	Low	High	Very Low
Low	Low	Low	Very Low
DECISION MAKING FUZZY LOGIC			
Output 1	***Output 2***	***Decision output***	
High	High	High	
High	Low	Medium	
High	Very Low	Low	
Low	High	Medium	
Low	Low	Very Low	
Low	Very Low	Low	
Very Low	High	Low	
Very Low	Low	Very Low	
Very Low	Very Low	Very Low	

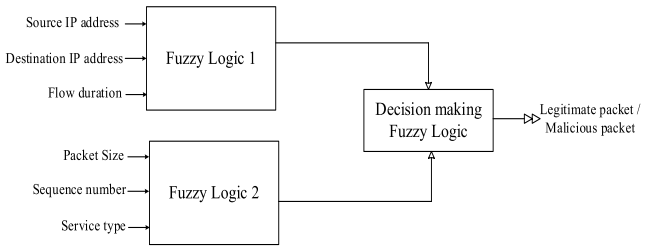


FIGURE 4. Multi-Fuzzy model.

- *Packet size* – In this forensic architecture, three different traffics are taken into account. Each traffic type has a peculiar maximum size, exceeding the size for the corresponding traffic, which is suspected.
- *Sequence number* – This feature denotes the sequence number of the packet from the corresponding device Identity (ID).
- *Service type* – Service type is one of the significant packet features that represents the required network service for the particular device.

Fuzzy logic considers the input as high, low and very low based on which the output is given in terms of high, medium, low and very low. Table 3 represents the probability values of output that are used for decision making. According to the rule, the probability values are predicted for classifying the packets.

TABLE 3. Probability values of fuzzy output.

Fuzzy output	Probability value
High	1
Medium	0.75
Low	0.50
Very Low	0.25

By using all the above mentioned six features, the classifier is executed. These features are extracted in a feature analyzer that is present in each controller. The decision of high in fuzzy denotes that the device is assumed to be legitimate and the condition of medium is also taken into account since it has passed the signature-based authentication. But if the very low condition obtained in the final fuzzy, the packet from the particular device will be ignored.

However fuzzy is a well-known algorithm, using many numbers of a rule on single fuzzy consumes little higher time. So, in this work, multiple fuzzy is introduced with a neural network for faster processing and accurate detection of forged packets injected into the system. An adaptive- network-based fuzzy interference system (ANFIS) is used based on the Takagi-Sugeno interference system.

In ANFIS, the membership parameters are tuned using back-propagation algorithm and assisted with hybrid learning [49]. The ANFIS is faster in learning and it is operable with the knowledge on both linguistic and numeric. The IF-THEN fuzzy rules in ANFIS is determined using the Sugeno model as,

Rule: IF x is A_1 AND y is B_1 THEN

$$F_o = p_1 x + q_1 y + r_1$$

Let x and y be the input parameters that obtains F_o as output from A_1 and B_1 fuzzy sets with p_1, q_1 and r_1 design parameter. A set of six neurons are present in the hidden layer using which the features are extracted in the proposed work. In the proposed forensic architecture, the neuro multi-fuzzy logic model is used as shown in Fig. 5. The benefit of the neural network and fuzzy are faster processing speed and take into account multiple parameters. Both the potential benefits are combined and constructed as a neuro multi-fuzzy logic model. In this model, six significant parameters are considered for making a faster decision. Most of the packets are addressed to be legitimate after authentication, but in some cases, the malicious activity can find only using the packet features. Then the designed forensic architecture on SDN enabled IoT environment. Security is achieved by means of blockchain technology. Hereby, finally, the evidence is stored on SDN-controllers that are present in the control plane. The stored evidence will include hash values; here the maintenance of evidence is carried over by the establishment of CoC. In this architecture switches also play a vital role in inhibiting the growth of malicious users on the control layer. The

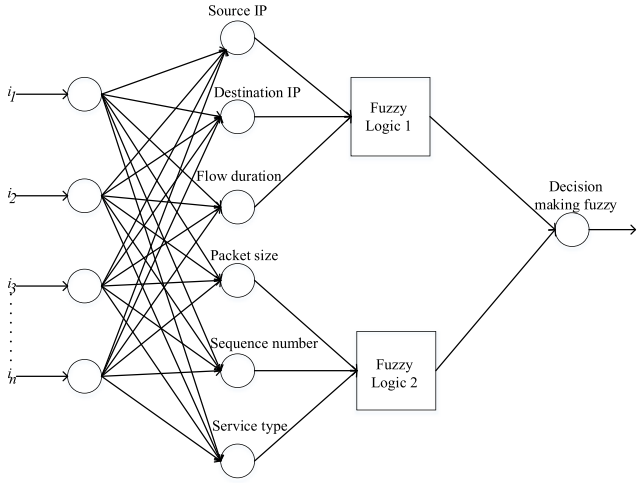


FIGURE 5. Neuro Multi-Fuzzy logic Model.

complete forensic network architecture is developed under SDN based IoT environment. The majority of the proposed Forensic SDN-IoT is handled by using packet features which are the key with which a fake person can enter into the system.

Due to this reason, we have contributed our entire work with a detailed analysis of packet features on algorithms. The previous work SDN-Fog was also involved with the processing of packet features but it was enabled to identify specify security threats and the maintenance of data log was not discussed which is essential in blockchain technology. The evidence as data logs is the change of status representation along with the actions that are taken for the status. Storing of these logs is available for forensic investigators.

Let Packet Parser be PP, Feature analyzer is FA, source IP be Scr_IP, destination IP be Dst_IP, flow duration is Flw_Dur, packet sized be Pck_Size, sequence number be Seq_Nub, Service type be Srv_type, Fuzzy Output 1 be FO_1, Fuzzy Output 2 be FO_2 in pseudo code 2. This depicts the proposed SDN-controller's working procedure. Packet Parser and Feature analyzer in controller monitors the behavior of packet and extracts features, then the packet allowed into the blockchain. The signature of each user is validated in the blockchain using LHS algorithm for authenticating the user. After authentication, the user's packets are classified with neuro-fuzzy based on the defined fuzzy membership functions. Six different packet features are taken into account for classifying the packets.

Record entities **Description**

user - User identity

Scr_IP- IP address of corresponding source device

Dst_IP - IP address of the destination

time - Time of event occurrence

location - Latitude and Longitude coordinates of the source device

action - Carried out action

In this Forensic-SDN-IoT, the packets are classified and the evidence is stored into the SDN-controllers. The evidence in the controller is stored with the hashes of the corresponding evidence for maintaining CoC in the blockchain. Evidence is stored in the pre-configured location in a controller, the data logs include user identity, Source IP address, Destination IP address, local time of event occurrence, location and action. Each entity in the record as defined above based on which those data are stored.

TABLE 4. Simulation Parameters.

Parameters		Specifications
Network environment	IoT devices	20 – 40
	Gateway	2
	OpenFlow Switches	4
	Controllers	4
Inter packet interval		40 ms
Blockchain	Block size	4 bytes
	Block header	80 bytes
	Transaction counter	1 – 9 bytes
	Number of transactions	Variable
	Signature generation	Linear Homomorphic algorithm
	Proof Type	Proof of Work
Simulation time		40 s

V. PERFORMANCE EVALUATION

This section is segregated into two sub-sections as simulation environment and comparative result. In this section, the proposed forensic architecture in SDN based IoT environment is validated under different significant network parameters. The achievements of this proposed architecture are illustrated and the results are discussed in this section.

A. SIMULATION ENVIRONMENT

Forensic Architecture in SDN based IoT is developed using Network Simulator version 3 (NS3). In NS3, to integrate the concept of blockchain in SDN based IoT this architecture has been designed using the Bitcoin coding part into NS3 [50], [51]. NS3 tool implementation based on the work in [52]. Nearly 100 numbers of blocks have been generated for our simulation and 16 miners are involved for testing. The blocks in the blockchain are created at an average of 10 sec time intervals. The number of malicious packets from IoT devices is gradually increased by 50, 75, 100 and 125 for evaluating the efficiency of the proposed forensic SDN architecture. OpenFlow switch version 0.8.9 which creates conventional flow table along with the deployment of proposed rules regarding traffic type. Each switch affords with 50 – 75 flow entries. Then the control employed in this proposed simulation constructed internal SDN controllers that includes packet features which are used for classifying the packets.

Table 4 depicts the major parameters that are involved to design a forensic architecture over SDN based IoT. The specifications are not limited to this extent. Based on the blockchain specifications, the controllers create blocks for the registered IoT devices and generate the signature.

Pseudo Code 2 Process Followed in Controllers

```
1:  begin  // start the process
2:  i1, i2, i3, ....., in → Controller  //Packets from individual user's
                                        // is submitted into controller
3:  if (PP → Flow_Mod, Packet_In, Status_Reply, Features_Reply)
      {                  // Begin controller processing
    PP = 1
    Regular packet
4:  else
    Irregular packet
    }
5:  end if  // end of Packet Parser
6:  FA extract (Packet features)   // Packet feature extraction
7:  if (St = True)   // Signature authentication for user
    {
     Authorized user   // User permitted into the system
                       //with signature validation
     Goto step 10
8:  else
    Unauthorized User // Invalid signature and user is
     not permitted
    }
9:  end if  // end of Signature authentication
10: packet classification
11: features extraction (Scr_IP, Dst_IP, Flw_Dur,\
                         Pck_Size, Seq_Nub,  Srv_type)
12: FL1 → Scr_IP, Dst_IP, Flw_Dur→ FO1  // Features processed
                                        //in fuzzy logic 1
13: FL2 → Pck_Size, Seq_Nub, Srv_type → FO2   // Features
processing
                                        // in fuzzy logic 2
14: if (FO1 = 1 & FO2 = 1)   // Decision making in fuzzy logic
    {
     Legitimate Packet
15:  else if (FO1 = 1 & FO2 = 0.50) or (FO1 = 0.50
     & FO2 = 1)
        {
         Legitimate Packets
16:    else
         Malicious packets
         }
17:    end if
    }
18: end if  // end of Decision making in fuzzy logic
19: evidence stored in controller
    {
     records r1, r2, r3, ...
20:   for each ri
      {
21:     user = user id     // identity of the user
22:     Scr_IP = xxx.xxx.xxx.xxx
23:     Dst_IP = yyy.yyy.yyy.yyy
24:     time = hh:mm:ss   // hour:minute:second
25:     location = X,Y position
26:     action = user action
      }
27:   end for
    r1, r2, r3, ... → blockchain   // records stored in the blockchain
    blockchain → Tr1, Tr2, ...   // Transactions in blockchain
    }
28: end   // finish the process
```

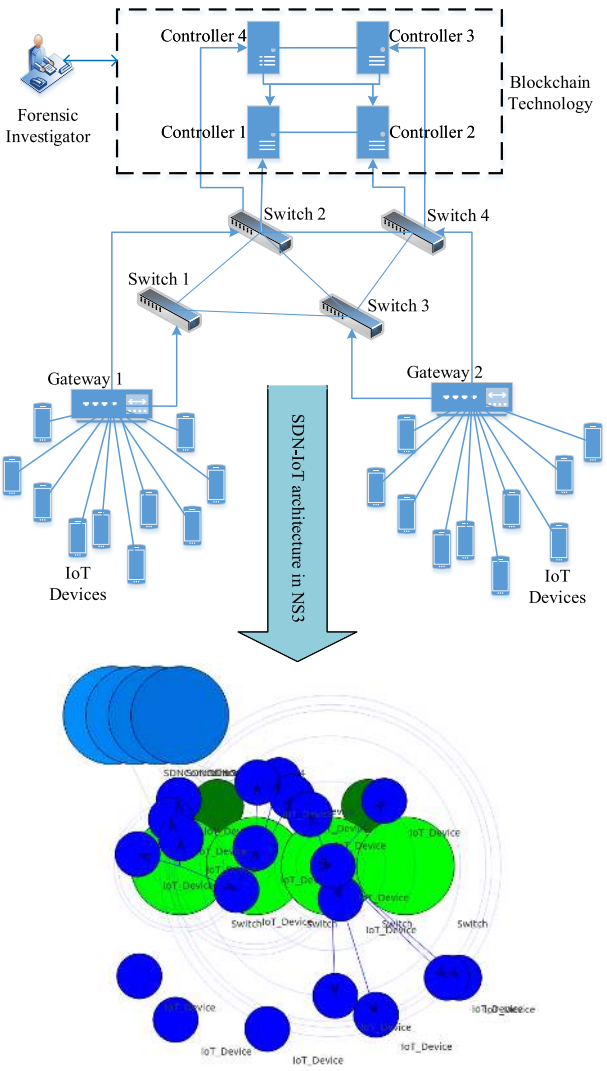


FIGURE 6. Forensic simulation architecture model.

The impact of blockchain technology is studied by comparing significant parameters in upcoming sections.

This NS3 is installed on the Ubuntu operating system and executed the developed forensic architecture. C++ is the programming language used for generating algorithms and Python is used for the purpose of compiling the created architecture. The designed forensic architecture is shown in Fig. 6 and their performances are evaluated. Also, the real implementation setup executed in NS3 is demonstrated in accordance with the simulation parameters that are discussed above. Based on this architecture, the better achievements of the proposed architecture are analyzed in the next section.

B. COMPARATIVE RESULTS

A detailed comparative study is presented on the following metrics like delay, response time, throughput, processing time and security analysis. These five parameters are considered to be significant for validating the achievements in the forensic

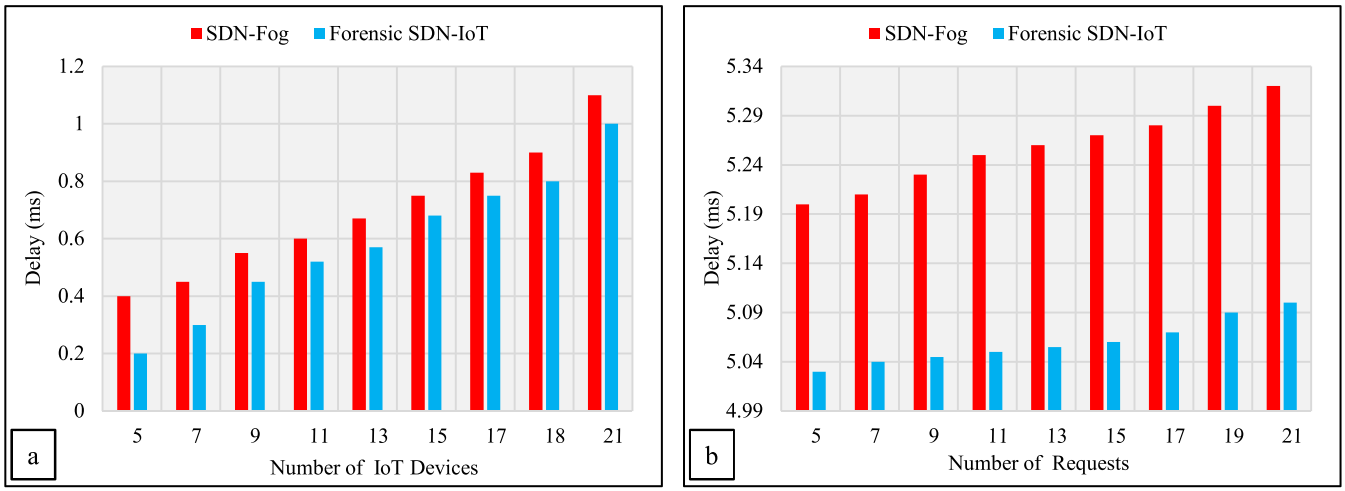


FIGURE 7. Delay incurred by a) increasing the number of devices; and b) increasing the number of requests.

and network. The proposed forensic SDN-IoT is compared with previous SDN-Fog architecture which detects flooding attacks in controllers. SDN is integrated with different areas for ensuring better system performances.

However, it introduced the problem of security in each sequential process. SDN-Fog uses the technology of blockchain, where flooding is the only attack detected. Still, many other malicious packets participate in the system. So SDN-Fog with blockchain is compared with our proposed Forensic SDN-IoT with blockchain technology.

1) DELAY

Delay is one of the significant metrics that is measured in the developed network environment. A well-designed network is supposed to have less delay, since the delay is a metric which is required to lessen in order to achieve a better quality of service. The variation in delay with respect to the number of IoT devices is shown in Fig. 7(a).

This comparison shows that the proposed Forensic SDN-IoT with minimized delay. In previous SDN-Fog design delay is higher, since it focused on the identification of attacks which increases the delay. Whereas in this proposed forensic architecture, the packets are verified by using simple rules and hence they are forwarded into a control plane without any delay. The value of delay gradually increases while the number of devices increases.

The variation in delay is only a few milliseconds of 0.1 – 0.2 after beginning packet transmission from the end user. However this is a minor change in values, it will be large if the number of devices is further increased. In the proposed SDN forensic architecture, three different traffics are taken into account; if any one type of traffic is involved, the delay could be minimized more. Delay is also plotted with respect to the arrival of the number of requests. The number of requests denotes the arrival of packets at each second into a gateway from each device.

Fig. 7(b) demonstrates the minimization of delay when compared with prior SDN-Fog design. As per the increase in number of requests, it tends to increase the participation of IoT devices.

The reduced mathematical computation is also a major reason in mitigating delay metric. Delay is associated with packet transmission and so it is plotted in accordance with the number of requests. However the changes are minor in delay variations, it reflects over other significant network parameters. The better achievement of delay metric is due to minimized computation and faster processing of packets.

2) RESPONSE TIME

Response time is the time taken by the IoT devices to receive the response for the requested service. This metric is validated based on the number of requests that are arrived from end devices.

In the proposed forensic architecture, every IoT device sends packets to the gateway which is forwarded to switches and then they are authenticated by using the signature in controllers. Until verification is completed, the time is known to be response time. Fig. 8 illustrates the comparison of response time for proposed forensic architecture with respect to the previous SDN based fog architecture.

This comparison shows that the proposed forensic architecture is better since the processing of rules and verification is faster and it minimizes response time even if the number of requests increases.

3) THROUGHPUT AND ACCURACY

Throughput is one of the important parameters that is taken into account for validating the proposed Forensic architecture. Throughput is defined as the measure of successful transmission of packets between users in a given time in accordance with the number of request packets.

Fig. 9 demonstrates the variation in throughput for validating the better efficiency of proposed forensic SDN-IoT architecture. The increase in throughput denotes that there are many numbers of successful data transmissions. Increase in

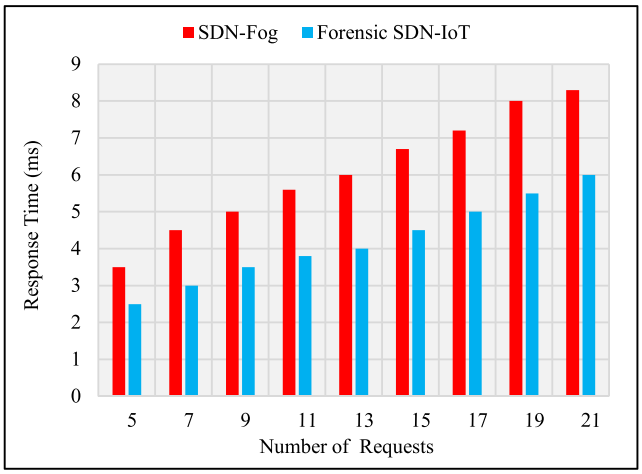


FIGURE 8. Comparison on response time.

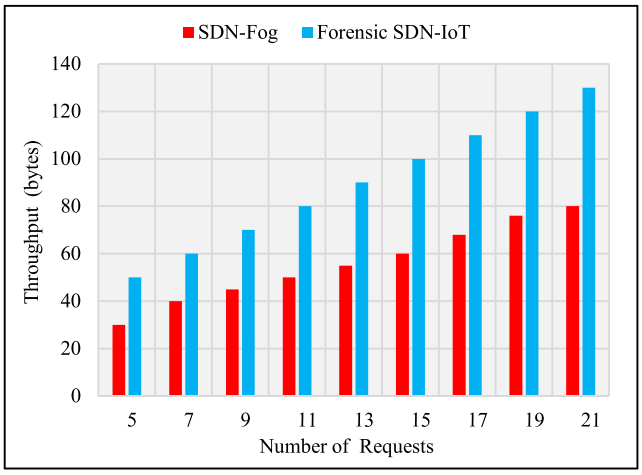


FIGURE 9. Comparison on throughput.

the throughput enables to achieve improvement in network performance.

Improvements in forensic architecture are achieved due to the involvement of flow rules based traffic analyzing on switches and signature verification in the controller. The reduction of malicious packets into the network is one of the reasons for the increase in throughput. This metric also indicates the quality of devices connected in the network. During the simulation time, forensic architecture has attained 50 – 130 bytes of throughput, whereas the previous work achieves only 30 – 80 bytes at similar simulation time.

The measurement of throughput is enabled to illustrate any type of large scale network infrastructure. An increase in throughput on forensic architecture impacts on other significant network parameters and ensures better performances of the network. Gradual growth in throughput illustrates that the further increase in throughput will be achieved at higher simulation time.

Accuracy plays a significant role in detecting accurate malicious packets. A poor mechanism will result in detecting legitimate packets as malicious which drops the accuracy.

TABLE 5. Detection accuracy.

Packets Arrived Per Second	Total Number of Packets		Packets Classified		Detection Accuracy (%)
	Legitimate	Malicious	Legitimate	Malicious	
10	350	50	348	52	99%
20	725	75	720	80	98%
30	1100	100	1090	110	98%
40	1475	125	1460	140	97%

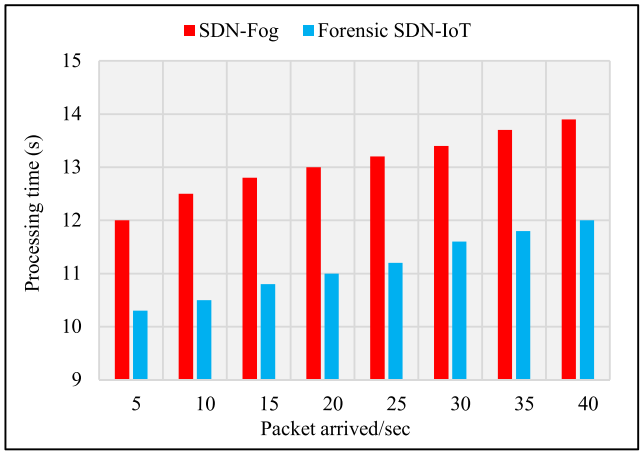


FIGURE 10. Comparison on processing time.

We evaluate the accuracy of our proposed work in terms of the incoming packets.

Table 5. depicts the detection accuracy for the present work that processes with the number of packets from IoT devices. As per the increase in packet arrival rate, the packet detection accuracy shows a gradual decrease since the number of incoming packets is higher.

4) PROCESSING TIME

The complete packet handling time from the gateway to the control plane is computed as processing time. This includes the working of algorithms at each plane and each entity for the arrived number packets from IoT devices.

Fig 10 demonstrates the variation of processing time with respect to the arrival of packets for SDN-Fog and proposed Forensic SDN-IoT architecture. According to the increase in the number of packets arrival, the processing time increases since it needs to process on more number of packets.

The processing time at 5 packets per second is 10 seconds in forensic SDN-IoT, whereas in SDN-Fog it is 12 seconds. However, the difference is smaller, the gradual increase in the number of arrival packets reflects on the network. The reduction of processing time tends to achieve a good quality of the designed architecture and ability to tolerate many numbers of packets from IoT devices. The noticeable minimized processing time is lesser, even if the numbers of arrival packets are grown. Computation complexity is defined from

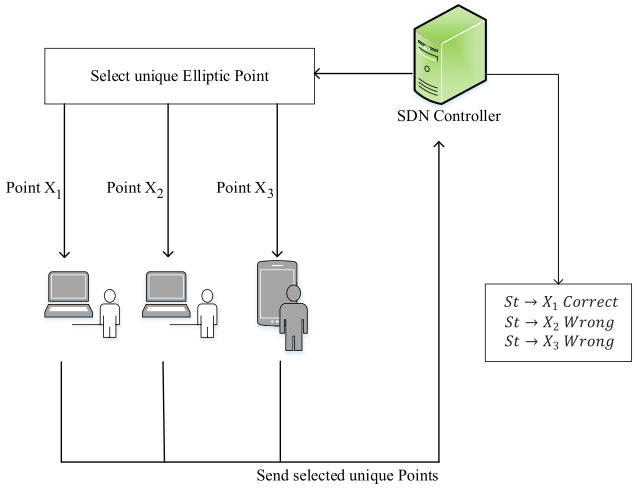


FIGURE 11. Signature based Proof generation.

TABLE 6. Time complexity.

Algorithm Used	Time Complexity
Neuro Multi-Fuzzy	$\approx O(n^2)$
Linear Homomorphic Signature algorithm	$\sim O(n)$

the utilization of resources for the algorithm with respect to the total number of inputs. Resources involved in this forensic architecture are the configuration of individual devices in the plane. To express the complexity, we predict time complexity for the proposed LHS algorithm and neuro multi-fuzzy algorithm. Let n be the number of inputs and c be the constant which is required to determine execution time. The algorithm executed in a loop until all the n inputs are processed, so the total execution time will be $T(n)$. From the determined total time, the complexity is predicted using the asymptotic notation O. Using big-O notation time complexity is determined from the following formulation,

$$f\ (n) \leq c * g\ (n)\ for\ all\ n \geq n_0$$

$f(n)$ and $g(n)$ are the monotonic functions, here $f\ (n) = O(g(n))$ when $c > 0$ and $n_0 > 0$.

Table 6 depicts the time complexity based on the number of input. O represents an order of the time complexity. In neuro multi-fuzzy, however, three fuzzies are used they process parallel; hence, the time complexity is comparatively higher than of algorithms in the control plane. In LHS, the algorithm is operated linearly which takes all the steps to undergo for each input. On the whole, all the comparative result shows that forensic SDN-IoT architecture is better than SDN-fog that uses blockchain technology for enhancing network performances. The involvement of port number based flow rules and blockchain technology with signature algorithm have supported to attain better results in terms of delay, throughput, response time and processing time. All the significant network parameters show improved results when compared with previous SDN-Fog architecture. The use of blockchain technology for security is highlighted and the applicability on IoT devices is presented, further, their performances are validated.

5) SECURITY ANALYSIS

The provisioned security in this proposed work is validated by provenance, interoperability evidence acquisition, and trust. The proposed forensic SDN-IoT is efficiently designed for detecting malicious involvement in the system. The utilization of blockchain technology in the control plane of SDN ensures to provide security. Our security analysis is depicted as follows:

- Provenance: Provenance is the aggregation of evidence by suspecting the malicious user. In our proposed work, the packets from devices are validated in accordance with the port numbers, so only unsuspected packets are allowed for further processing. Hence forensic SDN-IoT supports provenance requirement since, each user log includes address, time, location and packet features that created provenance and evidence are collected in the controller and if there is a change in data log it is updated. In existing SDN-Fog architecture, the abnormal behavior of users is detected.
- Evidence Acquisition: Forensic SDN-IoT makes sure that all the data logged and evidence are stored in the controller which can be accessed by the forensic investigator i.e. the person in charge to detect the cause of the issue. On using blockchain technology the data is maintained secure and hence this work supports evidence acquisition too.
- Trust: In this Forensic SDN-IoT design, the generated logs are stored within the SDN-controllers, which is highly secure and it cannot be easily accessed by any third party. In addition to storing events/logs (as evidence) in controllers, the hash of evidence is also stored by the controller in Blockchain. This is used to maintain the integrity of evidence and increase reliability level of CoC. We will be authenticating the access for the forensic investigator before providing the data logs. The assurance in trust also ensures with the increase of confidentiality.
- Simplicity: The data logs are simply stored on the controller since they are secured parties in the control plane. The controllers are assisted with sufficient memory capacity for storing data logs.
- Detection of the malicious act: Compromising of intermediate entities and entering into the network is the main act of attackers. In this forensic SDN-IoT, we allow user's traffic in accordance with port number and then permit into a data plane for processing. And then neuro-fuzzy classifies the data packets for predicting malicious packets. Hence it identifies any suspicious packets entering into the network.

In this proposed Forensic SDN-IoT, the authentication of IoT devices and detection of malicious users/traffics with classifications of packets with Neuro Multi-fuzzy based on

packet features and three predefined traffic rules in OpenFlow Switches greatly mitigate attacks at the edge of the network.

6) SECURE SIGNATURE FOR DECENTRALIZED AUTHENTICATION

In the blockchain, the PoW is presented for confirming that the transactions are handled by the miners. For PoW, a mathematical puzzle is submitted to users as a hash function, integer factorization. In our proposed work, the users are requested to select a unique elliptic point using the formulation discussed in above sections.

Using the elliptic point (X_1, X_2, X_3), a signature is generated and the correct problem solving users are rewarded. *St* is the signature that is generated using the elliptic point and identity of the user, which is unique for each user. Here the problem is the selection of point from the elliptic curve. If the miner is enabled to solve this then a new block will be created for placing the status.

Fig. 11 depicts the signature generation method of authentication presented in Forensic SDN-IoT architecture. The major advantage of PoW is to ensure anti-DoS attacks. Using this LHS algorithm, it is complex for the attacker to identify the unique point.

VI. CONCLUSION

In this paper, a new forensic architecture is developed on SDN based IoT network environment. Provisioning of security in the designed architecture is the main scope of this research. The proposed forensic architecture is presented with a blockchain technology that assisted to provide the increase in confidence level security and CoC effectively accomplished for evidence collection for integrity. According to a common SDN design, our forensic architecture comprises of control plane and data plane. IoT devices get connected with data plane via gateway nodes. The aggregated packets in the gateway are forwarded to the data plane that is comprised of OpenFlow switches. Three different traffics and their corresponding port numbers are fed into switches. In accordance with the flow rules that are applied on switches, the action for each packet is held. Also, the overload at a switch is mitigated by migrating packets based on the flow entries. This process initially drops the mismatching packets and forwards all the remaining packets to control plane. The control plane is composed of controllers which involve blockchain technology. LHS algorithm is used with a unique device ID and elliptic curve point. Device signatures are authenticated before transactions. Once the device is authenticated, the packets are classified, based on six significant features, using Neuro Multi-fuzzy logic model for achieving completed security in the designed architecture. Forensic SDN-IoT architecture is prepared to collect data log evidence in the SDN-controller and blockchain for future analysis. On the whole, the performances of the proposed architecture are evaluated in terms of delay, throughput, accuracy, response time, processing time, and security. The results of our performance evaluation clearly demonstrate that compared to the previous work, our proposed architecture is more efficient and secure. It also indicates SDN-IoT is lightweight forensic architecture with minimal overhead.

In the future, we have planned to validate this proposed architecture in a large scale network environment and include an initial authentication and load balancing mechanism at gateway entities. Still, the evidence acquisition in this forensic design could be enhanced and increase the reliability level of CoC using smart contracts.

REFERENCES

[1] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN control: Survey, taxonomy, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 333–354, 1rd Quart., 2018.

[2] M. B. Yassein, S. Aljawarneh, M. Al-Rousan, W. Mardini, and W. Al-Rashdan, "Combined software-defined network (SDN) and Internet of Things (IoT)," in *Proc. Int. Conf. Elect. Comput. Technol. Appl. (ICECTA)*, Nov. 2017, pp. 1–6.

[3] K. Kalkan and S. Zeadally, "Securing Internet of Things with software defined networking," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 186–192, Sep. 2018.

[4] Z. Zhou, J. Gong, Y. He, and Y. Zhang, "Software defined machine-to-machine communication for smart energy management," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 52–60, Oct. 2017.

[5] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern. Syst.*, to be published.

[6] A. Nayak and K. Dutta, "Blockchain: The perfect data protection tool," in *Proc. Int. Conf. Intell. Comput. Control (I2C2)*, Mar. 2017, pp. 1–3.

[7] K. Christidis and M. Devetsikiotis, "Blockchain and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] B.-K. Zheng, L.-H. Zhu, M. Shen, F. Gao, C. Zhang, Y.-D. Li, and J. Yang, "Scalable and privacy-preserving data sharing based on blockchain," *J. Comput. Sci. Technol.*, vol. 33, no. 3, pp. 557–567, May 2018.

[9] C. Ehmke, F. Wessling, and C. M. Friedrich, "Proof-of-property: A lightweight and scalable blockchain protocol," in *Proc. 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, 2018, pp. 48–51.

[10] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Aug. 2018.

[11] Y. Zhang, Y. Han, and J. Wen, "SMER: A secure method of exchanging resources in heterogeneous Internet of Things," *Frontiers Comput. Sci.*, vol. 13, no. 6, pp. 1198–1209, 2019,

[12] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[13] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[14] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jul. 2018.

[15] Z. Li, M. Shahidehpour, and X. Liu, "Cyber-secure decentralized energy management for IoT-enabled active distribution networks," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 900–917, Sep. 2018.

[16] M. Vukolić "Rethinking permissioned blockchains," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts (BCC)*, 2017, pp. 3–7.

[17] B. A. Scriber, "A framework for determining blockchain applicability," *IEEE Softw.*, vol. 35, no. 4, pp. 70–77, Jul./Aug. 2018.

[18] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2017.

[19] J. Li, "Data transmission scheme considering node failure for blockchain," *Wireless Pers. Commun.*, vol. 103, no. 1, pp. 179–194, Nov. 2018.

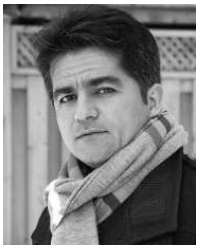
[20] D. Zhaoyang, L. Fengji, and G. Liang, "Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 958–967, Sep. 2018.

[21] H. Hyvärinen, M. Risius, and G. Friis, "A blockchain-based approach towards overcoming financial fraud in public sector services," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 441–456, Dec. 2017.

[22] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 464–467.
[23] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.
[24] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[25] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.
[26] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.
[27] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 303–308.
[28] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, May 2017, pp. 720–725.
[29] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Availability, Rel. Secur. (ARES)*, 2017, Art. no. 14
[30] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.
[31] M. Wang, Q. Wu, B. Qin, Q. Wang, J. Liu, and Z. Guan, "Lightweight and manageable digital evidence preservation system on bitcoin," *J. Comput. Sci. Technol.*, vol. 33, no. 3, pp. 568–586, May 2018.
[32] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, 2017, pp. 173–178.
[33] C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, blockchain based access control framework for the heterogeneous Internet of Things," in *Proc. 3rd ACM Workshop Attribute-Based Access Control*, 2018, pp. 61–69.
[34] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.
[35] M. Steichen, S. Hommes, and R. State, "ChainGuard—A firewall for blockchain applications using SDN with OpenFlow," in *Proc. Princ., Syst. Appl. IP Telecommun. (IPTComm)*, Sep. 2017, pp. 1–8.
[36] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018.
[37] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, no. 8, p. 141, Aug. 2018.
[38] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.
[39] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Trans. Intell. Technol.*, vol. 3, no. 2, pp. 114–118, Jun. 2018.
[40] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
[41] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*. [Online]. Available: https://arxiv.org/abs/1802.01746
[42] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 152, 2018.
[43] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *Proc. 11th Int. Conf. Auton. Infrastruct., Manage. Secur. (AIMS)*, 2017, pp. 16–29.
[44] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[45] C. H. Lee and K.-H. Kim, "Implementation of IoT system using block chain with authentication and data protection," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, 2018, pp. 936–940.
[46] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 296–301.
[47] A. G. Abbasi and Z. Khan, "VeidBlock: Verifiable identity using blockchain and ledger in a software defined network," in *Proc. 10th Int. Conf. Utility Cloud Comput. (UCC)*, 2017, pp. 173–179.
[48] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.
[49] A. A. Hmouz, J. Shen, R. A. Hmouz, and J. Yan, "Modeling and simulation of an adaptive neuro-fuzzy inference system (ANFIS) for mobile learning," *IEEE Trans. Learn. Technol.*, vol. 5, no. 3, pp. 226–237, Sep. 2012.
[50] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2016, pp. 3–16.
[51] A. Gervais. *Bitcoin Simulator*. Accessed: May 27, 2019. [Online]. Available: http://arthurgervais.github.io/Bitcoin-Simulator/
[52] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, Apr. 2018, Art. no. 9675050.

MEHRAN POURVAHAB received the B.Sc. degree in software engineering from Islamic Azad University, Bafgh Branch, Iran, in 2001, and the M.Sc. degree in information technology engineering-networking from Guilan University, Rasht, Iran, in 2013. He is currently pursuing the Ph.D. degree in software system engineering with the Islamic Azad University, Rasht Branch, Rasht.

Since 2016, he has been a Faculty Member of the Department of Computer Engineering, Islamic Azad University of Langarud Branch, Iran. Since 2001, he founded the first Internet Service Provider (ISP), Langrud, Guilan, Iran. Since then, he has been the System/Network Administrator of MehranNet (ISP) with more than 3000 subscribers. From September 2006 to November 2018, he was the Manager of information and communication technology at the Azad University of Langarud Branch. Since 2011, he has been the MikroTik Certified Trainer and Consultant. Since August 2018, he has been the Head of the Security and Network Commission of Iranian ICT Guild Organization (IIG). His main research interests include software-defined networking (SDN), cloud forensics, network security, and blockchain technology. He is a member of the IEEE Computer Society and serves as a Reviewer of the IEEE Access Journal.



GHOLAMHOSSEIN EKBATANIFARD received the B.Sc. degree in software engineering from the Islamic Azad University, Lahijan Branch, Guilan, Iran, in 2001, and the M.Sc. degree in computer network security, and the Ph.D. degree in software systems from the Ferdowsi University of Mashhad, Iran, in 2004 and 2013, respectively. He has been an Assistant Professor with the Azad University of Lahijan Branch, Iran, since 2013. He attends to Islamic Azad University, since 2005. From February 2012 to August 2012, he was a Visiting Researcher with the Delft University of Technology, The Netherlands. From November 2013 to April 2017, he was the Director of the Information and Communication Technology Center, Azad University of Lahijan Branch. His research interests include design and performance evaluation of communication protocols for wireless networks, network security, and cryptocurrency technologies.