phdprimehelp@gmail.com
+91-97 91 62 64 69

Ph.D. Research Proposal

Doctoral Program in "Department Name"

Forensic Investigation and Digital Evidence Detection in Smart Cloud enabled SDN Environment using Modified Blockchain Technology

by

<Name of the Candidate>

<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>

I. INTRODUCTION / BACKGROUND

Digital Forensics (DF) is one of the fast growing technologies that has significant role in the area of criminal investigation. The basic goal of forensic is to understand the interest of event by finding and analyzing the facts related to that event. DF is the process of converting the collected data at collection phase into evidence.

According to study in [1] has changed the definition of cyber-crime to cloud crime as, a crime which takes place at cloud computing environment where cloud is considered as the object, subject and tool of crimes. The cloud service provider is considered as the object, cloud environment is the subject where crime took place i.e. cloud and tool is the application tool used to processed a plan and implemented in cloud crime. Cyber criminals may use different types of attacks (like Distributed Denial of Service) to target the cloud service provider or can commit a crime for illegal access of data, theft of the user identity or can use cloud for storing the data related to crime. He also stated that, cloud computing is done on the basis of wide network access and network forensics is the investigation of networks.

The security is becoming a great threat to all the industries in recent years. In today's world, everything around us is connected with the environment. With the introduction of Internet of Things (IoT) things started communicating with each other. The cloud computing technology offers unlimited storage with other useful resources for the people. Researchers nowadays focus on working in the integrated domain environments, since the drawbacks of one domain is balanced by the advantages of the other domain. This showed a great increase in the realization of full-potential of the number of domains being considered.

SDN is one of the type of networking area that consists of separation of the network control plane (controls several devices) and the data plane (forwarding plane).SDN encompasses several types of technologies including the functional separation, network virtualization and automation through programmability. With the separation of control and data plane, the control plane

decides how the packets should flow through the nodes present in the network. On the other hand, the data plane simply makes the movement of packets from one place to another as directed by the control plane. In any network environment with the implementation of SDN, The packets that arrive at the network switch will follow the rules built into the switch's proprietary firmware. These rules are transferred to the switch from the centralized controller.

1.1 Research Outline & Scope

The security is becoming a great threat to all the industries in recent years. Digital Forensics (DF) is one of the fast growing technologies that has significant role in the area of criminal investigation.

1.2 Research Objectives

The main research objectives of this work are as follows.

- To reduce computational overhead
- To reduce key generation time and encryption and decryption time
- To strong authentication with accurate verification of evidence's reliability
- To invent new hashing algorithm instead of using $(SHA256)^2$ with small timing and space complexity
- To detect any false flow rules with use of blockchain technology

II. RESEARCH GAPS

Primarily, there are three issues in this integrated domain i.e. (1). Centralized evidence collection leads to poor security, (2). Poor data integrity and evidence reliability, and (3). Weak authentication with poor accuracy.

2.1 Common Problem Statement

A smart cloud environment is centralized in which attacker is able to crack all logs and evidences by compromising single entity (i.e.) CSP. Blockchain based distributed cloud storage was designed address such security and privacy preservation issues. Here involvement of (SHA-

256)[2] increases time consumption for hashing whereas elliptic curve based digital signature algorithm (ECDSA) algorithm minimizes security level due to ineffectual key generation.

2.2 Problem Definition

In [1] proposes an expert system for forensic monitoring, analysis, and evidence generation for cloud logs. The overall process is involved with identification of source, data collection from source, analysis of evidences, and reporting of evidences. For forensic acquisition, a fuzzy based data mining technique is adapted. Here evidences are stored in log storage under the control of cloud service provider.

Problems

- Centralized log storage decreases the reliability of collected evidences and log integrity is not ensured
- Fuzzy based forensic monitoring is simple trace by attackers

Proposed solution

- Use of blockchain for evidence collection and preservation resolves the single point failure since blockchain is stored in a distributed manner
- Blockchain ensures data integrity through SPONGENT and integrity is verified by investigator through Evidence Graph Construction.

In [2], a security information and event management is designed for cloud forensics. Here the collected evidences are shared among cloud users instead of stored in cloud server. To improve security Rivest Shamir and Adelman (RSA) encryption algorithm is adapted. The proposed work includes following processes: Digital Forensic Data Collection, Digital Forensics Data Generation, Real-Time Processing, Machine Analysis, Digital Forensic Analytics, Actionable Intelligence, And Incident Response.

Problems

- Here evidences are shared among cloud users but the cloud users are not authenticated. Thus the malicious user can be access the evidences which leads unreliable evidence collection.

Proposed solution

- Each user as well as investigator are authenticated by SRVA scheme which prevents the malicious user activity in the system

In [3] 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 will transfer 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. A Potential solution for solving forensic is the use of Blockchain in software-defined networking (SDN).

Problems

- Homomorphic encryption is not suited for real-time implementations since is slow with poor performance and security is poor with the algorithm implemented
- Elliptic Curve Cryptography point is used to authorize the IoT devices. However, IoT is resource constrained so that the lightweight cryptography algorithm must require to handle this issue.

Proposed Solutions

- Four Q-Curve is the best which is better than ECC since IoT is resource constrained which requires lightweight security solution

An efficient and secure process (ESP) [4] is characterized by employing a Blockchain - based provenance record chain and can provide a secure and efficient system for data outsourcing, where the correctness, integrity, and timeliness of provenance records can be ensured. Furthermore, this paper introduces a concept of window of latching (WoL) to assess the practicality of secure provenance schemes. Data provenance, which records the history of the ownership and process of a document during its lifecycle, is essential for the success of cloud storage systems. However, it also inevitably incurs some challenging security and privacy issues.

Problems

- The authenticated credentials are easily cracked by the attackers
- Very poor security with weak authentication schemes

In this paper [5] 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 is performed in this paper. In this, the first step validates the service profile and then the controller is provided with device profile for validation.

Problems

- Validator needs to verify all the devices
- Packets are dropped if the servers are not known by the controller.

Proposed Solutions

- All the packets from devices are validated, we discard malicious packets only

III. RESEARCH CONTRIBUTIONS

- **User Registration and Authentication**

In our proposed system, the user will initially perform the registration process with the legal authority. The Cuckoo Search Optimization algorithm is implemented for this registration purpose. The key is provided to the user who has successfully registered their

account. After that the user will enter into the system with the help of these credentials. The user will provide the id, password, finger vein, PUF and a random number to the trusted authority for the verification purpose. If the verification is successful, the user is granted authentication, otherwise the access is rejected.

- **Data Encryption and Storage**

The authenticated user can upload or download the data in a secure manner. The user can determine the sensitivity level of their data as either sensitive or non-sensitive. In case of sensitive data, it is encrypted twice and in case of non-sensitive data it is encrypted only once. For the purpose of encryption, we have implemented Privacy Aware Neural Four Q-Curve algorithm. This encrypted data is uploaded into the cloud. The encrypted data from the user is stored into the cloud through the switches.

- **Evidence Collection in Blockchain**

The encrypted data is stored in the IaaS cloud. The SDN controller will create the blocks in the Blockchain for each data being uploaded into the cloud. This block contains the list of transactions and the hash value of data, previous block and then the timestamp value. In the blocks, the hashes are created using the Spongent Function algorithm. The main idea behind the Blockchain implementation is to capture the actions performed on the data while ensuring the security of the data.

For the purpose of tracking the access of data on the cloud, we implemented Neutrosophic Intelligence Smart Contract Algorithm. Any access on the data is noted in the Blockchain (i.e.,) any modification done to the data in the cloud, it is also reflected in the Blockchain. The information such as who accessed the information and what type of action has been performed and from where the data has been accessed and other such details are stored in the block.

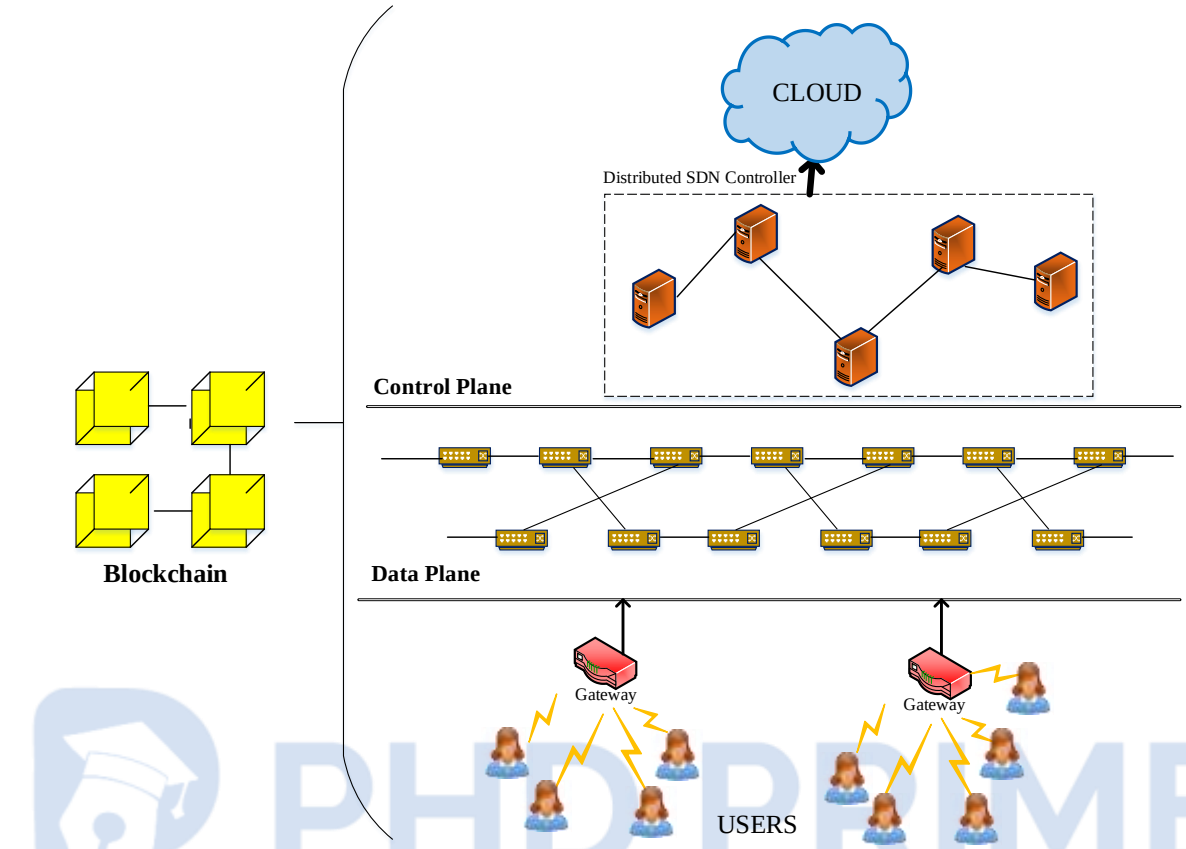
- **Mining of Evidence Information**

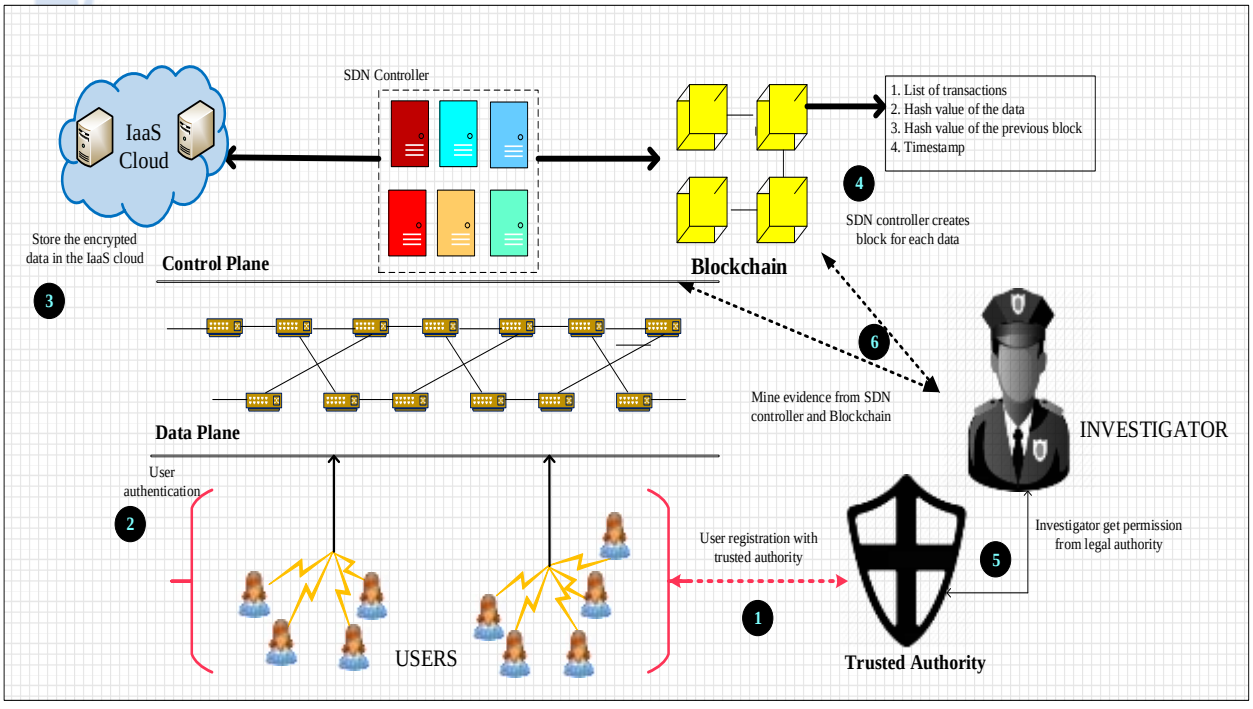
The investigator will get the permission from the legal authority before accessing the data. After getting permission, the investigator will mine the data from the SDN controller and the Blockchain, and then the investigator constructs the Consistent Evidence Graph (CEG). Thus, our system guaranteed to provide security and also tracing back the user who is suspect. The performance evaluation also showed the worth of the proposed system.

Performance Evaluation

- Response time
- Evidence insertion & verification time
- Communication & computational overhead
- Hash computation time
- Key generation time
- Encryption and Decryption time

SYSTEM ARCHITECTURE


CLOUD
Distributed SDN Controller
Control Plane
Blockchain
Data Plane
Gateway
Gateway
USERS


SDN Controller
IaaS Cloud
Store the encrypted data in the IaaS cloud
3
Control Plane
Blockchain
1. List of transactions
2. Hash value of the data
3. Hash value of the previous block
4. Timestamp
4
SDN controller creates block for each data
6
Mine evidence from SDN controller and Blockchain
INVESTIGATOR
Data Plane
User authentication
2
USERS
User registration with trusted authority
1
Trusted Authority
5
Investigator get permission from legal authority

IV. RESEARCH NOVELTIES

- All these approaches are deployed flawlessly and can be implemented for real-time application. Since we deployed a distributed architecture, the security level of our system is improved.
- The deployed latest algorithm provides optimal results with the consumption of low computational overheads.
- The investigator can mine the data from the SDN controller and the Blockchain. This information can be very well used for identifying who has made the modifications to the evidence.
- Thus, the reliability of the collected evidence is improved while preserving the privacy of user's data.

V. PREVIOUS WORKS & LIMITATIONS

Paper 1

Title – Distributed SDN Control: Survey, Taxonomy and Challenges

Concept

This paper expands a detailed talk over Software Defined Network and different controllers that are being used in this type of Network. A distributed SDN architecture is comprised of data layer, control layer and application layer. The major challenges are discussed such as scalability, reliability, consistency, interoperability, monitoring and security. The challenges include security and hence it needs to be concentrated in SDN architecture.

Paper 2

Title – P4-to-Blockchain: A Secure Blockchain-Enabled Packet Parser For Software Defined Networking

Concept

In this paper, a new entity called blockchain packet parser (BPP) is used which play the significant role in this paper. It is fed into switches and support for examining the user behaviors and patterns from the received packets. A multivariate correlation analysis approach is proposed to detect the attacks according to the packet traffic. A multivariate approach allows more than two metrics to analyze at once.

Limitations

- Security tests are not properly investigated and when the packet traffic is high, it causes the computational overhead. It is due to the frequent selection of the switch. To avoid the frequent selection of switch, optimum switch selection is required.
- Multivariate correlation analysis uses more assumptions to interpret the data
- Time consumption for hash generation is very high

Paper 3

Title – BEST: Blockchain-based Secure Energy Trading in SDN-enabled Intelligent Transportation System

Concept

In this paper, authors proposed a new architecture called BEST, which is referred as blockchain based secure energy trading approach. This approach is validated for the electric vehicles request. Blockchain is used in this paper to verify the EV's request and it runs in a distributed way. In order to serve as low latency and high data rate for real-time services, SDN is used, which manages the whole network flow.

Limitations

- Conventional blockchain technology does not support for strong data integrity and also it causes computational overhead

Paper 4

Title – - Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q-Learning Approach

Concept

This paper proposes a deep reinforcement learning approach namely dueling deep-Q-learning approach. Nowadays, industry 4.0 is an emergent field in IoT and massive data flows are generated and arrived from the IIoT devices. For monitoring the whole environment, a global technology is invented i.e. SDN. In SDN, centralized or distributed control plane can monitor the network status and avoid the complexity among communications. To enhance the security, blockchain technology is used. Computational resources are allocated to the switches using dueling deep-Q-learning approach.

Limitations

- In this paper, trust features of SDN controller and blockchain is not considered. It is a huge drawback in this paper.

Paper 5

Title – Security enhancement for software defined network using game theoretical approach

Concept

In this paper, the game theory approach is proposed which is used to improve the security of the network. In SDN controller, IDPS component is used, which purpose is to terminate, suspend, active, configure, running and install. The proposed framework addresses the following security attacks including Vampire Attack, Directional Antenna Attack, and Malicious Discovery Attack. It is implemented over the multi-user environment.

Limitations

- Security enhancement using game theory approach does not sufficient to find intrusions

Paper 6

Title – Combined Software-Defined Network (SDN) and Internet of Things (IoT)

Concept

This paper presents a detailed discussion about the combination of Software Defined Network with Internet of Things. Various solutions defined for the issue of security in SDN with IoT is also illustrated. Internet of Things is supported for different types of devices in real time to create intelligent environment.

Paper 7

Title – Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment

Concept

In this paper a forensic architecture is designed for investigating cyber-attacks in cloud environment. A model based on trusted third party (TTP) along with a cloud forensics investigation team (CFIT) is proposed to enhance trustworthiness of the service provider. Each user is authenticated by TTP before access the cloud resources in order to prevent unauthorized user access in cloud environment. Involvement of effectual cloud forensics system supports evidence collection which might help in further legal process.

Paper 8

Title – Trustworthy Electronic Voting Using Adjusted Blockchain Technology

Concept

The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the Blockchain adjustable to meet the need of the polling process. The use of consortium Blockchain is suggested, which ensures that the Blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside. The framework proposed in this paper discusses the

effectiveness of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration by using the adjustable Blockchain method

Limitations

- All the data of the users are stored in the system therefore the attacker can easily get all the information.
- Poor security since the vote can be faked by any user who gets the authentication credentials.

Paper 9

Title – Trustworthy Digital Forensics in the Cloud

Concept

This paper designs a digital forensic model in the cloud environment. Here open cloud forensics (OCF) model and FECloud architecture are proposed to enable effective cloud forensics. The authors also detail the issues involved in cloud forensics. For instance following issues are involved in cloud forensics: dependency on cloud providers, volatile data, multi-tenancy, distributed and heterogeneous infrastructures, and legal issues. To mitigate these issues, the cloud forensic architecture is designed to ensure security as well as integrity for collected evidences.

Paper 10

Title – Blockchains and Smart Contracts for the Internet of Things

Concept

Blockchain and smart contracts are two major entities designed to improve the security for internet of things (IoT). Blockchain allows users to have distributed peer-to-peer network in which each member can verify each transactions held on the network. Blockchain facilitates the

sharing of services and resources leading to the creation of marketplace. Smart contracts are the scripts stored on blockchain and smart contracts are performed based on certain rules.

Paper 11

Title – Towards a practical cloud forensics logging framework

Concept

This paper presents practical log collection architecture to cope with cloud forensics. For logging collection, cloud forensics log framework (CFLOG) is proposed. Initially each log user is authenticated and log is collected from each user with necessary parameters. All collected logs are stored in a hypervisor under the control of cloud service provider (CSP). The logging parameters are adaptive and can be modified by CSP.

Limitations

- The CFLOG is centralized framework in which attacker is able to crack all logs by compromising single entity (i.e.) CSP.
- Integrity of logs is not ensured which increases malicious activities.

Paper 12

Title – MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain

Concept

This paper proposes a smart contracts and an access control mechanism to effectively track the behavior of data. For this purpose, user layer, data query layer, data structuring and provenance layer, existing database infrastructure layer are included in the architecture. Data structuring and provenance layer is involved with different entities such as authenticator, processing and consensus nodes, smart contracts. Smart contract permissioned database, and blockchain network.

Limitations

- This method increases latency with increase in number of users due to large tuple size and processing time.
- Here smart contract mechanism is not efficient due to non-optimal rules.

Paper 13

Title – Blockchain-Based Secure Data Provenance for Cloud Storage

Concept

In this paper, secure data provenance is achieved with the support of blockchain. Data provenance is defined as the record of history of ownership and process of documents or data during its lifecycle. To achieve this, an efficient and secure data provenance scheme (ESP) is proposed in this paper. In ESP, the data provenances are stored in blockchain and all users are authenticated by authentication server. In authentication process, user ID and password generated by AS are considered as authentication credentials.

Limitations

- Security is achieved through timestamp verification. But in blockchain, timestamp of a block is cannot be accurate and subjected to many errors. Thus security provisioning is also not efficient. Authentication is not effectual since user ID and password only considered for authentication.

Paper 14

Title – Block-Secure: Blockchain Based Scheme for Secure P2P Cloud Storage

Concept

This paper proposes a blockchain based distributed architecture for cloud storage in order to improve security and privacy. Initially the data is divided into chunks and encrypted by ECC algorithm then signed by ECDSA algorithm. In order to preserve integrity in merkle tree, (SHA-

256)^2 algorithm is adapted. Then genetic algorithm is applied to minimize redundant data presented in blockchain network.

Limitations

- ECDSA based digital signature involves with problems such as prime number generation is not efficient which decreases security level
- However, SHA-256 is less secure and increase time consumption for hash generation. Thus applying SHA-256 for two times increases time consumption rapidly.

Paper 15

Title – Adaptive Evidence Collection in the Cloud Using Attack Scenarios

Concept

This paper presents an adaptive evidence collection mechanism in order to handle dynamic configuration of cloud architecture. To make evidence collection as adaptive, three different scenarios such as vulnerable database, security breaches, and cloud configuration are considered. Based on these configurations, evidence collection process is adaptively updated.

Limitations

- Perhaps this method is adaptive; this method is not able to provide data provenance and evidence integrity

BIBLIOGRAPHY

Santra, P., Roy, P., Hazra, D., & Mahata, P. (2018). Fuzzy Data Mining-Based Framework for Forensic Analysis and Evidence Generation in Cloud Environment. Ambient Communications and Computer Systems, 119–129.

Irfan, M., Abbas, H., Sun, Y., Sajid, A., & Pasha, M. (2016). A framework for cloud forensics evidence collection and analysis using security information and event management. Security and Communication Networks, 9(16), 3790–3807.

M. Pourvahab and G. Ekbatanifard, "An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology," IEEE Access, vol. 7, pp. 99573–99588, 2019.

Y. Zhang, X. Lin, and C. Xu, "Blockchain -Based Secure Data Provenance for Cloud Storage," vol. 7618, no. 2017, T. W. Chim and T. H. Yuen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, pp. 3–19.

Kotaro Kataoka, Saurabh Gangwar, Prashanth Podili, "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN", IEEE 4th World Forum on Internet of Things, 2018.

Fetia Bannour, Sami Souihi, Abdelhamid Mellouk, "Distributed SDN Control: Survey, Taxonomy and Challenges", IEEE Communications Surveys & Tutorials, vol 20, no 1, pp 333 – 354, 2018.

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Choo, K.-K. R. (2020). P4-to-Blockchain: A Secure Blockchain-enabled Packet Parser for Software Defined Networking. Computers & Security, 88, 101629.

Chaudhary, R., Jindal, A., Aujla, G. S., Aggarwal, S., Kumar, N., & Choo, K.-K. R. (2019). BEST: Blockchain-based Secure Energy Trading in SDN-enabled Intelligent Transportation System. Computers & Security. 85, 288-299

Qiu, C., Yu, F. R., Yao, H., Jiang, C., Xu, F., & Zhao, C. (2019). Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep Q-Learning Approach. IEEE Internet of Things Journal, 6(3), 4627-4639

Anithaashri, T. P., Ravichandran, G., & Baskaran, R. (2019). Security enhancement for software defined network using game theoretical approach. Computer Networks, 157, 112–121.

Muneer Bani Yassein, Shadi Aljawarneh, Mohammad Al-Rousan, Wail Mardini, Wesam Al-Rashdan, "Combined software-defined network (SDN) and Internet of Things (IoT)",

International Conference on Electrical and Computing Technologies and Applications, 2017.

Manoj, S. K. A., & Bhaskari, D. L. (2016). Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. Procedia Computer Science, 85, 149–154.

B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," IEEE Access, vol. 7, pp. 24477–24488, 2019.

Zawoad, S., & Hasan, R. (2016). Trustworthy Digital Forensics in the Cloud. Computer, 49(3), 78–81

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

Pichan, A., Lazarescu, M., & Soh, S. T. (2018). Towards a practical cloud forensics logging framework. Journal of Information Security and Applications, 42, 18–28.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access, 5, 14757–14767.

Zhang, Y., Lin, X., & Xu, C. (2018). Blockchain-Based Secure Data Provenance for Cloud Storage. Lecture Notes in Computer Science, 3–19.

Li, J., Wu, J., & Chen, L. (2018). Block-secure: Blockchain based scheme for secure P2P cloud storage. Information Sciences, 465, 219–231

Pasquale, L., Hanvey, S., Mcgloin, M., & Nuseibeh, B. (2016). Adaptive evidence collection in the cloud using attack scenarios. Computers & Security, 59, 236–254.