Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm

Article *in* Materials Today: Proceedings · November 2020

DOI: 10.1016/j.matpr.2020.08.519

CITATIONS
15

READS
1,676

4 authors, including:

Velmurugadass Pandiaraj
Kalasalingam University
4 PUBLICATIONS **15** CITATIONS

SEE PROFILE

Dhanasekaran Subbiah
Kalasalingam University
34 PUBLICATIONS **43** CITATIONS

SEE PROFILE

Vinod Vasudevan
University of Bradford
50 PUBLICATIONS **75** CITATIONS

SEE PROFILE

Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm

P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand *, V. Vasudevan

Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu 626 126, India

ARTICLE INFO

Article history:
Received 11 August 2020
Accepted 18 August 2020
Available online xxxx

Keywords:
Blockchain
Internet of Things – IoT
Cloud computing
Cryptographic security
Software-Defined Networking – SDN

ABSTRACT

Blockchain is one of the fast growing technologies that has significant role in the area of criminal investigation. The security is becoming a great threat to all the industries, Electronic Health Record (EHR), Banking, Smart Applications (SA), Supply Chain Management (SCM) and IoT environment in recent years. In this research, we have developed a novel framework that will monitor the activities that takes place on particular data evidence, We create a Cloud based Software Defined Network (SDN), its consists of 100 - mobile Nodes (IOT devices), open flow switch and Blockchain based controllers, cloud server, Authentication Server (AS) and investigator. Initially all users are registered with AS and obtain their secret key from AS based on the Harmony Search Optimization (HSO). In the mobile nodes the packets are encrypted by using Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm and transfer to the cloud server. SDN controller maintains blockchain to preserve evidences collected from data and signature of the users based on the SHA-256 Cryptographic Hash Algorithm. Authorized investigator performs following processes: identification, evidence collection, evidence analysis, and report generation based on the Logical Graph of Evidences (LGoE). we plot the resultant graph for Response time versus Number of users, Evidence insertion time versus number of users, Evidence verification time versus Number of users, Computational overhead versus number of users, Total change rate versus Number of users, Hash computation time versus number of users, Key generation time versus number of users, Encryption time versus number of users and Decryption time versus number of users. Finally, the investigator or other legal people can obtain the evidences from the controller and construct as a Logical Graph of Evidence (LGoE). The experimental analysis revealed the fact that the proposed system obtained better performance in terms of response time, accuracy, increasing throughput and total change security parameters.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Newer Trends and Innovation in Mechanical Engineering: Materials Science.

1. Introduction

In today's world, everything around us is connected with the Internet of things (IoT) 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 on-demand computing resources for the IoT users. 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 [1]. 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 implementa-

* Corresponding author.
E-mail addresses: dass.spv@gmail.com (P. Velmurugadass), shasi.sridharan@aiht.ac.in (V. Vasudevan).

https://doi.org/10.1016/j.matpr.2020.08.519
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the International Conference on Newer Trends and Innovation in Mechanical Engineering: Materials Science.

tion of SDN, The packets that arrive at the network switch will follow the rules built into the switch's proprietary firmware [8]. These rules are transferred to the switch from the centralized controller. Some of the unique features of SDN are listed in Fig. 1.

In some cases, the switches present in the SDN environment will issue a route request to a controller for a packet that does not have a specific route. This is termed as dynamic mode of operation in SDN. This is not adaptive routing in which the switches issue route request through the routers and routing algorithms based on network topology rather than through the controller [8]. SDN has a major impact on the management of IT infrastructure and network design. SDN makes network control programmable, often using open protocols, such as OpenFlow [3]. Because of this, enterprises can apply globally aware software control at the edges of their networks to access network switches and routers rather than the closed and proprietary firmware generally used to configure, manage, secure and optimize network resources.

1.1. Dynamic routing prioritization

It is based on the real time digital data network processing feedback and this new networking structural design uses in dynamic routing tables of helps in priority option routing, Based on the real-time network feedback, this new networking architecture uses dynamic routing tables for that helps in prioritizing routing, calculating and managing the SDN Machines. it is managed the traffic to various IP addresses and devices.

1.2. Edge cloud to deploy CORD to transform their networks

The edge CORD (Central Office Re-architected as a Datacenter) is innovative next-generation services and SDN for the network edge. Integrating multiple environment and software's projects though middleware technology, CORD delivers a content based environment and managed on flexible infrastructure through agile DevOps processes then continuous delivery workflows to create innovative services. CORD provides a complete integrated middleware platform.

1.3. Supports cloud-based traffic

Cloud is one of the biggest centralized storage trends of information and computing architecture. The cloud computing basically storage and managing the pool of storage in correlation with on-demand services. It is easy for SDN to dynamically deliver the on demand available services such as Infrastructure as a Service (IaaS), Platform as Services (PaaS) and Software as Services (SaaS) are provide within the data center [9].

1.4. High throughput for big data

Now a day's all the industries, Social Medias, Research Sectors and Electronic Health Record (EHR), ERP and IoT users are managing huge amount of digital data that time require centralized storage and parallel processing, but this time needed more bandwidth also, SDN makes it possible by quick access time, connectivity and throughput [1].

Fig. 1. Features of SDN.

1.5. Manages security and policies

Security is more concern policies over the internetworking architecture and other elements. SDN help to more possible high secure and ring authentication in present cloud and IoT environment.

2. Blockchain technology

The Blockchain technology is one of the fast spreading security cryptographic mechanisms to provide decentralized approaches that replaced many existing security implementations. As the name indicates, this field consists of chain of blocks with each containing certain information and more formally appears as a distributed ledger. It is a software protocol that could not be executed without internet and comprises of several components like a database, software application and some connected computers [2]. The information in each blocks are hashed and stored to enhance the level of security being offered.

Fig. 2 represent technology is an online distributed system which can store information and it is based on interconnected blocks which are open to everyone like it is clear from it is name blockchain is the chain of connected blocks [1]. which can store information there are three things on every block first data which is the information we store on block and that depends upon the type of blockchain for example crypto currencies they store information about the sender the receiver and transaction the second thing every block contains is the hash of that block and that hash is the fingerprint of block it is always unique and we use that hash to identify that block and last thing every block contains is the hash of previous block which connects the current block with remaining blockchain and that is the property which makes this technology so secure there is also another property which makes this technology more secure and peer-to-peer nature of work like instead of having a central authority which normal banks have a central authority which contains all the information about every other block and they manage blocks blockchain [6].

Smart contracts are just like contacts in real word. In fact a smart contract is actually a ting computer program that is stored inside a blockchain [2]. Smart contract processes are completely digital process and has everything is completely distributed [1]. Smart Contract are stored on a blockchain, they inherit some interesting properties. They are immutable and it is distributed. Immutable means that once a smart contract is created after that it cannot be changed anything in a block and hash values again [2]. So that no one can go behind blockchain, it has been authenticated and eliminates the legal uncertainties data access with transaction concluding a contracts is processed on the blockchain [10].

In this Fig. 3 represent some of the security challenges will be occurred. First thing unauthorized access to SDN controller so that some of the information stolen from SDN network, second thing Man-in-Middle attack between switch and controller in this reason all the source data will be modified, stolen then resource stealing also will be happened. Finally vSwitch also will be attack through unauthorized access over the SDN using blockchain technology [9]. The blockchain technology has been generally used as a secu-

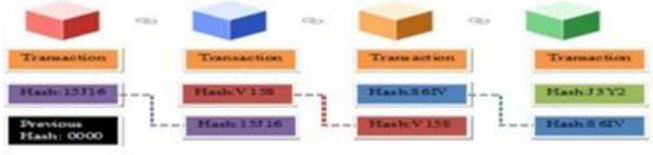

Fig. 2. Process structure of the Blockchain technology.

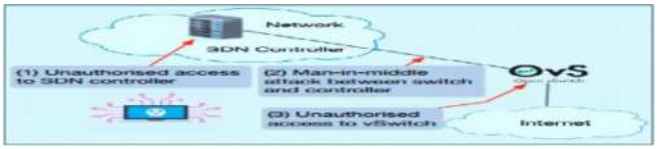

Fig. 3. SDN controller with Open-Flow Switches without using blockchain (Source: Lukman Adewale Ajao et al.,).

rity aspect to side of Internet of Things (IoT) and software-defined network (SDN) securities challenges with cyber attacks [1,2].

2.1. Advantages of Blockchain technology

- Faster transactions.
- Blockchain note within peer-to-peer connection.
- Proof-of- work will be generated based on the algorithm.
- No payment for intermediaries Services.
- High level of security based on the data validity & security.
- Automatic reconciliation of accounts.
- Different levels of accessibility.
- Hacking threat reduced.
- Transparency of transactions increased.

3. Proposed system

In this research work, Fig. 4 represents and developed Blockchain architecture for evidence collection and provenance in cloud storage and SDN [9]. Initially, the user will register to the trusted authority and receive the key for data encryption using HSO. The user will then authenticate using user id, password and random number. The authenticated user can then upload their encrypted data to the cloud. For the purpose of encryption, we implement Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm and also the data is encrypted twice for sensitive data and only once for the non-sensitive data. Then, the encrypted data is stored in the cloud through the switches. The SDN controller will create a block for each data that is uploaded by the user [8]. The block contains list of transactions, the hash value of data and previous block along with a time stamp value. Any modification performed on these data can be traced using the smart contract. If any access has been made, a report is generated and provided to the user. In the end, the investigator can collect the evidences and the various modifications performed on those evidences from the controller and the Blockchain and construct as a LGoE [9]. The experimental evaluation reveals that the proposed approach has obtained better performance with response time and total change rate. Thus, our proposed system has overcome all the major drawbacks of the existing systems as.

- Centralized evidence collection leads to poor security.
- Poor data integrity and evidence reliability.

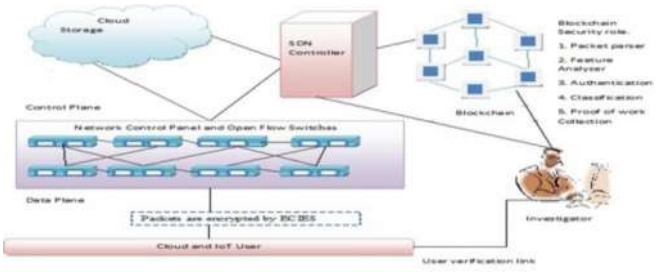

Fig. 4. Blockchain technologies in Cloud, SDN and at the IoT users.

- Weak authentication with poor accuracy.

3.1. Advantages of our proposed system

- Reduced computational overhead.
- Reduced Key generation time and encryption and decryption time.
- Strong authentication with accurate verification of evidence's reliability.

4. Modules

- User Registration and Authentication.
- Data Encryption and Storage.
- Evidence Collection in Blockchain.
- Mining of Evidence Information.

4.1. Module description

4.1.1. User registration and authentication

In our proposed system, the user will initially perform the registration process with the legal authority. The HSO 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 and a random number to the authentication verification purpose. If the verification is successful, the user is granted authentication, otherwise the access is rejected.

4.1.2. 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 [1]. For the purpose of encryption, we have implemented ECIES algorithm. This encrypted data is uploaded into the cloud. The encrypted data from the user is stored into the cloud through the switches [2].

4.1.3. 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 [3]. 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 SHA-256 algorithm. The main idea behind the Blockchain implementation is to capture the actions performed on the data while ensuring the security of the data [7].

For the purpose of tracking the access of data on the cloud, we implemented Fuzzy 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.

4.1.4. 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 LGoE. Thus, our system guaranteed to provide security and also tracing back the user who is suspect [7]. The performance evaluation also showed the worth of the proposed system.

5. Proposed architecture

It is observed that hash technology is an excellent mechanism to prevent the security risks of data leakage. The specialty of hash function is that even if the attacker enters into the block, they cannot get hold of the data as calculation of hashes is a tedious task. Also, block chain makes use of the concept of Proof-of-Work. It is a mechanism which slows down the creation of the new blocks. A proof-of-work is a computational problem that takes certain to effort to solve. But the time required to verify the results of the computational problem is very less compared to the effort it takes to solve the computational problem itself [1].

6. Dataflow diagram

The below Fig. 5: Represent a dataflow diagram for proposed architecture on Blockchain technologies in Cloud, SDN and at the IoT users. Initially start the process of user registration after that user data, for the purpose of encryption and we have implemented ECIES algorithm. SDN controller maintains blockchain to preserve evidences collected from data and signature of the users based on the SHA-256 Cryptographic Hash Algorithm. Authorized investigator performs following processes: identification, evidence collection, evidence analysis, and report generation based on the Logical Graph of Evidences (LGoE). After getting permission, the investigator will mine the data from the SDN controller and the Blockchain, and then the investigator constructs the LGoE. This encrypted data is uploaded into the cloud. The encrypted data from the user is stored into the cloud through the switches [2].

7. SHA-256 Cryptographic hash algorithm

In this Fig. 6, represent as a SHA-256 Cryptographic Hash Algorithm associated with the blockchain technology and this algorithm creates hashes for secure access, mainly used for verifying data and message integrity during transaction, session time, data identification then password verification. Blockchain technology is a combination of blocks and hash pointers can be used to build a linked list, which is also called blockchain architecture [4]. Each

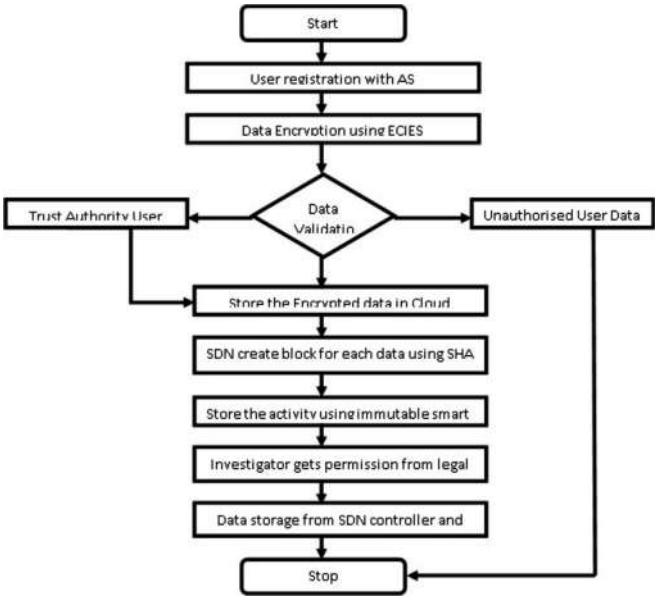

Fig. 5. Dataflow diagram for proposed architecture on Blockchain technologies in Cloud, SDN and at the IoT users.

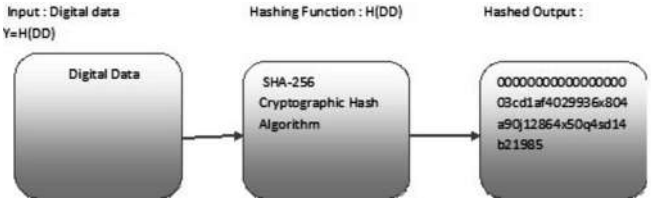

Fig. 6. The Hashing algorithm generates a "hash" of the input text and output values.

block has a data and a unique hash value of the previous block then except for original block that is contains no previous hashing [7]. Authorized investigator performs following processes: identification, evidence collection, evidence analysis, and report generation based on the Logical Graph of evidence (LGoE) [8,9]. Initially all users are registered with AS and obtain their secret key from AS based on the Harmony Search Optimization (HSO).

7.1. Algorithm execution (SHA-256 Cryptographic Hash)

Step 1:
Digital Data: input up to 100 nodes IoT device
. . . . . So that
Legth of Plain Text is 128 < multiple and 1024 bits.
Step 2:
Append 128 bit Representation of original plain text
Such that length = Multiple and 1024 bit
Step 3:
Initialize the Buffers (a, s, d, f, g, h, k, l) 64 bit.
Step 4:
Process each block and plain text in 100 steps.
Step 5:
Output in buffer is Hash Code (SHA-256 Cryptographic Hash)
Plain Text Block Size = 1024 bits;
No. of steps = 100;
Each steps -> QWORD = 64 bit [Generated from plain text]
Each steps -> Constant F;
Store intermediate results -> Buffer;
Each buffer size = 64 bit
Store output (hash code).

We create a Cloud based Software defined network (SDN), it is consists of 100 - mobile Nodes [IOT devices], open flow switch and Blockchain based controllers, cloud server, authentication server (AS) and investigator. The user has user_id, public key, resource id, URL address and digital signature. Digital signature was used in Hash Block and used for authenticate the user and lastly with verification id sent from a smart contract [9]. Hash Block and used for authenticate the user and lastly with verification id sent from a smart contract.

8. Create a Blockchain hash value, data, timestamp and nonce

The above Fig. 7 represents a hash value generation and bockchain creation. Initially hash value is generated as 0000000000000000003cd1af4029936x 804a90j12864x50q4sd624c9df block mined and block mined means add a new block of transactions to the blockchain that time particular blocks has stored block creation timestamp, nonce and block of the data with previous hash values. The block chain generates and hash value, previous hash, time stamp and nonce [5].

Fig. 7. Blockchain hash value, data, timestamp and nonce generated output.

Table 1
Represent blockchain properties.

Blockchain properties	Implication
Previous block hash	To the reference of the previous block for the hash value.
Merkle Root	A representative hash of all transactions included in the block.
Timestamp	The time at which the block was created
Target	Proof-of-work algorithm for a transaction states of the block.
Nonce	The variable used in the proof-of-work progression

Table 1: Represent a Blockchain characterize and it is properties, previous block hash is indicate the value of the hash number example #1296. Merket Root is representative a hash of all transactions and created one of the block including time stamp, hash value, nonce. Such as timestamp is refer to the time at which the block was created. Target is PoW (Prof-of-Work) algorithm for used a transaction states of the block [5]. Nonce is mention at the variable used in the algorithm process.

9. The Elliptic Curve Integrated encryption Scheme (ECIES) algorithm

In the mobile nodes the packets are encrypted by using the Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm and transfer to the cloud server. SDN controller maintains blockchain to preserve evidences collected from data and signature of the users based on the Secure Hash [8]. ECIES is public-key mechanisms that provide authenticated encryption, digital signature and key exchange scheme and symmetric encryption key. It is join an Elliptic Curve Cryptosystem based an asymmetric cryptography with symmetric ciphers to provide data encryption based on Elliptic Curve private key and decryption by the corresponding EC public key. Public-key schemes are difficult implementation and design but that is very useful and must be secure and efficient method for data exchange. Elliptic Curve (EC) is smaller key size so that secure authentication, key generation, key exchange methods and less bandwidth for keys transmitting and over a network through cloud server [9].

The Elliptic Curve Integrated Encryption Scheme (ECIES) select a curve was often used when want to be need our key exchange also do it sign without something but our public key with private key and then proof with our public key but we can also use the method to be able to encrypt data. this is a some of the basics around elliptic curve encryption what we have is a point an elliptic curve G, we create our private key a random number this is a private key, this is a random number is the gradient of the line that will be from G, until we find our public key which is an x-y point [9]. On the curve here we have an X and we have a wide but a private key is just a scalar about you so the question that we have is that the public key we will call it Q is equal to the private key times G.

$$Q = P \cdot g \tag{1}$$

This is really difficult if you use large private prime Y large integer to find the value of P in oval we have the value of Q and G. Elliptic curve cryptography equation given as

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

in this equation represent on the curve and values, x and y is point of the curve value then a and b values represent the value of the points that define the curve. so this is how elliptic key encryption works we have certain standard that we use that are seen to be safe so the way that Integrated Encryption Scheme (IES) works is that we generate a symmetric key form the public key of the person that were sending the data to so differs from our key exchange method where the same key would be generated to the order side.

Blockchain implementation to be used Elliptic curve (EC) to generate public key pairs. Elliptic curve cryptography (ECC) is a 256 bit and provides public keys and more comparable security to a 3072 bit RSA algorithm. The elliptic curve uses smaller key sizes with respect to RSA providing comparable security. The main advantages of using EC based cryptography security is reduced key size with is processing speed is very high.

ECIES algorithm key generation method Sender generates a random private key (RP_AP_A) and the takes a point on an elliptic curve (G) and then determines sender public key (PK_A):

$$PK_A = RP_A \times G \text{ and } PK_A = P_A \times G \tag{3}$$

G and PKA are thus points on an elliptic curve. Sender then sends PKA to receiver. Next receiver will generate: $R = r \times G$, $S = r \times PK_A$ and where r is a random number generated by receiver. The symmetric key (S) is then used to encrypt a message. Sender will then receive the encrypted message along with R and sender will be able to determine the same encryption key with:

$$S = RP_A \times R \tag{4}$$

This is the same as the key that receiver also generated secret key consists of 100 - mobile nodes of the Internet of things (IOT devices).

$$S = RP_A \times (r \times G) \tag{5}$$

$$S = r \times (RP_A \times G) \tag{6}$$

$$S = r \times PK_A \tag{7}$$

In the Table 2 represent security properties, SDN, Blockchain and cloud storage. SDN based blockchain is more secure gateway process for following advantages Digital signature, OFS supports

Table 2
Represent security properties for blockchain based Cloud and SDN.

Security Properties	SDN with Blockchain	Cloud Storage
Authentication and Id	Digital Signatures	Hash value along with proof of work
Access mechanism	OFS - support multiple transaction	Verified link with previous hash value between all the blocks
Protocol stack and network security	ECIES based encryption	ECIES based encryption with SHA – 256 hash value.
Privacy method	PK_A or ID	Transaction ID along with hash value.
Non – Reputation	Signature	Proof of Work created.

Fig. 8. Key generation based on Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm.

Fig. 9. Identification, evidence collection, evidence analysis, and report generation based on the Logical Graph of Evidences (LGoE).

multiple transaction, ECIES based encryption, key generation and proof of work signature. Furthermore cloud and blockchain are given more secure process of hash value, verified link with previous hash value between all the blocks, protocol stack, transaction id creation and PoW (Proof of Work).

10. ECIES key generation

In the Fig. 8, represent a ECIES is public-key mechanisms that provide authenticated encryption, digital signature and key exchange scheme and symmetric encryption key. It is join an Elliptic Curve Cryptosystem based an asymmetric cryptography with symmetric ciphers to provide data encryption based on Elliptic Curve private key and decryption by the corresponding EC public key. Public-key schemes are difficult implementation and design but that is very useful and must be secure and efficient method for data exchange. Elliptic Curve (EC) is smaller key size so that secure authentication, key generation, key exchange methods and less bandwidth for keys transmitting and over a network through cloud server. The Elliptic Curve Integrated Encryption Scheme (ECIES) select a curve was often used when want to be need our key exchange also do it sign without something but our public key with private key and then proof with our public key but we can also use the method to be able to encrypt data.

11. Report generation based on the LGoE

In the Fig. 9: An identification, evidence collection, evidence analysis, and report generation based on the Logical Graph of Evidences (LGoE) is create a Cloud based Software defined network (SDN), its consists of 100 – mobile Nodes [IOT devices], openflow switch and Blockchain based controllers, cloud server, authentication server (AS) and investigator. In the mobile nodes the packets are encrypted by using the Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm and transfer to the cloud server. SDN controller maintains blockchain to preserve evidences collected from data and signature of the users based on the Secure Hash Algorithm (SHA-256).

12. Experimental analysis reports

In this Fig. 10, represent as a Plot the graph for Decryption time versus Number of users, Plot the graph for Encryption time versus

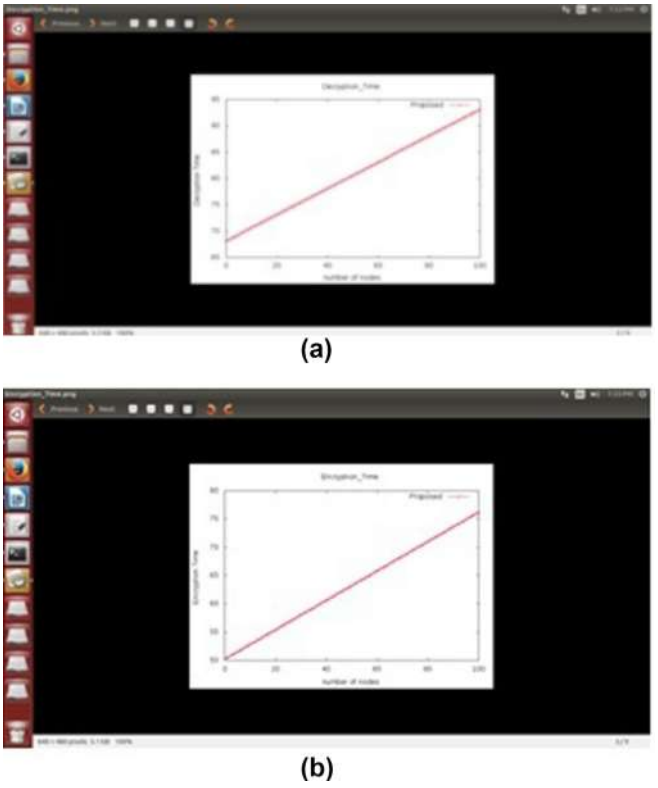

Fig. 10. Plot the graph for Decryption time versus number of user, Plot the graph for Encryption time versus number of users.

Number of users, Plot the graph for Evidence insertion time versus Number of users, Plot the graph for Evidence verification time versus Number of users, Plot the graph for Hash computation time versus Number of users, Plot the graph for Key generation time versus Number of users, Plot the graph for Response time versus. Plot the resultant graph for Response time versus Number of users, Evidence insertion time versus number of users, Evidence verification time versus Number of users, Computational overhead versus number of users, Total change rate versus Number of users, Hash computation time versus number of users, Key generation time versus number of users, Encryption time versus number of users and Decryption time versus number of users. The investigator or other legal people can obtain the evidences from the controller and construct as a Logical Graph of Evidence (LGoE). The experimental analysis revealed the fact that the proposed system obtained better performance in terms of response time, accuracy, increasing throughput and total change security parameters.

13. Conclusion

In this project, we have constructed a blockchain architecture that is used for evidence collection and provenance preservation in IaaS cloud. The proposed system consists of user registration, authentication, data encryption, storage of data, tracing the user activity and mining the data from the controller. 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. We deployed latest algorithm that 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. The experimental observation revealed that the proposed system has obtained better performance in terms of response time and total change rate.

14. Future work

In future, we will extend our system to process the collected evidence and come up with some useful information. In blockchain, the data collected has significant value and SDN controller suffers from several attacks like DoS, DDoS and so on. Thus, we have planned to use novel approach to mitigate those security threats without increasing the computational overheads of the system. Also, we will attempt to provide lightweight hash algorithms to ensure the durability of the proposed system.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Pourvahab, G. Ekbatanifard, An efficient forensics architecture in software-defined networking-IoT using blockchain technology, IEEE Access. 7 (2019) 99573–99588.
[2] W. Yang, E. Aghasian, S. Garg, A survey on blockchain -based internet service architecture: requirements, challenges, trends, and future, IEEE Access. 7 (2019) 75845–75872.
[3] Z.A.E. Houda, A.S. Hafid, L. Khoukhi, Cochain-SC: an intra- and inter-domain ddos mitigation scheme based on blockchain using SDN and smart contract, IEEE Access. 7 (2019) 98893–98907.
[4] B. Shahzad, J. Crowcroft, Trustworthy electronic voting using adjusted blockchain technology, IEEE Access. 7 (2019) 24477–24488.
[5] B. Zhao, P. Fan, M. Ni, Mchain: a blockchain-based VM measurements secure storage approach in IaaS cloud with enhanced integrity and controllability, IEEE Access. 6 (2018) 43758–43769.
[6] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, Y. Tang, An ID-based linearly homomorphic signature scheme and its application in blockchain, IEEE Access. 6 (X) (2018) 20632–20640.
[7] L.A. Ajao, J. Agajo, E.A. Adedokun, L. Karngong, Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry. MDBI Access, 2, 300–325. A Privacy-Preserving Signature.
[8] F. Bannour, S. Souihi, A. Mellouk, Distributed SDN control: survey, taxonomy, and challenges, IEEE Commun. Surveys Tuts. 20 (1) (2018) 333–354.
[9] M. Pourvahab, G. Ekbatanifard, Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology, IEEE Access. 7 (2019) 153349–153364.
[10] N.M. Kumara, P.K. Mallickb, Blockchain technology for security issues and challenges in IoT, Procedia Comp. Sci. 132 (2018) 1815–1823.

Further Reading

[1] K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, Blockchain-based soybean traceability in agricultural supply chain, IEEE Access. 7 (2019) 73295–73305.
[2] J. Al-Jaroodi, N. Mohamed, Blockchain in industries: a survey, IEEE Access. 7 (2019) 36500–36515.
[3] Z. Zhou, B. Wang, M. Dong, 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. 50 (1) (2019) 1–15.
[4] P.K. Sharma, M.Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access. 6 (2018) 115–124.
[5] Y. Zhang, X. Lin, C. Xu, Blockchain-based secure data provenance for cloud storage, in: D. Naccache et al. (Eds.), Information and Communications Security. ICICS 2018. Lecture Notes in Computer Science, Vol. 11149, 2018, pp. 3–19. Springer, Cham.
[6] J. Li, J. Wu, L. Chen, Block-secure: blockchain based scheme for secure P2P cloud storage, Inf. Sci. (Ny) 465 (2018) 219–231.
[7] T. Zhang, Z.W. Geem, Review of harmony search with respect to algorithm structure, Swarm Evol. Comput. 48 (2019) 31–43.
[8] M.K. Pandya, S. Homayoun, A. Dehghantanha, Forensics investigation of openflow-based SDN platforms, Adv. Inform. Security 70 (2018) 281–296.
[9] Y. Xie, D. Feng, X. Liao, L. Qin, Efficient monitoring and forensic analysis via accurate network-attached provenance collection with minimal storage overhead, Digit. Investig. 26 (2018) 19–28.
[10] J. Yi, X. Li, C.H. Chu, L. Gao, Parallel chaotic local search enhanced harmony search algorithm for engineering design optimization, J. Intell. Manuf. 30 (1) (2019) 405–428.
[11] B.K. Zheng et al., Scalable and privacy-preserving data sharing based on blockchain, J. Comput. Sci. Technol. 33 (3) (2018) 557–567.
[12] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles, IEEE Commun. Mag. 56 (10) (2018) 50–57.
[13] P. Dubey, V. Tiwari, S. Chawla, V. Chauhan, Authentication framework for cloud machine deletion, Lect. Notes Netw. Syst. 10 (2018) 199–206.
[14] J. Ricci, I. Baggili, F. Breitinger, Blockchain-based distributed cloud storage digital forensics: where's the beef?, IEEE Secur Priv. 17 (1) (2019) 34–42.