Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

UNIVERSAL WISER PUBLISHER

Research Article

Fog-Driven Approach for Distributed Intrusion Detection System in Auditing the Data Dased on Blockchain-Cloud Systems

Hanumantharaju R[1*], Shreenath KN[1], Sowmya BJ[2], Srinivasa KG[3]

[1]Siddaganga Institute of Technology, Tumkur, Affiliated to Visvesvaraya Technological University, Belagavi, India
[2]M S Ramaiah Institute of Technology, Affiliated to Visvesvaraya Technological University, Belagavi, India
[3]International Institute of Information Technology, Naya Raipur, Chhattisgarh, India
Email: rajurjs@gmail.com

Received: 13 October 2023; **Revised:** 26 October 2023; **Accepted:** 27 October 2023

Abstract: Intrusion detection is a familiar phrase in the information and network security domain. An Intrusion Detection System (IDS) is a device or software that will keep track of the networks, for unlawful movements, and policy breaches that arise within the network. There are different forms of IDS, Host Intrusion Detection System (HIDS) helps in identifying unauthorized activities on the host, Network Intrusion Detection System (NIDS) helps in identifying attacks in the network, whereas Distributed Intrusion Detection System (DIDS) consists of multiple IDS over a large area of network where individual IDS communicates with each other or with the central the authorized central server. The proposed work has a three-layered architecture for DIDS for securing data sharing among different IDS. The bottom layer uses multiple IDS, the fog layer is supported with Blockchain functionality, and the cloud service at the upper layer stores required data permanently for future analysis. The fog computing-based architecture for DIDS tries to implement the application in a scalable and trustless environment using distributed ledger technology. The evaluation of the proposed work is carried out for fog, cloud, and integrated fog-cloud with the Blockchain functionality and without Blockchain functionality in measuring performance metrics related to throughput, service latency, response time, block creation time, and block execution time.

***Keywords*:** blockchain, distributed systems, fog computing, intrusion detection system

1. Introduction

An intrusion detection system plays a major role in securing IT infrastructure by capturing and analyzing the network traffic [1]. Currently, the available intrusion detection approaches fall into two major categories (A) Signature-based detection and (B) Anomaly-based detection. Signature-based detection systems identify intrusion by looking for specific patterns, such as byte sequences in the network traffic and these directives are compared with the network traffic to identify the attack. This method is very effective and efficient in detecting the known types of attacks and they have a very low false alarm rate. However signature-based detection system requires updating of signature and protocols often and they are impotent to recognize any unknown or novel attacks. In anomaly anomaly-based intrusion detection system, the traffic or host operating system behavior is observed based on numerous parameters and they are compared with the normal behavior. If the intrusion detection system identifies any diversion from the normal behavior, then the alert will be raised [2].

DOI: https://doi.org/10.37256/ccds.5120243772

IDS is a device or an application that is used to monitor the network traffic and alert the network administrator when there is an attempt for unauthorized access. The different IDS will share the logs and alerts generated with each other when deployed across a large network; such an orchestration of several IDS is called a Distributed Intrusion Detection System (DIDS). A DIDS will observe the target environment to monitor multiple hosts that are connected via the network as well as the network itself [3]. The type and amount of generated information exchanged between the distributed systems is configured and fine-tuned whenever it is required. It facilitates the advanced persistent threat analysis, network supervision, and quick attack analysis of the entire network which helps the administrator to get a broader view of the network attack [4].

The data sharing and thrust management among the various IDS will be the big challenge in distributed intrusion detection systems. Also presently the attack pattern on the network is unpredictable, and more complicated where data can be tampered with anytime, and in a large network, one of the networks may compromise with the attacker. Blockchain technology provides a potential solution to these challenges. Blockchain is a continuously growing list of records; blockchain provides a distributed and trustless environment to store the records in an encrypted form. The data from each IDS are considered as blocks, each block is linked to the previous block using the cryptographic hash, and the blockchain is used to manage the peer-to-peer network.

The data in the blockchain are transparent and they cannot be tampered with (any small modification of the blocks will result in the changing the hash function of the block, since all the blocks in the blockchain are linked it can be traced easily as they cannot be changed without the alteration of all subsequent blocks) and they are immutable. In DIDS privacy, integration, and a common consensus among all the participating intrusion detection system is necessary [5] as DIDS is vulnerable to attack within the network where the attacker may get access while transferring the data for storage.

Fog computing reduces the latency processes the data locally and also provides scalability. In the DIDS system, fog computing enhances scalability and helps to process the data locally when the intrusion detection system performs over a large geographical area. All the data from IDS are transferred to the fog nodes in the fog layer and are later uploaded to the cloud for an overview of the entire system and permanent storage.

The proposed work aims to address defining a fog-enabled distributed intrusion detection system:

• Identifying the selective forwarding attack in the network using the I-Watchdog mechanism.

• Also, designing a secured alert system in the fog layer supporting the use of distributed ledger technology and lastly comparing and contrasting the results obtained with various experimental setups.

• The distributed intrusion detection systems give the administrator the easiest and fastest ways to identify the intrusions coordinated across multiple networks in a large geographical area.

• There are chances of data tampering when multiple networks are involved in the system, and there may be scalable problems when multiple IDS are involved.

• In this work, a distributed intrusion detection system is implemented along with blockchain and fog computing to provide security and scalability respectively.

• The main focus of this work is to identify the Network Intrusion Detection System (NIDS) in the network using two different intrusion detection systems.

• The blocks are generated and linked using the previous hash of the block. The fog nodes receive the data from the intrusion detection system and are processed and updated to the cloud.

The rest of the paper is organized as follows. Section 2 highlights key elements of existing frameworks and compares them with the proposed framework. In Section 3, a description of the DIDS framework is provided. The implementation of DIDS is discussed in Section 4. Section 5 concludes the paper by proposing future works to improve DIDS.

2. Related works

In [6] designed a fog computing and blockchain architecture for scalable control of IOT devices. The proposed architecture addressed a case study for water dam control where every fog node is furnished with blockchain to guarantee data veracity with the help of a smart contract. Using a proof-based concept testbed [7] the performance of

the architecture is evaluated.

The authors in this paper [8] discuss the various advantages of fog computing over the cloud such as scalability, low latency, and low energy consumption. The authors present an architecture for smart cities using Blockchain and Fog based Architecture Network (BFAN). The data are secured and authenticated using blockchain. The simulation results are shown by authors who prove that fog computing technology consumes less energy and reduces network latency. In the future, the authors plan to use this architecture in many areas such as video chatting in the various areas of smart cities and 5G/6G for online games streaming applications.

The authors in the paper [9] proposed a distributed charging system based on IOT for the sustainable operation of electrical vehicles (EV). Here fog computing is also used to provide localized service. The Blockchain technology is deployed for distributed fog computing nodes, to provide a decentralized and secured storage environment. The authors provide a threat model and proof of the online duration of this work.

In [10] proposed an intrusion detection system using blockchain analysis for bitcoin exchange models. In this work, authors described various intrusion detection models in bitcoin exchanges and also presented identification and minimization of intrusion using blockchain technology for analysis of every technique. This work is proposed assuming that every rented hash rate will be away from main the network module.

In the paper [11] authors discussed various approaches in which intrusion detection systems and blockchain technologies are integrated, to overcome the various challenges that occur in the hybrid intrusion detection system. The authors provided an overview of all the works carried out earlier. Types of blockchain, and schematic decision diagram to determine which blockchain technology to be used based on the application scenario is also discussed in detail in this work. Data sharing and thrust management are considered for evaluation purposes.

In this work [12] authors present fog-based architecture for IOT-based healthcare systems. The proposed architecture is validated by performing experiments in iFogSim. The proposed system was applied and network usage values, latency, and cloud-based, fog-based scenarios were compared. From the results obtained it was observed that the proposed architecture minimizes the latency and network usage value to the significant level to manage the identities of the user securely.

In the proposed work [13] authors designed an anomaly-based network intrusion detection system. The authors used 90.8 GB of real network packet dataset from the Information Security Center for Excellence. The system analyzes the captured packet from the dataset files in the environment by using Hadoop Apache and Spark. The authors applied Principle Component Analysis (PCA) for the reduction of feature dimensions and used GMM to identify the anonymous behavior of the network packets. This work focuses mainly on single-mode intrusion detection systems. In the future, this, model needs to be addressed with DIDS.

In [5] they proposed a distributed intrusion detection using blockchain and cloud infrastructure. Various advantages of DIDS are discussed by the authors and a common consensus protocol is used for all IDS systems. Alerts generated by the individual system are integrated. The experiment results are shown in terms of data transfer speed for various-sized files.

In this paper [14], the authors proposed a distributed intrusion detection system model for smart homes. The architecture is designed by assuming that at least the service provider can maintain the HG for monitoring and controlling. The proposed solution meets the expectations using a) fast preliminary analysis and processing security security-related data received locally from smart devices within HAN b) advanced data processing by the service provider c) Knowledge of security incidents is maintained across the network. The results are compared with functionalities with data collection, selection, and data comparison.

Authors in this paper [15] designed a fog-cloud architecture using blockchain, and the system is analyzed for security improvement. The authors discuss the various advantages and disadvantages of fog computing and blockchain technology. Also, various threat analysis of blockchain technology is carried out by the authors like DDoS attack, man in man-in-middle attack. The work is evaluated for maximum service latency, CPU usage, maximum number of service responses, and maximum power consumption. The results obtained in this proposed work show that CPU usage, power consumption, and service latency are high when blockchain is used. Also, the system is analyzed for various security aspects.

In [16] we proposed a fog computing architecture to share sensor data using blockchain functionalities. The permitted blockchain with a managed membership is used in this work. The versatile fog gateway HCL-BaFog is

used where the data plane and the controlled plane are separated, and the lightweight Linux container virtualization is provided with the help of the docker framework. For sensors single board computer (SBC) system based on 32-bit with Cypriot cluster lab (HCL) is used. The work is evaluated using a multi-chain network with three fog nodes on a separate Raspberry Pi. The response time is calculated by varying the number of clients in the network.

This research paper [17] proposes a three-tiered system in which the lower layer represents the device layer, which consists of IOT devices and sensor devices. The middle layer enables fog computing, by deploying fog nodes to handle data forwarded by dedicated IOT nodes, and allows for edge monitoring, classification, and analyzing capabilities. Results from the second layer are forwarded to the topmost third layer, named the cloud layer. The entire network communicates through two communication protocols, namely Software-Defined Networking (SDN) and the blockchain. Using SDN gives network administrators fined-grained control over Fog and IOT nodes, through the use of programmable APIs.

The authors in the paper [18] proposed a privacy-preserving blockchain validation system in fog architecture. This work aims to support the integration of IOT, Blockchain, and fog computing technology. In this architecture, the more trusted fog node is given the higher authority to validate a block on behalf of blockchain nodes. To guarantee privacy awareness a Blockchain-based PKI architecture is used which can provide higher abnormality levels, which maintains the decentralized property of the blockchain system. This work is compared with the current validation mechanism in PoW.

The authors in this paper [19-20] proposed-blockchain and fog computing for trusted industrial internet of things-fusion. In this paper, the authors investigated how to manage distributed trust information and enable trusted configuration action in the industrial IOT. Specifically, the author focused on how the joint and coordination adoption of such technology can make technician intervention on industrial equipment. The architecture is designed to simplify the management, configuration, and assessment of industrial IOT systems; the application of the proposed architecture is carried out using the railways use case. For evaluation of work reliability and availability, it is calculated for three test cases. The authors in this paper [21] propose Reverse Engineered Design Science Research (REDSR), artifacts from leading vendors are used to elicit the design principles and rules with relevant details of Big Data components. We conclude that the findings are relevant and useful for DevOps architects and practitioners in operating complex, heterogeneous Cloud-based Big Data platforms. The authors in this paper [22] provide the use case scenarios of the applications, The found applications can be grouped into the main categories of Emissions Trading and Green Certificates, Sustainable Energy, Sustainable Mobility, and Green Financing. Within these applications, blockchains are being used as supporting technology. Transparency, traceability, and immutability are particularly beneficial in blockchain-based applications against climate change. As a downside of the technology, controversial aspects of the blockchain are considered as the energy consumption of the technology.

In [23] the authors discuss about Access control method which allows data accessing of an authorized user. In recent years, file or data access control has been a very challenging issue in Big Data (BD). Existing access control schemes mainly focus on the confidentiality of the data storage from unauthorized users. In this paper, a novel file or data access control scheme has been presented. The proposed scheme allows for reducing the searching cost and accessing time while providing BD to the user. It also minimizes the problem of data redundancy.

3. Proposed model

The implementation of the “Distributed intrusion detection system using blockchain and fog computing” in Figure 1 is designed in the simulation environment using the NET software development framework. The intrusion detection system is targeted on the text files, where selective forwarding attacks need to be detected using an improved watchdog approach. Once the attack is detected the intrusion detection system will reroute the path. The alerts and data from the intrusion detection system are added as blocks in the fog layer to preserve the privacy of the intrusion information. The fog node will process the data and upload the log to the cloud to have an overview of the entire network.

This implementation aimed to address the gap that has been deduced from an extensive literature survey of existing and related works.

In this architecture, the bottom level tier consists of multiple IDS systems, fog nodes at the middle layer, and cloud

at the topmost level.

These tiers interact with their upper-level tiers to transfer the data. Blockchain support is provided at the fog nodes, here the data generated by IDs are added as the blocks, and block hash is generated using the SHA256 algorithm.

Data from various IDS are linked to the blocks using a hash of the previous blocks.

The drive cloud service is used to store the data permanently.

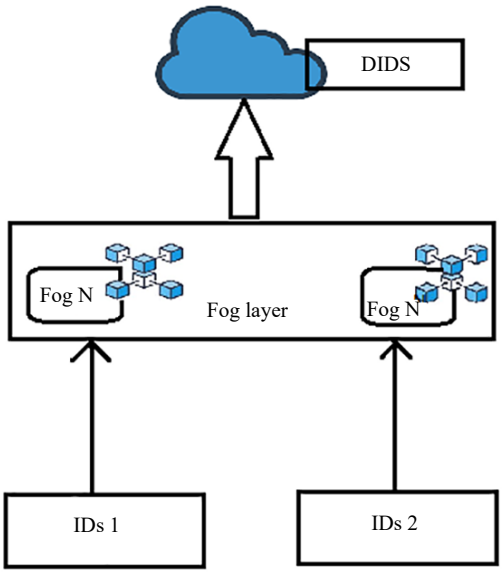

Figure 1. System architecture. This figure represents the three-layered architecture of the proposed system

3.1 *Network model*

SFA node: The selective forwarding attack node is the compromised or malicious node that will try to drop the packet without forwarding it to the neighboring nodes. Some nodes in the network is randomly selected as SFA nodes which will drop all the packet it receives.

Intermediate node: Intermediate node will try to detect abnormal behavior of the nodes that is whether the next hop neighboring nodes discard its data without forwarding it to the next node.

It is assumed that the Selective Forwarding Attack (SFA) node in the network is the normal node with the same transmission range as the other node in the network. The attacker may obtain some nodes through compromising. After analyzing and modifying programs within the node, the node becomes a misbehaved SFA node. The SFA node will participate in the routing as a normal node. However, this node will discard the packets without forwarding them to the neighboring nodes.

3.2 *Fog and blockchain*

The second layer in the architecture consists of fog nodes supported with blockchain functionalities. The data generated from multiple intrusion detection systems are transferred to respective fog nodes where the data processing is carried out and data from intrusion detection systems are added as blocks. The first block in the blockchain will be the genesis block; the newly generated blocks will be linked to the previous block using their unique hash. SHA256 cryptographic hash function is used to create a hash to the blocks as in Figure 2 and Figure 3.

```
public class Block
{
    public int Index { get; set; }
    public DateTime TimeStamp { get; set; }
    public string PreviousHash { get; set; }
    public string Hash { get; set; }
    public string Data { get; set; }

    public Block(DateTime timeStamp, string previousHash, string data)
    {
        Index = 0;
        TimeStamp = timeStamp;
        PreviousHash = previousHash;
        Data = data;
        Hash = CalculateHash();
    }

    public string CalculateHash()
    {
        SHA256 sha256 = SHA256.Create();

        byte[] inputBytes = Encoding.ASCII.GetBytes($"{TimeStamp}-
{PreviousHash ?? ""}-{Data}");
        byte[] outputBytes = sha256.ComputeHash(inputBytes);

        return Convert.ToBase64String(outputBytes);
    }
}
```

Figure 2. Creation of genesis block. The first block in the blockchain is known as the genesis block, the program for the generation of the first block is shown in Figure 2

```
public IList<Block> Chain { set;  get; }

public Blockchain()
{
    InitializeChain();
    AddGenesisBlock();
}

public void InitializeChain()
{
    Chain = new List<Block>();
}

public Block CreateGenesisBlock()
{
    return new Block(DateTime.Now, null, "{}");
}

public void AddGenesisBlock()
{
    Chain.Add(CreateGenesisBlock());
}

public Block GetLatestBlock()
{
    return Chain[Chain.Count - 1];
}

public void AddBlock(Block block)
{
    Block latestBlock = GetLatestBlock();
    block.Index = latestBlock.Index + 1;
    block.PreviousHash = latestBlock.Hash;
    block.Hash = block.CalculateHash();
    Chain.Add(block);
}
```

Figure 3. Generation of blocks. The new blocks are added and linked to the previous block so that log data from IDS can not be manipulated by a compromised or malicious system

4. Results and discussion

This Section discusses on the Experimental results carried out on the said scenario. Figure 4 represents the intrusion detection with SFA using Watchdog approach, Whereas Figure 5 shows the generated blocks with log of its details.

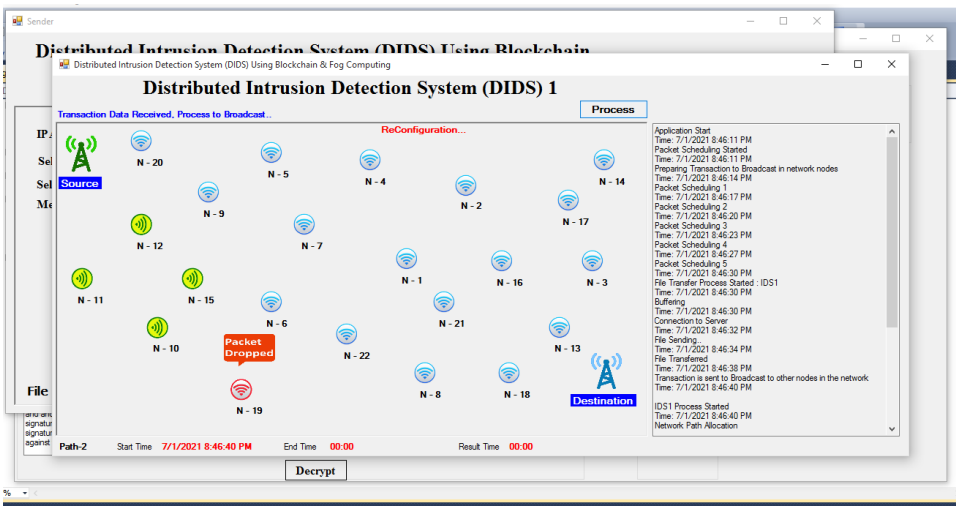

Figure 4. Detection of intrusion. The selective forwarding node detection using the watchdog approach is shown in Figure 4. The log from IDS is shown on the right side of Figure 4

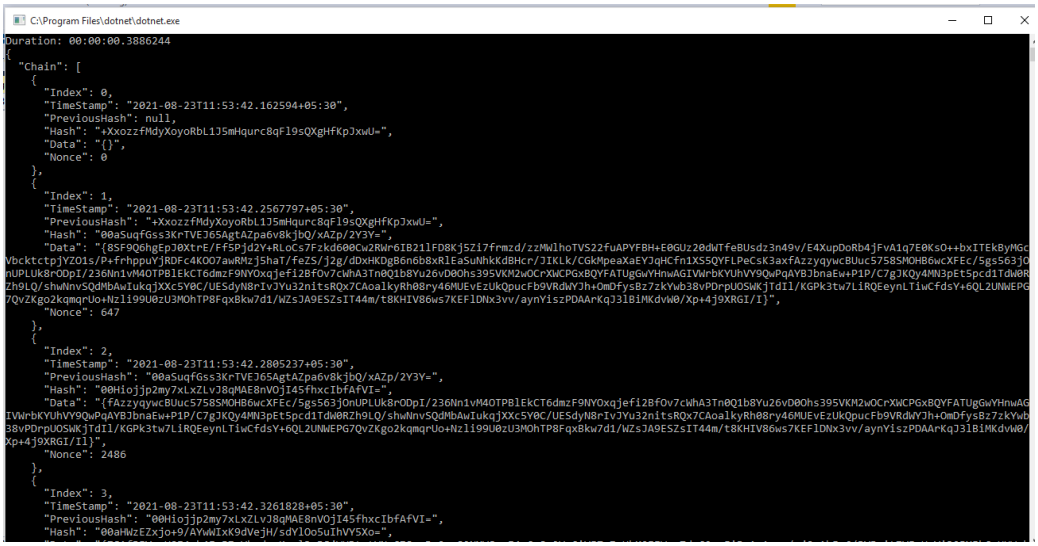

Figure 5. Block generated. The logs from IDS are added are blocks and proof of work is calculated

The data from the intrusion detection systems are added as the blocks in the fog layer as in Figure 6 to provide security to the alert generated from the IDS system as some of the participating systems may have compromised to the intruder. Each block is linked to the previous block using the hash. The SHA256 cryptographic hash algorithm is used to generate block hash and block index. The log data tamper-proof roof.

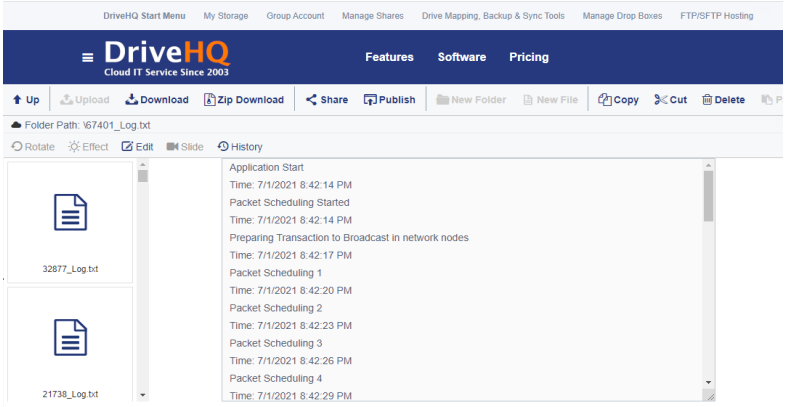

Figure 6. Data uploaded to the cloud. The data from multiple intrusion detection systems are uploaded to the cloud for permanent storage and future analysis of data

The data from various IDS are secured using blockchain technology and are uploaded to the cloud to have an overview of the entire system. The driver-free cloud service is used in this project to store the data permanently. Using these data, the network admin can take necessary action to prevent the intrusion and to discard the malicious nodes from the network.

4.1 *Experimental setup*

All the simulation performed in the work is carried out by designing a simulation setup using. NET in visual studio IDE. Based on the proposed scheme, a trial system is developed, the system consists of multiple (two) IDS where one is the replica of the author, the fog layer is integrated with blockchain functionality, where the PC is considered as a fog node [Intel i3 CPU, 16GB DDR3 RAM], and drive free cloud storage is used as cloud service.

Steps to detect malicious nodes:

Step 1: N1 sends the packet to N3 via N2, and I will eavesdrop on the packet and save a copy in buffer b.

Step 2: Node I eavesdrops on the communication between N2 and N3 for t second (depends on Node processing and sending speed) and refers to step 5 in case of not receiving any packet.

Step 3: Mi value is calculated if I eavesdrop on the packet PN2 N3.

Step 4: If Mi = 0 the message in cell bi will be deleted and the algorithm returns to step 6. If Mi ≠ 0 then the message remains in the buffer and moves to step 5.

Step 5: The warning message is raised signaling the maliciousness of node N2, is sent to an upper layer by the I node and the path will be rerouted.

Step 6: End of algorithm.

For the experiment, data from IDS are recorded with different scenarios.

a) Fog/Cloud/Integrated

To calculate service latency and response time, data from IDS are experimented with different architectures. This experiment setup refers to whether application execution is solely conducted on fog, cloud, or integrated.

b) With/without blockchain

The application is experimented with disabling the blockchain functionality at the computing layer. It is observed that blockchain functionalities reduce performance.

4.2 *Performance analysis*

Service latency as in Figure 7 is the delay between the client request and service provider response, here service latency is calculated as the summation of network delay and task completion. Service latency is calculated with different environment setups by using only fog, cloud, integrated fog, and cloud with and without blockchain. It is observed that service latency increases with blockchain functionality.

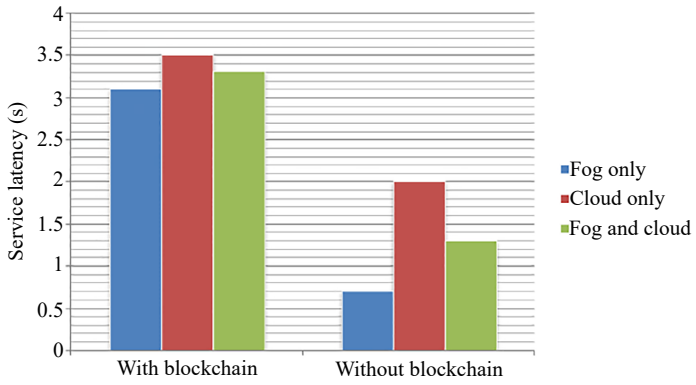

Figure 7. Service latency. The service latency is calculated for different experimental setups

Response time as in Figure 8 is the total amount of time, it takes to respond to a request for a service. It starts when a user sends a request and ends at the time the application states that the request has been completed. It is observed that fog responds faster than the cloud.

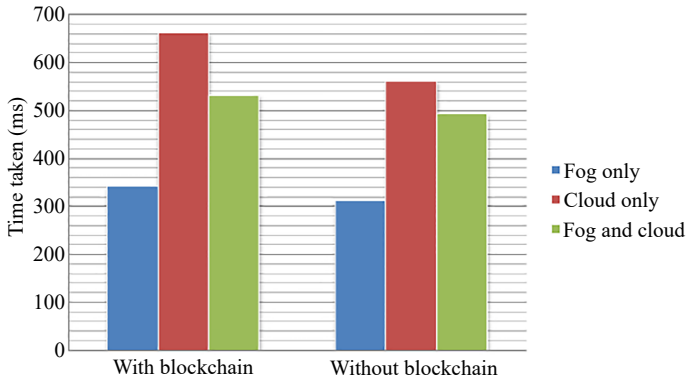

Figure 8. Response time. The response time is calculated for different experimental setups

The block creation time in the proposed work is calculated by varying the number of transactions (number of blocks) from 10 to 1,000. It is observed that the time taken to create 1,000 blocks are 2.4 sec. The response time of the system increases linearly with the number of blocks as in Figure 9.

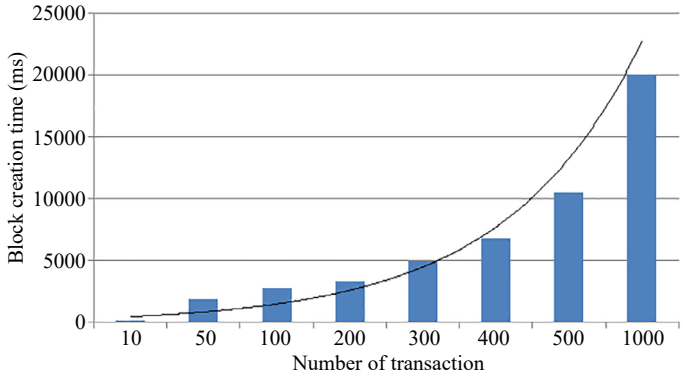

Figure 9. Block creation time

The total execution time for blockchain functionality is calculated by varying the number of blocks as in Figure 10. The execution time includes the creation of blocks, validating the block, and mining the block for proof of work. The result obtained shows that blockchain functionality reduces the response time with the increase of transactions or blocks. This increases the communication overhead in a large network where huge transactions are carried out.

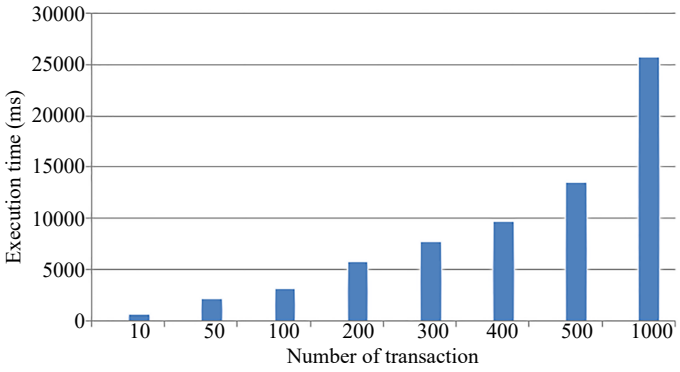

Figure 10. Execution time for blockchain functionality

5. Conclusion and future work

The architecture of a distributed intrusion detection system is presented to enrich the single-mode IDS system. Individual IDS systems will transfer the data to the fog node to minimize network congestion that may occur when data is directly transferred to the cloud. Each fog node is endowed with blockchain to preserve the privacy of data. Upon successful transmission of data from source to destination all the data will be stored in the cloud. The performance of this work is calculated with various loads of data. This work is evaluated with transmission delay, packet delivery ratio of IDS system, response, and service latency. In the future the integration of blockchain and fog computing approaches can be implemented in real real-time environment and communication overhead problems need to be addressed.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Axelsson S. *Intrusion detection systems: A survey and taxonomy* (*vol. 99*). Technical Report; 2000.
[2] Debar H, Dacier M, Wespi A. Towards a taxonomy of intrusion-detection systems. *Computer Networks*. 1999; 31(8): 805-822.
[3] Snapp SR, Brentano J, Dias GV, Goan TL, Heberlein T, Ho C, et al. DIDS (Distributed Intrusion Detection System)-Motivation, architecture, and an early prototype. *Proceedings of the 14th National Computer Security Conference*. Washington, DC; 1991. p.167-176.
[4] Ghribi S, Makhlouf AM, Zarai F. C-dids: A cooperative and distributed intrusion detection system in a cloud environment. *2018 14th International Wireless Communications & Mobile Computing Conference* (*IWCMC*). Limassol, Cyprus; 2018. p.267-272.
[5] Kumar M, Singh AK. Distributed intrusion detection system using blockchain and cloud computing infrastructure. *2020 4th International Conference on Trends in Electronics and Informatics* (*ICOEI*) (*48184*). Tirunelveli, India; 2020. p.248-252.
[6] Baouya A, Chehida S, Bensalem S, Bozga M. Fog computing and blockchain for massive IoT deployment. *2020 9th Mediterranean Conference on Embedded Computing* (*MECO*). Budva, Montenegro; 2020. p.1-4.

[7] Singh VK, Chawla H, Bohara VA. A proof-of-concept device-to-device communication testbed. *Computer Science: Networking and Internet Architecture*. 2016. Available from: https://doi.org/10.48550/arXiv.1601.01398
[8] Singh P, Nayyar A, Kaur A, Ghosh U. Blockchain and fog-based architecture for the internet of everything in smart cities. *Future Internet*. 2020; 12(4): 61.
[9] Li H, Han D, Tang M. A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. *IEEE Systems Journal*. 2020; 15(3): 3189-3200.
[10] Kim S, Kim B, Kim HJ. Intrusion detection and mitigation system using blockchain analysis for bitcoin exchange. *Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things.* Singapore; 2018. p.40-44.
[11] Meng W, Tischhauser EW, Wang Q, Wang Y, Han J. When intrusion detection meets blockchain technology: A review. *IEEE Access*. 2018; 6: 10179-10188. Available from: https://doi.org/10.1109/ACCESS.2018.2799854.
[12] Awaisi KS, Hussain S, Ahmed M, Khan AA, Ahmed G. Leveraging IoT and fog computing in healthcare systems. *IEEE Internet of Things Magazine*. 2020; 3(2): 52-56.
[13] Kato K, Klyuev V. Development of a network intrusion detection system using Apache Hadoop and Spark. *2017 IEEE Conference on Dependable and Secure Computing*. Taipei, Taiwan; 2017. p.416-423.
[14] Gajewski M, Batalla JM, Mastorakis G, Mavromoustakis CX. A distributed IDS architecture model for smart home systems. *Cluster Computing*. 2019; 22(1): 1739-1749.
[15] Ashik MH, Maswood MM, Alharbi AG. Designing a fog-cloud architecture using blockchain and analyzing security improvements. *2020 International Conference on Electrical, Communication, and Computer Engineering* (*ICECCE*). Istanbul, Turkey; 2020. p.1-6.
[16] Cech HL, Großmann M, Krieger UR. A fog computing architecture to share sensor data using blockchain functionality. *2019 IEEE International Conference on Fog Computing* (*ICFC*). Prague, Czech Republic; 2019. p.1-40.
[17] Baniata H, Kertész A. PF-BVM: A privacy-aware fog-enhanced blockchain validation mechanism. *Proceedings of the 10th International Conference on Cloud Computing and Services Science* (*CLOSER*). SciTePress; 2020. p.430-439.
[18] Elisa N, Yang L, Chao F, Cao Y. A framework of blockchain-based secure and privacy-preserving e-government system. *Wireless networks*. 2018; 3: 1-1.
[19] Ceccarelli A, Cinque M, Esposito C, Foschini L, Giannelli C, Lollini P. FUSION-fog computing and blockchain for trusted industrial internet of things. *IEEE Transactions on Engineering Management*. 2020; 69(6): 2944-2958.
[20] Sharma PK, Chen MY, Park JH. A software-defined fog node-based distributed blockchain cloud architecture for IoT. *IEEE Access*. 2017; 6: 115-124. Available from: https://doi.org/10.1109/ACCESS.2017.2757955.
[21] Sharma RS, Mannava PN, Wingreen SC. Reverse-engineering the design rules for cloud-based big data platforms. *Cloud Computing and Data Science*. 2022; 3(2): 39-59.
[22] Thalhammer F, Schöttle P, Janetschek M, Ploder C. Blockchain use cases against climate destruction. *Cloud Computing and Data Science*. 2022; 3(2): 60-76.
[23] Namasudra S, Roy P, Balusamy B, Vijayakumar P. Data accessing based on the popularity value for cloud computing. *2017 International Conference on Innovations in Information, Embedded and Communication Systems* (*ICIIECS*). India, Coimbatore; 2017. p.1-6.