A Preventive Intrusion Detection Architecture Using Adaptive Blockchain Method

Pratima Sharma[1](✉), Rajni Jindal[1], and Malaya Dutta Borah[2]

[1] Delhi Technological University, Delhi, India
pratima.sharma1491@gmail.com, rajnijindal@dce.ac.in
[2] National Institute of Technology Silchar, Silchar, India
malayaduttaborah@cse.nits.ac.in

Abstract. This paper presents a network intrusion behavior detection utilizing an adaptive blockchain mechanism. A Layered Voting Rule System (LVRS) is introduced, which contains a positive layer, negative layer and propagation layer which trains the blockchain using the power consumption of the users to transfer and receive the data. The performance of the network is analyzed using Quality of Service (QoS) parameters, including throughput and power consumption. The observed throughput and power consumption of the proposed model is improved by more than 30% as compared to the model without blockchain.

Keywords: Layered Voting Rule System · Blockchain · Intrusion · Adaptive behavior

1 Introduction

The virtual world was built as the true global infrastructure when our technology system introduces both computer technology and network technology. The virtual world today is nearly as powerful as the real economy, placed as the basis for the corporate system. However, at the time when the information, in particular, the business information, exchanges online, a trustworthy authority is essential and necessary to ensure the credibility of the data and the actual value that can be grouped into the real world. This type of mode is the internet's company mode now. These so-called trusted parties, however, may also be likely and able to do some malicious and harmful things knowingly or unknowingly, such as tracking or selling customer data for company use [1].

Blockchain is suggested as a prospective alternative to the above issue. Blockchain is relatively an advanced technology that allows multiple authoritative domains which do not trust each other to collaborate, cooperate, and coordinate in a decision-making process. The advent of blockchain provides credible information management and exchange methods that can make internet transactions more real and free of third parties [2]. Various blockchain-based applications used to deliver company and other services that have a major effect on the online business system. Blockchain provides online transfer of data with non-modifiable data records, making the transfer of data more reliable. The blockchain boom is an integral part of the network, especially for the online business.

R. Patgiri et al. (Eds.): BigDML 2019, CCIS 1317, pp. 25–35, 2020.
https://doi.org/10.1007/978-3-030-62625-9_3

Blockchain-based applications can help to create internet reality and achieve fairness, equality, and sharing between online virtual reality in the real world. The object produced by blockchain technology in the non-real globe for the confirmed data becomes valuable and authentic. Blockchain will also play a more critical role in the future if online privacy and reliability become increasingly essential. Blockchain-based systems will be the basic infrastructure that can provide people with a wealth of services [3]. Chain management is applied when there is a need for a data transfer policy to maximize the efficiency of resource sharing. When one node in the network starts the data transfer to another node in the system, it is often observed that the source node includes other nodes in the transaction to a form a route. The intermediate nodes are referred to as hop in any chain architecture. As shown in Fig. 1, the source node aims to transfer the data to the destination node. To maximize resource utilization, one node becomes a data vendor for multiple nodes. This increases the randomness in the network, and the network becomes vulnerable to the intruders.

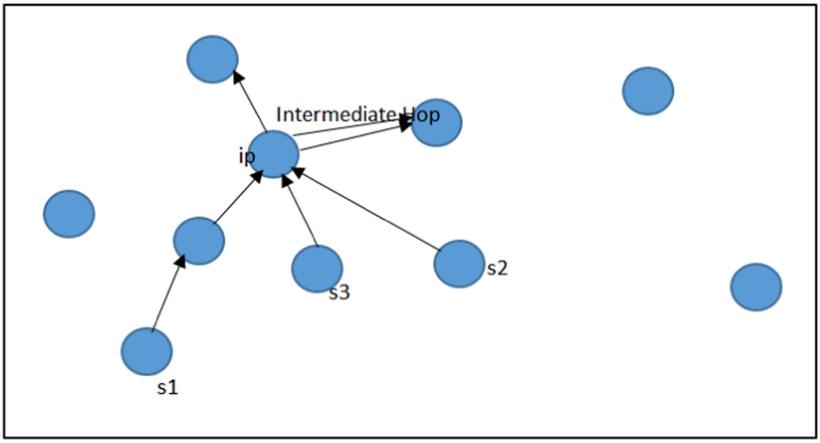

Fig. 1. The hop behavior

As shown in Fig. 1, if the intermediate node represented by “ip” receives a lot of data packets or data elements from source nodes s1, s2, s3 … sn and so on, the intruder may also attempt to transfer the data from “ip” which will further affect the network environment. If described practically, every network has a network admin, but the network admin does not aim to identify the intruder, it would instead go to find the node in its system, which is intruded. As a user is using AVG antivirus. The antivirus cannot do anything to the virus generator, but it prevents its network from the effects of the virus. This paper focuses on this logic and prepares a Layered Voting Rule System (LVRS) whose description is given in Sect. 3.

The rest of the paper is organized as follows. Section 2 explains the related work. Section 3 provides detailed information on the proposed architecture. In Sect. 4, the assessment of the results is presented. The paper is concluded in Sect. 5.

2 Related Work

Meng et al. (2018) presented a study of the integration of Intrusion Detection System (IDS) and Blockchain Technology. The context of this type of intrusion detection and blockchain addresses its application in its route to migrate the issues of information exchange and trust calculation cooperatively. Blockchain technology is an emerging possibility for decentralized activities and information management without a trusted third party. Khan et al. (2018) presented a survey of primary security issues related to the Internet of Things (IoT). It categorized the most critical security issues and its regard to the IoT layered structure and, different protocols used in networking also been discussed. This work shows the difference between current work and past work related to the IoT, even the security issue against the existing IoT security problem. The suggested work also defines open research issues and IoT safety difficulties. Banerjee et al. (2018) with the assistance of several observations, the IoT safety option suggested by authors, included the absence of public access in the IoT dataset used by the researcher and practitioner. They also included the possibly delicate elements of the IoT dataset; after this, they discuss the capacity of blockchain technologies in enabling safe storage of IT dataset, there is a need to create a normal stakeholder for this processing. Li et al. (2018) presented the background and recent situation of the intrusion detection system, the characteristics and its ranking in the specific situation. It is a kind of technology which protects the network security from the attacks. It is also useful in detecting the speed and improving the integrity of the data security infrastructure. In this, they applied the technology to the blockchain information security model. Kim et al. (2018) presented three types of intrusion detection model for the bitcoin exchange and gave the detection and mitigation system with the help of the blockchain analysis. The main justification for the monitoring and mitigation system exploits the decentralized and governmental behavior of bitcoin blockchain as a fail-safe way to complete the present time system. Advanced technology offers the ability to search for intrusion in real time, which cannot be provided by current job. Kolekar et al. (2018) proposed state-of-the-art, hidden wall strings. In four dimensions, we assess both in-generation and study schemes: disseminated ledger, intrusion detection, blockchain project, consensus protocol, and insightful agreement. They also conclude that the current BLOCKBENCH, skeleton criteria for understanding the effectiveness of private blockchain and government blockchain. Blockchain methods have been a substantial secure power in recent years. Blockchains are shared ledgers that allow sides that do not support each other continuously to maintain several ecumenical nations. The parties agree on states' easiness, norms, and background. Li. et al. (2019) presented a CBSigIDS which is a design of Cooperative Block-chained Signature-based IDSs. It is used to create and renew a reliable tag database in an IoT setting. CBSigIDS provide a solution for integrated architectures without the need for a reliable intermediary. The results show that the calculation of CBSigIDS can improve the toughness and performance of signature-based IDSs in adversarial cases. Collaborative Intrusion Detection Network (CIDN) has become an important and essential security option for safeguarding IoT systems, enabling distinct IDS nodes to swap information with each other, e.g., regulations. However, evil nodes in a CIDN can generate untruthful tags and communicate with others, which can considerably degrade tracking effectiveness and robustness. Signorini et al. (2018) proposed a method called ADvISE: the first anomaly detection tool for a blockchain system which gives blockchain metadata, named forks, for the addition of collect potential malicious request in the present network system to escape the attacks. ADvISE add-on and analyzes the malicious forks for the creation of a threat database that provide the detection and prevention of future attacks. In general, ADvISE give permission to the detection of the abnormal transaction and protect them for being further spread.

3 Proposed Architecture

The proposed architecture monitors the entire data stream as the primary input to the monitoring system, and the users are connected to form the blockchain. The proposed work adopts a behavioral framework. The proposed architecture is named as LVRS, which contains three layers, a positive layer, a negative layer, and a propagation layer, as shown in Fig. 2.

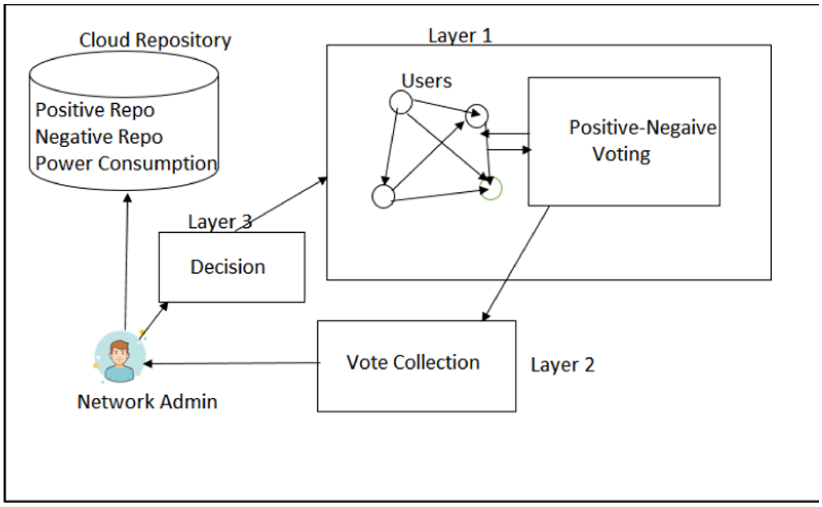

Fig. 2. Proposed architecture

Layer 1: The nodes are deployed in the network, and the nodes also referred to as users start sharing the resources from one end to another end. Blockchain technology is utilized for deploying the user nodes. Each user node stores the information in the form of ledger. Further, ledger information is utilized by the network admin for identifying the intruder node. The voting rule is based on the users, and each user had an independent set of data. The user design creates a semi-autonomous blockchain mechanism as each user is partially affected by another user who votes for him or against him. The sustainability of the user is dependent upon the positive votes, which is further controlled by the network administrator. The demanding user is referred to as destination, and the original resource holder is designated as the source in the proposed work. Each data transfer will also involve intermediate nodes, which are referred to as hop in the proposed work. Each data transfer is counted as one vote from source to destination vice and versa. The intermediate nodes are also benefited if the data is transferred successfully.

Layer 2: Layer 2 is operated by the Network Admin. The voting points are stored with the Network Admin at the Cloud Layer. Positive Layer Repository (PLR) and Negative Layer Repository (NLR) is created from the voting of the source to destination. Also, the power consumption in each simulative iteration of individual nodes and the total transfer is stored.

Layer 3: The third layer propagates the power consumption in combination with the positive repository and the negative repository. This layer decides whether the user is safe for resource sharing or not. LVRS further bifurcates the propagation layer identification mechanism in subsequent steps in which the first step is for the propagation mechanism, and the second step uses gradient functions, which is followed by linear quad architecture for data propagation. LVRS analyses the behavior of the user based on the propagation data, which is generated through the overall power consumption in transactions. A unique voting rule is presented in the paper, which helps in analyzing the network when it is scanned for the intrusion.

The workflow of the proposed architecture is described as follows:

a) The users are deployed with random locations in the network.
b) The users will share the data as a resource sharing mechanism.
c) The input data, i.e., the data user wants to transfer or share from one end to another end, can be sent only once in one simulation.
d) One data transfer will be considered as one vote to the destination.
e) Source and destinations are assumed to be immune from intrusion as the network considers the vote as a positive effect to the immunity.
f) The Network Admin (NA) has a veto power to reject the vote count of any node if NA feels like the node is compromised.
g) NA uses the blockchain mechanism in three layers of processing and stores the information in the cloud.

It is assumed that every intruded node which is involved in the data transfer, will consume more power but every high energy consuming node cannot be considered as intruded. The overall proposed structure is demonstrated in Fig. 3(a), Fig. 3(b) and Fig. 3(c) as follows.

As shown in Fig. 3(a), when a source ‘s’ transfer the data to ‘d’ successfully, the network admin counts it as a positive vote whereas, Fig. 3(b) shows that if the node is not able to transfer the data to ‘d’ successfully, the node suffers a penalty. It is assumed that 65% of the total transmitted data is received at the destination end, the transaction is said to be successful transaction and the network admin stores the information of the source node and the hops in blocks to rate the node between 0.50 to 1.0. The rating is done based on the total amount of actual data transfer from one end to another. If the node is involved in any other transaction, the average weight of all the previous operations and the current transaction is considered. If the transaction is not successful, i.e., if the

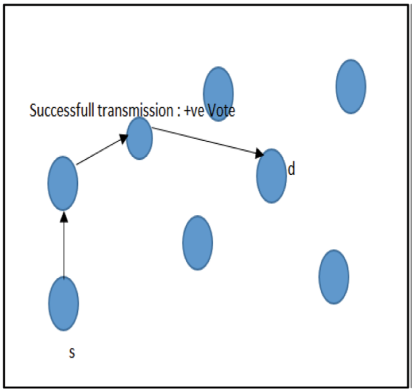

Fig. 3(a). Positive vote

received amount is less than 65%, the source node gets a penalty between 0.1 to 0.49, and hence. The negative weight is updated. The hops in the network also get penalty between 0.1 to 0.20. At the time of the network scan, if the node has a weight more than 0.60, the node is free from the scan. A node having a negative rating more than 0.20 is scanned twice at the time of the scan. The nodes are also referred to as users in our proposed model.

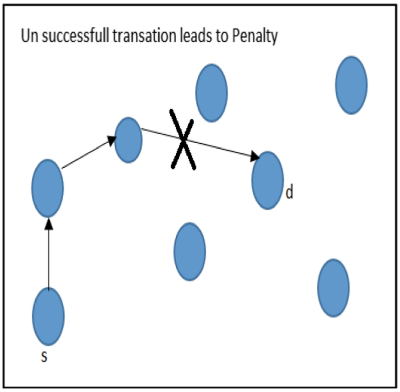

Fig. 3(b). Penalty

Figure 3(c) represents the decision-making architecture of LVRS, which involves Positive Layer Repo (PLR) and Negative Layer Repo (NLR) as discussed earlier. In addition to the PLR and NLR network, admin also keeps a record of consumed power in the data transaction through each user in the network and uses it for decision making to find any intrusion in the network. The nomenclature of all used variables is given in Table 2. The description of identification is as follows. The users are deployed randomly in the network with a random position. The ordinal measures of deployment are illustrated in Table 1.

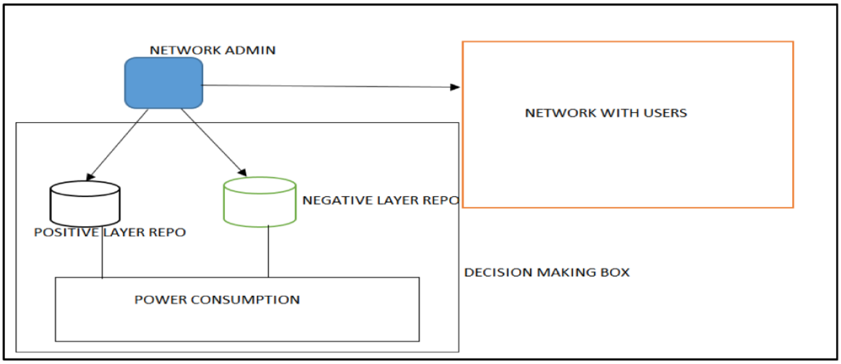

Fig. 3 (c). Decision making of LVRS

Table 1. Deployment parameters

Total user count	40–60
Deployment mode	Random
Data type	Bits
Area of deployment	1000 × 1000 m
Selection mode	Random
Total number of simulations	100–1000
Deployment tool	Anaconda
Deployment framework	Spyder
Language used	Python

Table 2. Nomenclature of variables

Variable	Description
$\mathrm{P_t}$	Amount of power required to transfer a data packet
$\mathrm{P_r}$	Amount of power consumption for receiving a data packet
$Consumed_{Power}$	Total power consumed by the node
$Model_{Weight}$	Weight given by the model to a node
$Input_{Architeture}$	Initial power consumption
$window_{size}$	Window size

The proposed model considers a power consumption model when it comes to transferring the data from one end to another. When a user must transfer the data from one end to another, it will consume $\mathrm{P_t}$ amount of power. Similarly, $\mathrm{P_r}$ is the power consumption to receive the data element. NA keeps a record of transfer and receiving of the data elements along with the users who are involved in the data transfer. P_t and P_r is heterogeneous, i.e., it is different for every node. A maximum of 1000 simulations is monitored with a breakpoint after every 100 simulations; hence, the window size of identification is 100. The NA analyses the network after every 100 simulations and can use his veto power at any instance. NA uses power consumption as the main identifying attribute. P_r and P_t has two sub-attributes. The user will consume less power under normal condition and more power under intruded conditions. The pseudo code of node deployment and data transfer with voting is as follows.

Pseudo Code of Node Deployment:

```
Input: $User_{Count}$
$For_{each}$ user in $user_{count}$
$User_{x\,=}$ Deployment_Mode.Random()
$User_{y\,=}$ Deployment_Mode.Random()
Generate $Power_{ConsumptionModel}$
Destination = Generate a random destination.
Source = Look for the resources from the destination
$Intermediate_{Hops}$ = Generate Resource Carrier
Initialize Network
Start Stimulation and Data Transfer
```

The pseudo code deploys the user with random x and y axis in the network. Every user contains some resource which is sharable in the network. A power consumption model is also deployed, which clarifies the total consumption of power when the user receives a data packet and total consumed power when a node receives a data packet. The data is transferred through intermediate hops which have any vacant slot to transfer the data. The data are documents which are available with the user. The resources are not editable; only the owner of the data has the authority to edit the data of the document. The rest of the users have read-only permission.

Identification of Power Consumption

$For_{each}establi$ shedconnection between User1 to User 2

$$Consumed_{Power} = \sum_{k=0}^{n} P_t + P_r \tag{1}$$

$$Prevention_{Input_{Architecture}} = \text{Consumed\_ Power} \tag{2}$$

Initialize Chain Mechanism with $Prevention_{Input_{Architecture}}$
Propagate Chain with linear and Quad propagation model.

$$\text{Linear Model follows} : ax + b = 0 \tag{3}$$

$$\text{Quad Model follows} : ax^2 + bx + c = 0 \tag{4}$$

$$Chain_{Weight} = Model_{Weight} + Input_{Architeture} \tag{5}$$

$$Chain_{Satisfying_{Element}} = Average_{Gradient} + window_{size} \tag{6}$$

$$Average_{Gradient} = \sum_{i}^{window_{size}} Consumed_{Power}$$

If the gradient is satisfied, then cross-validated using block-chain. Cross-validation is done using the same model, which is done to satisfy the chain training. After 1000 simulations, the result of every window is analyzed, and the max affected user is barred, and his/her voting is discarded, and the user is barred in the network.

4 Results

The results are evaluated using the following parameters.

a) Throughput: Total received packets per time frame.
b) Power Consumption: Total consumed power in each window/after total simulation.

Every result is evaluated with the window defined in Sect. 3. Figure 4 represents the throughput of the proposed model with a comparison of the model without blockchain. The throughput of the proposed architecture is high as compared to the network model with no intrusion model. The proposed algorithm has adopted the new intrusion model, which is adaptive and hence, the chances of network intrusion is quite low. The throughput is tested for a maximum of 500 simulation iterations. The average throughput for proposed architecture is noticed to be 13000 whereas, for the generalized network architecture, it stands 8700. A noticeable difference of (13000–8700)/1300 = 33% is noticed.

The proposed architecture is also evaluated for power consumption, as shown in Fig. 5. A Total of 500 simulations is tested based on Power Consumption. A noticeable difference in power consumption is observed. The power consumption of the proposed architecture is low as compared to the network model with no intrusion model.

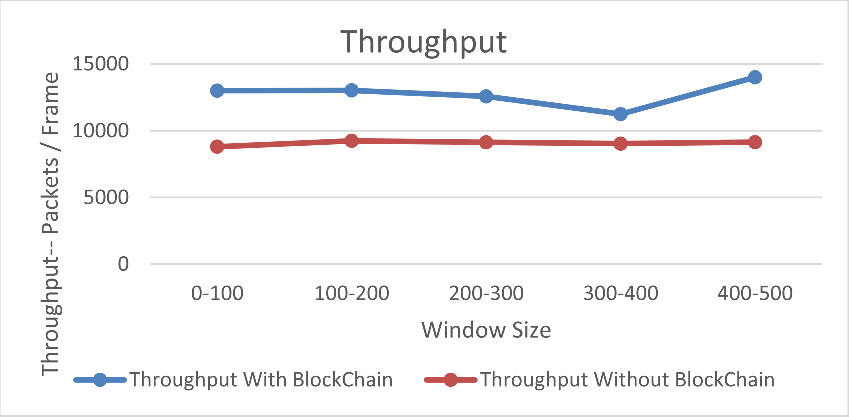

Fig. 4. Throughput

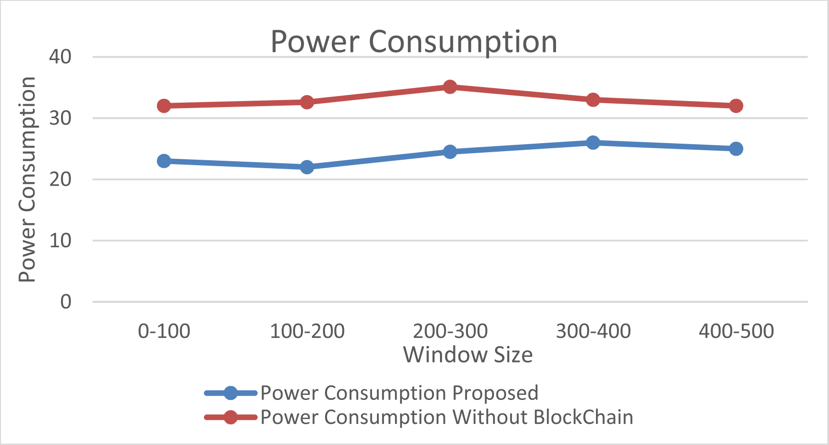

Fig. 5. Power consumption

5 Conclusion

This paper presented an intrusion behavior analysis architecture through adaptive blockchain behavior of intruders. Power consumption is kept as the critical aspect of the intrusion analysis. The proposed architecture is named as LVRS, which contains different layers for a different purpose. A positive layer, a negative layer, and a propagation layer are presented in the paper which utilizes power consumption. LVRS further bifurcates the identification mechanism in subsequent steps in which the first step is for the propagation mechanism, and the second step uses gradient functions, which is followed by linear quad architecture for data propagation. LVRS analyses the behavior of the user based on the propagation data, which is generated through the overall power consumption in transactions. A unique voting rule is presented in the paper, which helps in analyzing the network when it is scanned for the intrusion. Awindow size of 100 simulations is used to apply breakpoints and to analyze the data through breakpoints. A total of 500 simulations are tested based on Throughput and Power Consumption. A noticeable difference of more than 30% is observed in both throughput and power consumption.

References

Meng, W., Tischhauser, E.W., Wang, Q., Wang, Y., Han, J.: When intrusion detection meets blockchain technology: a review. IEEE Access **6**, 10179–10188 (2018)

Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395–411 (2018)

Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for the internet of things security: a position paper. Digit. Commun. Netw. **4**(3), 149–160 (2018)

Li, D., Cai, Z., Deng, L., Yao, X., Wang, H.H.: The information security model of blockchain based on intrusion sensing in the IoT environment. Cluster Comput. **22**, 451–468 (2018)

Kim, S., Kim, B., Kim, H.J.: Intrusion detection and mitigation system using blockchain analysis for bitcoin exchange. In: International Conference on Cloud Computing and Internet of Things, CCIOT 2018, pp. 40–44. Association for Computing Machinery, October, 2018

Kolekar, S.M., More, R.P., Bachal, S.S., Yenkikar, A.V.: Review paper on untwist blockchain: a data handling process of blockchain systems. In: International Conference on Information, Communication, Engineering, and Technology (ICICET), pp. 1–4. IEEE, August 2018

Li, W., Tug, S., Meng, W., Wang, Y.: Designing collaborative block chained signature-based intrusion detection in IoT environments. Future Gener. Comput. Syst. **96**, 481–489 (2019)

Signorini, M., Pontecorvi, M., Kanoun, W., Di Pietro, R.: Advise anomaly detection tool for blockchain systems. In: IEEE World Congress on Services (SERVICES), pp. 65–66. IEEE, July 2018