Soft Computing (2020) 24:15209–15221
https://doi.org/10.1007/s00500-020-04857-0

METHODOLOGIES AND APPLICATION

Blockchain Expansion to secure Assets with Fog Node on special Duty

M. Junaid Gul[1] · Abdul Rehman[1] · Anand Paul[1] · Seungmin Rho[3] · Rabia Riaz[2] · Jeonghong Kim[1]

Published online: 28 March 2020

Abstract
Blockchain expansion is the high priority necessity to improve security. Hacking and other attacks are headway from system innovation and security measures for the cloud architecture. That is why the countermeasure deployed for such attacks should act in an opportune way and ought to be situated as close as possible to attacking device. As an example, DDoS attacks were not that complex as they are getting now with the new technology known as IoT. Imagine the consequences if 25 billion of IoT devices generate a huge amount of data for DDoS attacks. That is why we propose a new framework that can expand blockchain in a manner where more companies can share their resources to enhance security. So, we proposed a new and complete framework with cloud, fog, to secure configuration files with blockchain technology. Our framework considers the configuration files from SDN or NFV as an asset to secure with blockchain. By saving configuration files into blockchain, we can detect illegal changes occurred to configuration files after hacking attack. This study also focuses on expanding blockchain between the multiple service providers with ease to prevent waste of resources. This paper mainly provides opportunities for different could or companies to secure their assets by employing the power of blockchain and smart contracts.

Keywords Blockchain · Fog · Cloud · DDoS · FNOSD (fog node on special duty) · IoT

1 Introduction

We are not only in the age of technology, but also observing decent advancement that is making our lives better. The major reason for this exponential advancement in technology is the downfall of devices in terms of price. Internet becomes a basic need of life from domestic to business users (Lytras et al. 2015). Now, nearly every organizations, offices, and homes are connected to the Internet with a broadband or other type of connections. Internet even helps travelers to find their routes by using online navigation services (Wang et al. 2018). This scenario helps us to understand the necessity of Internet in our daily routines. Access to the resources from all over the world is easy due to Internet connectivity. The conventional networking techniques did not upscale in that manner, and networks are created using hardware like routers and switches. Although researchers are developing more advance algorithms to make them better, but security and privacy issues are also getting more advanced and complex, hackers always try to be ahead of research and development and make their way to bypass the security mechanisms provided by latest algorithms. Updated network devices now support high transmission rate that are available to general public (Agiwal et al. 2016), like 5G services which are contributing to launch attacks with high data rates.

Researchers all over the world find open challenges and make communication even more reliable and faster (Alavian et al. 2009; Xu et al. 2014; Gódor et al. 2015; Kim et al. 2017), but high transmission rate means more network attacks and high in volume taking less time to reach attack destination. The word volume does not come alone, but we often hear words like varsity and velocity. These words point to a new era of big data science and raise more

Communicated by V. Loia.

✉ Anand Paul
paul.editor@gmail.com

Jeonghong Kim
jhk@knu.ac.kr

[1] The School of Computer Science and Engineering, Kyungpook National University, Daegu, South Korea

[2] University of Azad Jammu and Kashmir, Muzaffarabad, Pakistan

[3] Sejong University, Seoul, South Korea

question on privacy and security. Now security and privacy are on the stack again and with high transmission rates alongside with big amount of data. Big data analysis requires more computational power and storage capacity that cannot be done at the edge. Only solution is to do this analysis part at the cloud, which is very costly as far as delay matters, thus consumes bandwidth of the network. As the only option, researchers are working to analyze big data on cloud servers to mitigate attacks like DDoS attacks (Neupane et al. 2018; Somani et al. 2017; Osanaiye et al. 2016).

IoT is another big leap in the technology to make life better and easier. For example a fire sensor in home in an Smart Home IoT frame work (Saeed et al. 2018) in a smart city setting which generates huge amount of data is a reality today (Arasteh et al. 2016) providing information about every second. IoT is getting more mature as many researchers are interested in the field. As a result, IoT is evolving at rapid pace. Now researchers are making it possible for heterogeneous IoT devices to communicate with each other (Wang et al. 2015). Such scenario is a concern for data scientist, but researchers and hackers are also contributing to enhance and maintain security and privacy issues. Recent advancement in the field of computer sciences and security is known as blockchain.

Authors provide a complete framework to mitigate possible DDoS in fog and provide algorithm that helps fog network to reroute data to firewall or cloud as required. As fog will work along with blockchain, author also introduces an algorithm to add or remove node in fog blockchain or to revoke the smart contract as needed. As expansion property of blockchain, author also provides an algorithm that can help organization to expand their blockchain to enhance security features. Blockchain expansion is still under discussion and not yet been studied by the researchers. Framework provided by authors opens opportunities for the businesses to expand their blockchain infrastructure to enhance security requirements. Expansion requires some new algorithms to work along with cloud, fog, and the companies, that is why smart contracts were used in the framework to enhance trust and provide smooth business environment. This algorithm has two versions according to two different scenarios according to need of organization. Overall, author provides a comprehensive framework to mitigate DDoS attack and provide security for software and hardware assets to the company in detail.

The first section gives brief introduction about the work. The second section is motivation where we describe the problem and solution. Rest of the paper is comprising of the proposed framework where authors describe the main functionality of the framework and why it is important to look for new techniques to accommodate future explosions of data and security-related issue. Further, author explains the algorithms that are part of the framework to work network technologies along with blockchain. Authors explained the business opportunities for companies to provide blockchain as a service while choosing a best fog node on special duty to provide better services to the customers. At the end, authors discuss and conclude their research.

2 Literature review

The main focus for this research is to find solution to expand blockchain in fog to avoid 51% attacks by adding more nodes into blockchain and secure configurations file (which we used as an asset to store) into blockchain by hashing techniques which are verifiable if change occurs. Moreover, deploying fog node on special duty to accommodate third-party requests for blockchain services.

2.1 Distributed denial of service (DDoS)

DDoS attacks are popular among hackers. These attacks can vary from very simple to complex depending on the nature of the DDoS attack. Requirements for DDoS attacks seem to be very simple as only three basic components are required.

- Attacker
- Botnets
- Victim

The attacker does not perform DDoS attack directly from its computer or devices rather attacker just makes some modification on someone else's computers or devices that are not properly secured. These devices could vary from simple handheld devices to proper servers. These devices are named as botnet, and foremost function of the botnet is to send as much packet as they can until the victim's devices reach the state where it became unresponsive and unable to reply to any request for services. Although it seems a simple task, but certainly it requires some effort from the attacker side. The attacker needs to get botnet and configure them as required to perform attacks (Gul et al. 2012). DDoS attack is a variant of DoS attack but unlike DoS attack, DDoS uses a multiple number of compromised devices to generate large amount of data and send it to the victim. There are many tools provided to launch DDoS attacks. A lame attacker can use educational purpose lectures about DDoS and can launch an attack accordingly. Kali Linux is one of the best example which provides good environment to test and learn about attacks and develop algorithm to mitigate it, but tools provided by such operating system can be used for proper DDoS attacks as well. Mirai is one of the good example of DDoS attack

with a simple change in basic components. Botnet used by Mirai mainly comprised of four components.

- The bot
- Command and control center
- The loader
- Reporting server

Bots are simply infected devices which perform task of sending packets to the victim. Command and Control center provides information to the attacker about the current status of the botnets. Loader provides a platform to attack single or multiple devices. Report server contains the database about the growth and expansion of botnets (Kolias et al. (2017)). Kambourakis et al. (2017) discuss briefly about the Mirai and how IoT zombies work. Detection is not a problem for Mirai that is why Mirai do not try to hide. In the attack life cycle, Mirai leave its footprints. These footprints can easily be identified by network analysis or via forensics. These footprints can be examined by some of the following criteria.

- Consecutively testing explicit credentials ports.
- Exchanging reports that may generate distinguishing patterns,
- Getting attack binary code
- Communicating keep alive messages
- Generating same type of traffic like UPD, TCP, etc.

World observes the number of DDoS attack in recent years as shown in Figs. 1 and 2. Usually, DDoS attack is launched by botnets and other devices which require little effort, but the nature of DDoS attacks is also changing from simple to complex, i.e., from network level to application level. This could be the result where application and other services might be unavailable to the user. The main idea behind these attacks is to blackmail the organization and ask for ransom. As this happens, organizations start providing DDoS as a service which might be a reasonable business as businesses want to attack their business competitors (Zand et al. 2017).

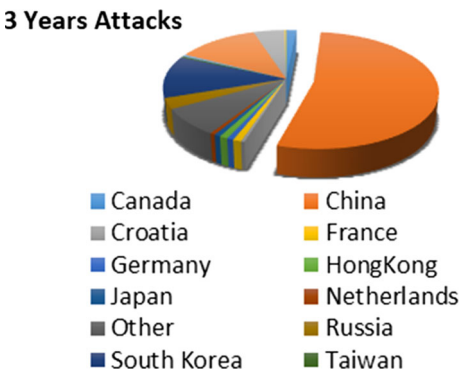

Fig. 1 Worldwide DDoS attacks in three years (2015–2017)

Fig. 2 Web graph representation of DDoS attacks all over the world

Big data generated by such attacks are creating new paradigm for big data analytics. These analytic tools can be used for monitoring and analytic purposes, but placement of these tools in network is still in question for researchers. DDoS attacks can be launched from different sites and can compromise the company responsible to provide security services. Firewalls can also be misconfigured by the attacker and to keep up the pace, and researchers are also trying to find novel solutions for such attacks (Cardenas et al. 2013).

2.2 Emerging security concerns

Internet of Things is changing the world as we see it now. Facilities provided by IoT are making life easier. IoT enables devices, machines to communicate with each other to get better results and understanding about the environment. Many countries spending a lot in IoT research and development. IoT is being most promising area in technology for the future. Researchers are studying the ways of developing and deploying the IoT-based devices up to another level that is from homogeneous- to heterogeneous-level communication (Lee and Lee 2015).

IoT devices are also generating a very large amount of data that categorized under its definition of volume. IoT devices are increasing in number, and count can go up to billions of devices which can generate data that could create a scenario where we required more sophisticated analytics and security platform. A number of platforms like Hadoop and spark are renowned for their big data analytics, but if we consider centralized architecture, we might need some more tools. The researchers are finding their ways to develop more tools to accommodate the new flood of data. We might observe more big data tools which can be

customized for different domains and according to the needs of the user. Data also come with the issue of security and privacy, and upcoming tools might have some feature where these tools provide built-in functionality to provide security for data as blockchain is providing (Marjani et al. 2017).

IoT is growing as an industry providing job security and economic growth. Now, IoT can also be categorized in to social or industrial IoT, etc. Industrial IoT enables the industry to find and adopt new ways to accommodate upcoming challenges on a larger scale. Manufacturing of IoT devices to an industrial level means a large amount of data. Due to different parameters, techniques, and domains, these IoT devices generate a variety of data. This is another open challenge for researcher to make some common grounds or protocols for industrial IoT devices to avoid any implications (Mourtzis et al. 2016). Flood of data from these industrial IoT devices creates more problems as we see it now. Problems are like data security, communication, data storage, and then data manipulation and analysis on a large scale (Ahmed et al. 2017).

IoT provides a platform for devices to communicate regardless of their type and functionality. IoT can interconnect devices from health sector to forest fire, from space to smart cities. If we talk about smart cities, there will be smart homes, smart automobiles, tracking systems, etc. It is essential to process a large amount of data generated by devices near to real time. This requires the optimal placement of data storage and analytic servers along with better computational power. Fog architecture provides opportunity for such kind of scenarios. Still, heterogeneous nature of IoT devices makes it more complex to mitigate attacks. The researchers are making frameworks to provide better security by utilizing fog architecture for smart homes and smart cities. This can simplify the problems to mitigate attacks in real time. It is not an easy task to embed such a diverse technologies and make them work together. So, we have to find a way to protect IoT devices in the first place. By utilizing fog architecture, Pacheco and Hariri (2016) use behavior anomalies analysis to mitigate attacks on sensor in IoT.

Cloud architecture is the attraction for DDoS attacks. A proper attack on a server can block all the services provided to the user by exhausting cloud resources. These attacks not only problem for cloud, but also the users. The researcher is now focusing on securing the cloud more than ever as IoT industry is expanding widely. New architectures, hardware, and software are required, as the cloud is not a simple architecture as far as security is concerned. There are many variables influencing security scenario. A hybrid architecture could be the solution (Tweneboah-Koduah et al. 2017). Social IoT is another big step for internet of things. If devices in IoT go bad and start sending data simultaneously, what would be the possible effect? It will shut down any services provided by the cloud. Twenty to 25 billion devices that go rough and start sending packets to its victim would be the bad scenario. It also make a threat of big data attacks as the world has already seen attack in terabits/second in the start of March 2018. It could be just a beginning to a disaster. Researchers are proposing protocols and solution for heterogeneous devices, highlighting the issue related to such expansion of devices (Frustaci et al. (2017)).

Devices that are not yet much powerful can outsource their computational task to server or more powerful devices. This scenario makes it harder to enforce security policy as IoT devices are already weak devices, and validating or recomputing is not an ideal solution. The model proposed by Olakanmi and Dada (2019), Stergiou et al. (2018), Zhu and Han (2018) performs well to full the privacy and security gaps while outsourcing the computational tasks. Blockchain being an emerging technology can also help android permission system to provide more security to android users. Permission can be stored and retrieve from blockchain to verify or check any changes (Ouaguid et al. 2018). Blockchain is based on modern cryptography (Gupta et al. 2016; Brij et al. 2019), and we also used SHA-based hashing for our simple blockchain that we build using C#.

3 Proposed framework

SDN and NFV configuration files are an asset to secure with blockchain properties. NFV uses servers and other commodities which opens ways for blockchain to be introduced properly. In our proposed framework, we suggest creating blockchain with NFV technology along with FOG nodes that helps to secure their assets from illegal modification. As shown in Fig. 3, NFV part of other network will perform analysis and other function, but it is also prone to attacks. In our framework, we consider ever node and server as fog node that have certain capabilities like storage/capacity, computation power.

With the properties of NFV, we can create a blockchain of devices residing within the NFV architecture. Internal blockchain can be used to secure devices within the architecture. This is a very feasible solution but, in some scenarios, organization might need more security. This means expanding the blockchain from internal to external level. For external level, two or more parties are required to create blockchain and secure each other's assets.

Blockchain is basically a ledger that records all transaction made by authenticated users while utilizing the power of smart contact and certain hashes. Blockchain is initially introduced by a Japanese hacker. Concept of the

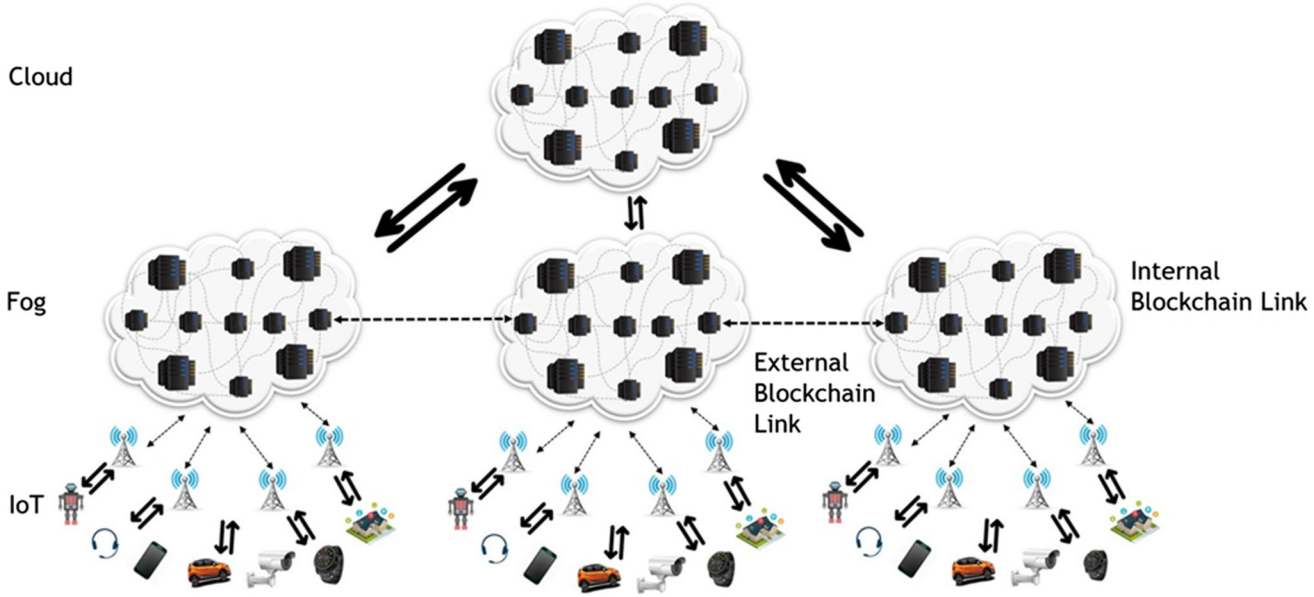

Fig. 3 Proposed architecture

blockchain is to save information in decentralized way so no one can modify certain record without knowing.

Smart contract are digital form of terms and conditions. It has information about what and how much privileges certain party has. As we are going to build private blockchain, smart contract will be initial point on which cloud and fog are agreed. For communication between fog and fog, we need cluster head to communicate with each other.

Hashes are backbone of blockchain. Hashes are used add, delete (search) during every communication that occur in blockchain. For our algorithm and framework, we choose SHA256 hash family. Hash will be shared across the blockchain and saved in the ledger. Smart contract also needs this hash information for future if any modification is required.

3.1 Adding and deleting block

We are developing private blockchain so, adding or deleting block function is assigned to cloud or fog on special duty. Fog on special duty and its responsibilities are explained in further section. If cloud want to add new fog node, then it will generate smart contract accordingly and share it with blockchain, and then, the information will be shared to every node. Revocation of smart contract will stop node to update its database. G_{n} is the node which wants to be the part of blockchain within the fog architecture. G_{n} has some business rules upon which could "C" must agree. These rules are specifically related to the business organization that are running cloud. If cloud is agreed upon such rules, then node in fog can be the part of blockchain, otherwise its request will be discarded. Once node and cloud are agreed, a smart contract "$S_m(G_n)$" will be created and node can get blockchain database. Node will keep on maintaining database until its smart contact is revoked.

Algorithm 1: Adding and deleting Blockchain

Step1:

$$G_n \rightarrow C$$

$$if\ (G_n == Business\ Rules)$$

$$\{\quad Accepted(G_n)$$

$$Acknowledge(G_n)$$

$$Go\ to\ step2\quad \}$$

$$Else\ \{$$

$$Reject\ and\ Acknowledge(G_n)\quad \}$$

Step2:

$$Add\ (G_n)$$

$$Create\ S_m(G_n) \rightarrow B_1$$

Step3:

$$G_n \rightarrow Request\ for\ D_b \rightarrow B_1$$

Step4:

$$Bool\ Result = B_1\_authentication(S_{m_{G_n}})$$

$$if\ (Result == 1)$$

$$\{\quad Share\ D_B(G_n)$$

$$Loop\ until\ D_B\ shared\quad \}$$

$$Else\ \{\quad Reject\_Request(G_n)$$

$$Go\ to\ step\ 5;\quad \}$$

Step5: $Finish();$

3.2 Save and exchange information

DDos and its after-effect on the network is the main focus of our system. So, we have to secure SDN and NFV from illegal modification. The modification is referred as "configuration update." Any change made by cloud is a transaction and recorded in the ledger according to the smart contract. Figure 4 shows the activities carried out to add a node in a blockchain and how it is going to share database across the blockchain.

Algorithm 2: Fog nodes on special duties

Step1:

$$C_1, C_2 \in C_n$$

$$Initial\ hand\ shake\ between\ C_1 \& C_2$$

Step2:

$$Create\ S_m(C_1, C_2) \rightarrow C_1\_S_m, C_2\_S_m$$

$$Share\ S_m(C_1, C_2)$$

Step3:

$$if\ (C_1\_S_m == C_2\_S_m)$$

$$\{$$

$$Calculate\ F_n\ Probability()$$

$$F_n \rightarrow B_1 \quad \}$$

Step4:

$$Create\ S_m(F_n\_S\_C_1C_2)$$

Step 5:

$$Share\ (F_n\_S\_C_1C_2)\ to\ involved\ parties$$

$$if\ (F_n\_S\_C_1C_2\ \ is\ not\ revoked)$$

$$\{$$

$$F_n\ Start\ sharing\ \ B_1 \qquad \}$$

Else

$$\{ \quad Go\ to\ step\ 6$$

$$\}$$

Step 6: $Finish();$

3.3 Fog node on special duty

We introduce a new term "Fog node on special duty." This node is vital if different types of fog need to increase their security. Fog can provide these services. We consider certain parameters like bandwidth, power, and storage capacity to select a special node. To do this, new algorithm is required that can choose the special node, create new smart contract on which both parties can agree and work accordingly to secure each other's assets. This ensures more security as now two clouds can work together to keep their commodities safe. This also fulfill the chaining property of blockchain.

3.4 FNOSD selection

$$\begin{aligned} P(X = x \ \text{ and } Y = y) &= P(Y = y|X = x) \cdot P(X = x) \\ &= P(X = x|Y = y) \cdot P(Y = y) \end{aligned} \tag{1}$$

where $P(Y = y|X = x)$ is the probability of $Y = y$ given that $X = x$.

The generalization of the previous two variable cases is the joint probability distribution of n discrete random variables $k_1, k_2, k_3, \ldots\ldots\ldots, k_n$

$$\begin{aligned} P = (X_1 = k_1, X_2 = k_2, \ldots, X_n = k_n) &= P(X_1 = k_1) \\ &\times P(X_2 = k_2|X_1 = k_1) \times P(X_3 = k_3|X_1 = k_1, X_2 = k_2) \\ &\times P(X_n = k_n|X_1 = k_1, X_2 = k_2, \ldots, X_{n-1} = k_{n-1}) \end{aligned}$$

$$N = \{k_1, k_2, k_3, \ldots, k_n\}$$

where $k_n \in N$ is the finite number of nodes in a fog

Each of the node in N has either computational power, storage capacity, or both according to the usage of the nodes.

S_c = storage capacity & C_p = computational power

$S_c = \{0, 1\},\ C_p = \{0, 1\}$ are the states of each node

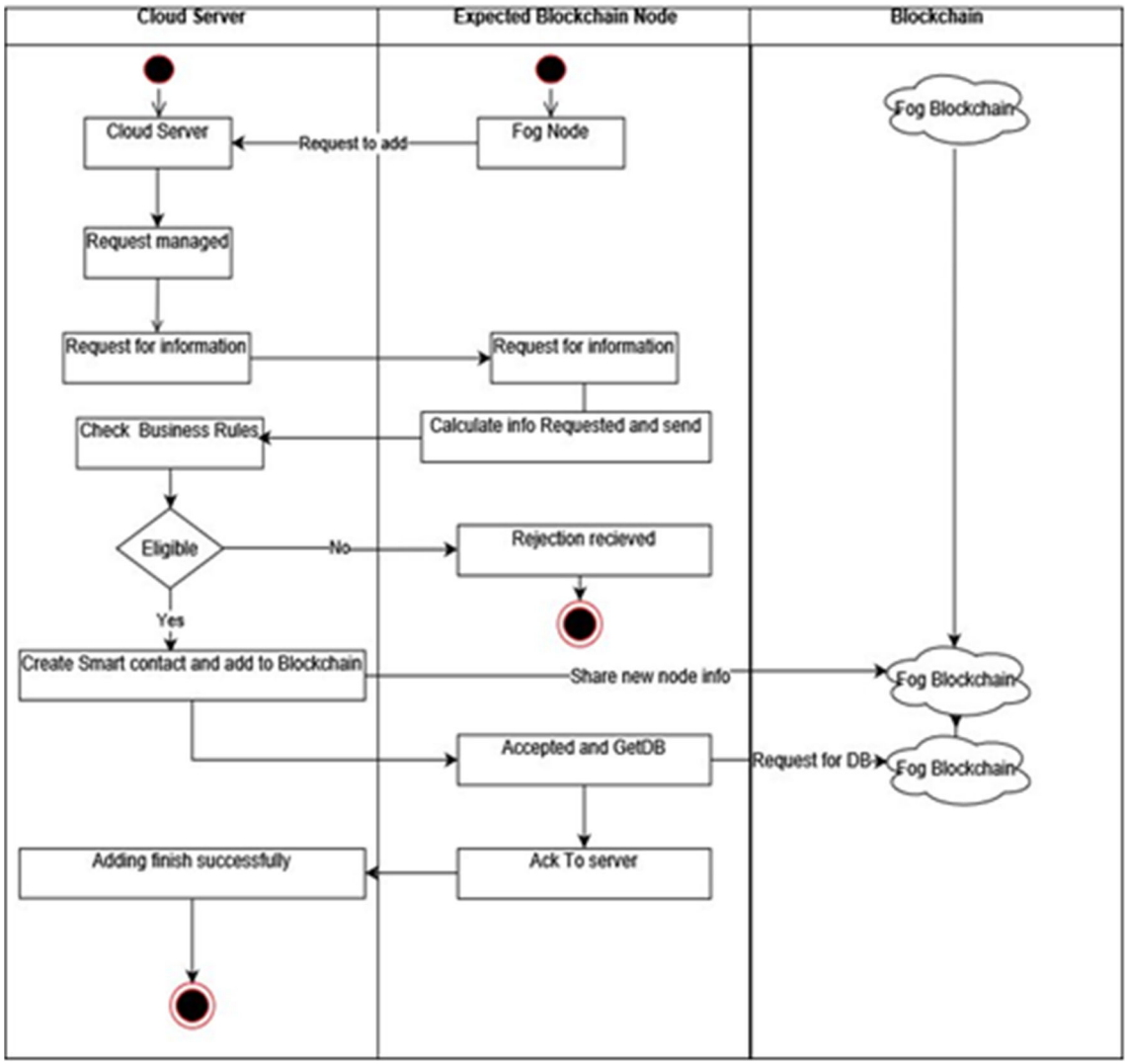

Fig. 4 Activity diagram

Some nodes can have both qualities (i.e., storage capacity and computational power) and either.

Suppose

$$S_c = \begin{cases} 1, & \text{if } k_n \text{ has Storage capacity} \\ 0 & \text{Otherwise} \end{cases}$$

$$C_p = \begin{cases} 1, & \text{if } k_n \text{ has Computational power} \\ 0 & \text{Otherwise} \end{cases}$$

$$f_N(k) = \begin{cases} \frac{k_{Sc,cp=1}}{N} & if\ S_c, C_p = 1 \\ \frac{k_{Sc,cp=0}}{N} & if\ S_c, C_E = 0 \\ 1 - \frac{k_{Sc,cp=0}}{N} - \frac{k_{Sc,cp=1}}{N} & \text{otherwise} \end{cases} \quad (2)$$

$$P(\text{not chosen}) = \left(S_c = 0, C_p = 0\right) = \frac{k_{Sc,cp=0}}{N} \quad (3)$$

$$P(\text{others}) = \left(S_c = 0, C_p = 1 \text{ or } S_c = 1, C_p = 0\right) = \frac{k_{Sc,cp=0,1}}{N} \quad (4)$$

$$P(\text{exp .candidate}) = \left(S_c = 1, C_p = 1\right) = \frac{k_{Sc,cp=1}}{N} \quad (5)$$

$$P(\text{not candidate}) = P(\text{not chosen}) + P(\text{others}) = \frac{k_{Sc,cp=0}}{N} + \frac{k_{Sc,cp=0,1}}{N} \text{ or } = 1 - \frac{k_{Sc,cp=1}}{N} \quad (6)$$

Probability of choosing cluster head among the nodes which are expected candidates.

$$P(c.h = k_i) = \frac{k_{Sc,cp=1}}{N} \quad (7)$$

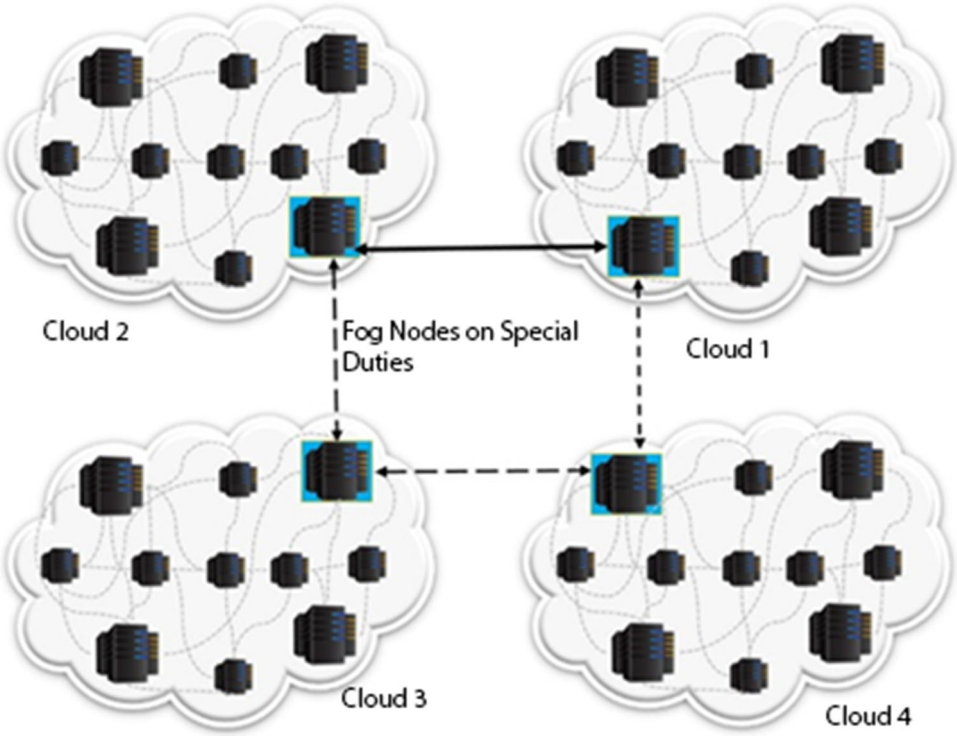

Fig. 5 Fog nodes on special duty

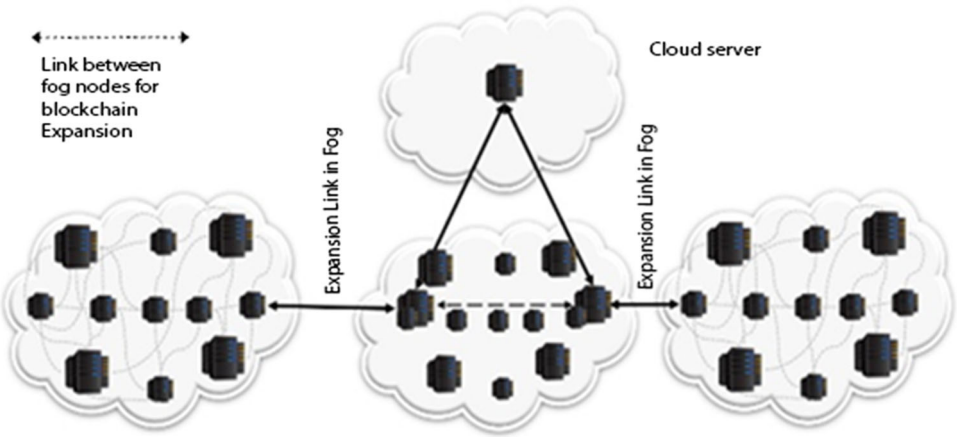

Fig. 6 Alternate blockchain route between clouds

Parameters	Nodes					
	k_1	k_2	k_3	k_4	$,\ldots,$	k_n
S_c	0	1	0	1		1
C_p	1	0	0	1		0

The probability of the next cluster head will be calculated by the following equation

$$P(c.h = k_i | c.h = k_{i-1}) = \frac{(k_{Sc,cp=1}) - 1}{N - 1}$$

$$P(c.h = k_{i-1} \cap c.h = k_i) = (P(c.h = k_i) \times P(c.h = k_i | c.h = k_{i-1}) = \frac{k_{Sc,cp=1}}{N} \times \frac{(k_{Sc,cp=1}) - 1}{N - 1} \quad (8)$$

$$P(ch) = \sum_n P\left(k_{Sc,cp=1} \cap \left(N - k_{Sc,cp=1}\right)\right)_n = \sum_n P\left(k_{Sc,cp=1} | \left(N - k_{Sc,cp=1}\right)_n\right) P\left(\left(N - k_{Sc,cp=1}\right)_n\right) \quad (9)$$

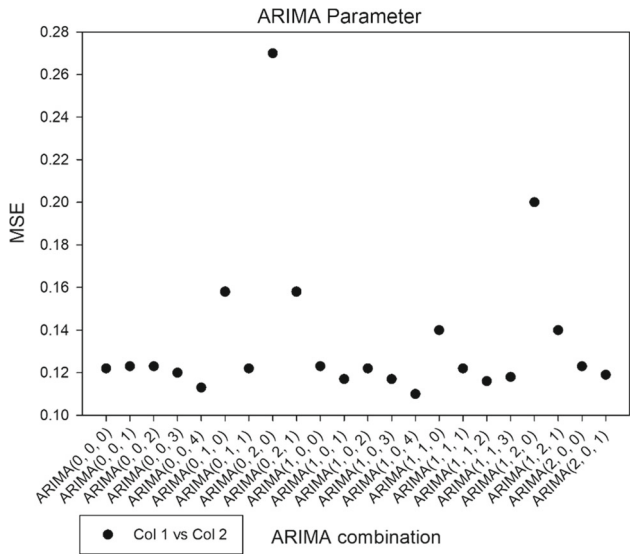

Fig. 7 ARIMA parameter combination

3.5 Blockchain expansion algorithm between clouds

Blockchain expansion mechanism or algorithm is required for the scenario where two or more cloud service providers want to expand their blockchain services to increase their security. In such scenario, one of the clouds has blockchain database from other parties. If we make new connection between other clouds individually, it will be waste of resources. So, efficient connection is required. Expansion algorithm checks if connection can be made within the fog which have databases of other parties. Once fog node on special duty are located, it provides cloud service which will enable a link between cloud without extra connection (Figs. 5, 6, 7).

4 Simulation results

For choosing our Fog node on special duty, we have collected performance dataset. Parameters we choose were processor information, average diskwrite, free disk in

Number of occurrence	S_c	$\overline{S_c}$	Sum
C_p	$k_{Sc=1,cp=1}$	$k_{Sc=0,cp=1}$	$k_{Sc=1,cp=1} + k_{Sc=0,cp=1}$
$\overline{C_p}$	$k_{Sc=1,cp=0}$	$k_{Sc=0,cp=0}$	$k_{Sc=1,cp=0} + k_{Sc=0,cp=0}$
Sum	$k_{Sc=1,cp=1} + k_{Sc=1,cp=0}$	$k_{Sc=0,cp=1} + k_{Sc=0,cp=0}$	N

Algorithm 3: Blockchain Expansion algorithm between clouds

Step1:

$$Intial\ hand\ shake\ between\ C_1, C_2, C_3$$

$$C_1, C_2, C_3 \in C_n$$

Step2:

$$Check\ if\ (C_1, C_2, C_3\ already\ have\ sum$$

$$\{$$

$$Go\ to\ step\ 3$$

$$\}$$

Else

$$\{$$

$$Create\ S_m(Accordingly\ for\ C_n$$

$$\}$$

Step3:

$$Get\ Cluster\ head\ from\ Algorithm\ probability()$$

Step4:

$$Share\ S_m\ with\ F \in G_{B(1,2)}\ \&\ F \in G_{B(2,3)}$$

Step5:

$$Create\ B_1(G_{B(1,2,3)})$$

$$Share\ D_B\ (S_m\_C_{(1,2,3)})$$

Step6:

$$Do\ until\ S_m\_C_{(1,2,3)}\ \ is\ \ revoked)$$

$$Finish()$$

MegaByte, etc. Data were collected from our laboratory server with Microsoft built-in tool named as "Resource Monitor" (Table 1).

From this dataset, we predict the performance of the server with respect to processor usage. This information is vital while choosing fog node on special duty. As we do not want to choose the server which is under stress. For our time series experiment, we consider autoregressive integrated moving average (ARIMA) model for forecasting. ARIMA model is used to forecast time series data. ARIMA model consists of three notions (1) AR which uses the relationship between lagged observation and the actual observation, (2) in ARIMA "I" stands for "Integrated" which uses the differencing method to make time series stationary, and (3) MA is moving average which uses dependency between the residual error and the observation.

Table 1 Dataset statistics

Statistic	value
Minimum	31.258
Maximum	95.233
Mean	40.667
SD	7.394

We have test ARIMA with ARIMA (1,1,2) combination which gave us some promising results.

Our ARIMA simulation for processor usage has 0.013 in the MSE test with parameter of ARIMA set to (1,1,2). AR = 1 is for autoregressive, I = 1 for integrated, and MA = 2. In Fig. 8, blue line is observations and red line is predicted values.

Figure 9 shows one step ahead predicted value for the processor with the unit of "%" percentage. y-axis shows percentage usage of processor and *x*-axis shows time in minutes.

To check the status of our blockchain, we made changes to the configuration file and save it to database. Some of the transaction made were validated, and some were not validated. It will show us the working of simulation, because if

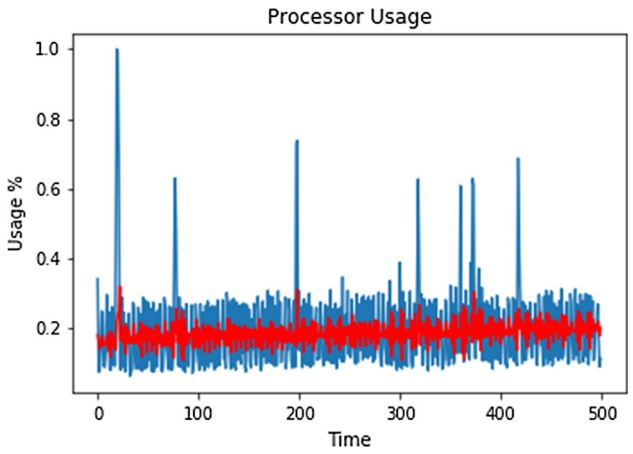

Fig. 8 Processor data ARIMA prediction

validation is not done then blockchain status should be false otherwise true. To generate our results with blockchain, we build a small blockchain with C# having simple structure basic blockchain properties. Our coded blockchain was able to detect any changes made in the data. If data are not validated, the whole chain shows false result and true if data are validated as shown in Fig. 10.

While securing the assets (NFV configuration files), any property of NFV is not changed. Configuration files from NFV are hashed after modification and forward information to validator. With validation, blockchain status will remain false. Likewise, blockchain is not directly injected to the architecture, so property of blockchain remains unchanged (Table 2).

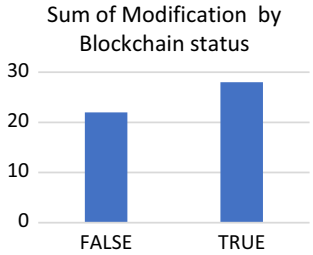

Fig. 10 Modification and validation results

Table 2 Sum of modification recorded while modifying config file

Blockchain status	Sum of modification
False	22
True	28

5 Conclusions

Blockchain in fog architecture along with SDN and NFV proves to be very secure, also, because fog architecture property response time is very low. This means localizing DDoS attack while maintaining the security with provided architecture is up to the mark. The expansion algorithm opens the ways to create better and secure blockchain while using fog architecture. As 5G proves to be faster than 4G because of SDN and NFV, this concludes that provided framework is not only fast but because of blockchain it is more secure and easy to maintain. Algorithms make sure expandability of blockchain which means more security. It is also very difficult to hack certain cloud and fog node to manipulate certain configurations. Choosing proper cluster head and providing right services open new ways for organization to deploy blockchain and provide services of blockchain to other companies.

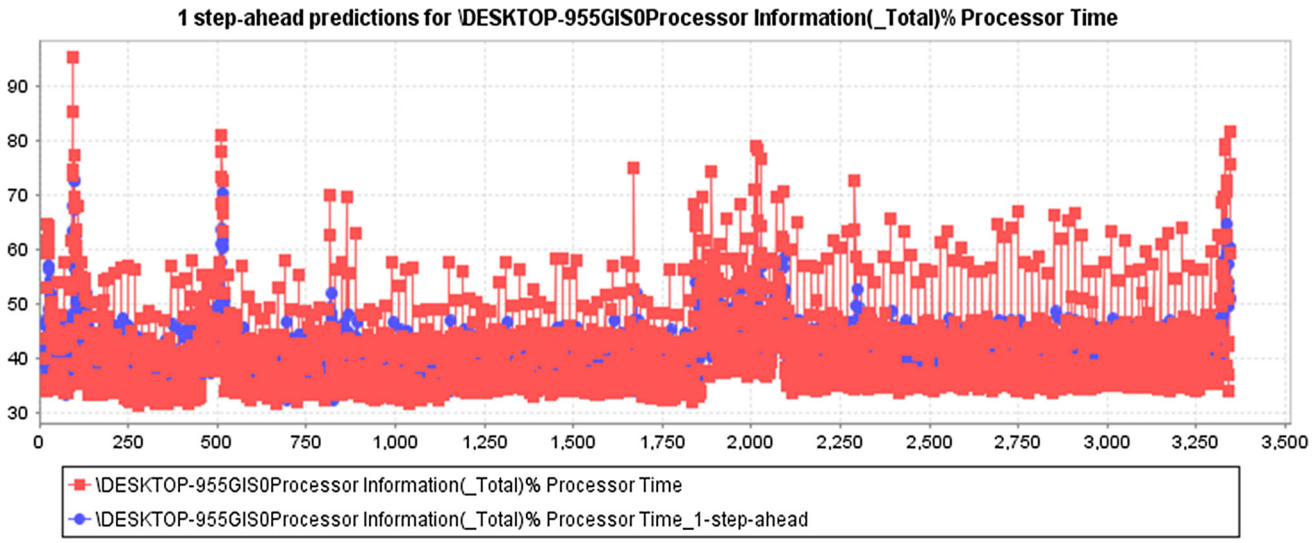

Fig. 9 Processor prediction one step ahead

Acknowledgement This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A1A09919551).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflicts of interest.

References

Agiwal M, Roy A, Saxena N (2016) Next generation 5G Wireless Networks: A Comprehensive Survey. IEEE Commun. Surv. Tutorials. https://doi.org/10.1109/COMST.2016.2532458

Ahmed E, Yaqoob I, Hashem IAT, Khan I, Ahmed AIA, Imran M, Vasilakos AV (2017) The role of big data analytics in internet of things. Comput Netw 129:459–471. https://doi.org/10.1016/j.comnet.2017.06.013

Alavian SA, Chimeh JD (2009) Mobile systems challenges in next generation networks. Int J Futur Gener Commun Netw 1: 15–22. https://www.sersc.org/journals/IJFGCN/vol1_no1/papers/03.pdf

Arasteh H, Hosseinnezhad V, Loia V, Tommasetti A, Troisi O, Shafie-khah M, Siano P (2016) IoT-based smart cities: a survey iot-based smart cities: a survey. In: 2016 IEEE 16th international conference on environment and electrical engineering (EEEIC), pp 2–7. doi:10.1109/EEEIC.2016.7555867

Cardenas AA, Manadhata PK, Rajan SP (2013) Big data analytics for security. IEEE Secur. Priv. 11:74–76. https://doi.org/10.1109/MSP.2013.138

Frustaci M, Pace P, Aloi G, Fortino G (2017) Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2017.2767291

Gódor G, Jakó Z, Knapp Á, Imre S (2015) A survey of handover management in LTE-based multi-tier femtocell networks: Requirements, challenges and solutions. Comput Netw 76:17–41. https://doi.org/10.1016/j.comnet.2014.10.016

Gul J, Mushtaq S, Riaz R (2012) Optimal guard node placement using SGLD and energy factor. J Comput 4:87–92

Gupta B, Agrawal DP, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global, Pennsylvania

Gupta BB, Perez GM, Agrawal DP, Gupta D (2019) Handbook of computer networks and cyber security: principles and paradigms. Springer, Berlin. https://www.springer.com/gp/book/9783030222765. Accessed August 19, 2019

Kambourakis G, Kolias C, Stavrou A (2017) The Mirai botnet and the IoT Zombie Armies. In: Proceeding of the IEEE military communication conference MILCOM, 2017, pp 267–272. doi:10.1109/MILCOM.2017.8170867.

Kim J, Kim D, Choi S (2017) 3GPP SA2 architecture and functions for 5G mobile communication system. ICT Express 3:1–8. https://doi.org/10.1016/j.icte.2017.03.007

Kolias C, Kambourakis G, Stavrou A, Voas J (2017) DDoS in the IoT: Mirai and other botnets. Computer (Long Beach Calif). 50:80–84. https://doi.org/10.1109/MC.2017.201

Lee I, Lee K (2015) The internet of things (IoT): applications, investments, and challenges for enterprises. Bus Horiz 58:431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lytras MD, Al-Halabi W, Zhang JX, Haraty RA, Masud M (2015) Enabling technologies and business infrastructures for next generation social media: Big data, cloud computing, internet of things and virtual reality. J Univers Comput Sci 21:1379–1384

Marjani M, Nasaruddin F, Gani A, Karim A, Hashem IAT, Siddiqa A, Yaqoob I (2017) Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access 5:5247–5261. https://doi.org/10.1109/ACCESS.2017.2689040

Mourtzis D, Vlachou E, Milas N (2016) Industrial big data as a result of IoT adoption in manufacturing. In: Procedia CIRP, 2016: pp 290–295. doi:10.1016/j.procir.2016.07.038.

Neupane RL, Neely T, Chettri N, Vassell M, Zhang Y, Calyam P, Durairajan R (2018) Dolus: cyber defense using pretense against DDoS attacks in cloud platforms. In: ACM international conference on proceeding series Part F1331 (2018). doi:10.1145/3154273.3154346.

Olakanmi OO, Dada A (2019) an efficient privacy-preserving approach for secure verifiable outsourced computing on untrusted platforms. Int J Cloud Appl Comput 9:79–98. https://doi.org/10.4018/ijcac.2019040105

Osanaiye O, Choo KKR, Dlodlo M (2016) Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. J Netw Comput Appl 67:147–165. https://doi.org/10.1016/j.jnca.2016.01.001

Ouaguid A, Abghour N, Ouzzif M (2018) A novel security framework for managing android permissions using blockchain technology. Int J Cloud Appl Comput 8:55–79. https://doi.org/10.4018/IJCAC.2018010103

Pacheco J, Hariri S (2016) IoT security framework for smart cyber infrastructures. In: Proceeding of the IEEE 1st international workshops on foundations and applications of self-systems, FAS-W 2016, 2016, pp 242–247. doi:10.1109/FAS-W.2016.58.

Saeed F, Paul A, Rehman A, Hong W, Seo H (2018) IoT-based intelligent modeling of smart home environment for fire prevention and safety. J Sens Actuator Netw 7:11. https://doi.org/10.3390/jsan7010011

Somani G, Gaur MS, Sanghi D, Conti M, Buyya R (2017) DDoS attacks in cloud computing: issues, taxonomy, and future directions. Comput Commun 107:30–48. https://doi.org/10.1016/j.comcom.2017.03.010

Stergiou C, Psannis KE, Gupta BB, Ishibashi Y (2018) Security, privacy and efficiency of sustainable cloud computing for big data & IoT. Sustain Comput Informatics Syst 19:174–184. https://doi.org/10.1016/J.SUSCOM.2018.06.003

Tweneboah-Koduah S, Skouby KE, Tadayoni R (2017) Cyber security threats to IoT applications and service domains. Wirel Pers Commun 95:169–185. https://doi.org/10.1007/s11277-017-4434-6

Wang P, Valerdi R, Zhou S, Li L (2015) Introduction: Advances in IoT research and applications. Inf Syst Front 17:239–241. https://doi.org/10.1007/s10796-015-9549-2

Wang Y, de Almeida Correia GH, van Arem B, Timmermans HJP (2018) Understanding travellers' preferences for different types of trip destination based on mobile internet usage data. Transp. Res. Part C Emerg. Technol. 90:247–259. https://doi.org/10.1016/J.TRC.2018.03.009

Xu X, Zhang H, Dai X, Hou Y, Tao X, Zhang P (2014) SDN based next generation mobile network with service slicing and trials. China Commun 11:65–77. https://doi.org/10.1109/CC.2014.6821738

Zand A, Modelo-Howard G, Tongaonkar A, Lee SJ, Kruegel C, Vigna G (2017) Demystifying DDoS as a service. IEEE Commun Mag 55:14–21. https://doi.org/10.1109/MCOM.2017.1600980

Zhu S, Han Y (2018) Secure data outsourcing scheme in cloud computing with attribute-based encryption. Int J High Perform Comput Netw 12:128. https://doi.org/10.1504/IJHPCN.2018.094363