ISSN 2278-3091
Volume 9, No.1, January – February 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse37912020.pdf
https://doi.org/10.30534/ijatcse/2020/37912020

Security of Data Access in Fog Computing using Location-based Authentication

Ahmad K. Al Hwaitat[1] , Mais Haj Qasem[2] ,Rim A. Fabozzi[3]
[1]The University of Jordan , Department of Computer Science, Jordan, Ahmad.Hwaitat1@gmail.com , ahm9160118@ju.edu.jo
[2]The University of Jordan , Department of Computer Science, mais_hajqasem@hotmail.com
[3]The University of San Diego , Department of Cyber Security and leadership, Rfabozzi@icloud.com

ABSTRACT

Many organizations, such as military, financial, and banking organizations, implement strict security policies for securing and protecting data from any possible attack. Moreover, these institutions use the Internet of things (IoT) and fog computing for communication and storage that require new solutions to confirming the login process between the two techniques. A methodology for increasing the security for fog computing is proposed in this research. The proposed methodology provides authentication that is based on the location of the device that will perform fog computing during communication, thereby ensuring the secure login to data and legal verification. Furthermore, the proposed methodology is simulated using the LabVIEW simulator with different case studies. Results show that location-based authentication increases authentication confidence and security.

Key words: Internet of things , Fog computing , Authentication ,Location Based , Security.

1.INTRODUCTION

Internet of things (IoT) is a concept and paradigm of the ubiquitous presence of different physical objects ("things") in the environment. The term "Internet of things" refers to a dynamic global network infrastructure that can perform self-tuning on the basis of standard and compatible communication protocols; in these protocols, physical and virtual "things" have identifiers, physical attributes, and intelligent interface uses and can integrate with an information network [1].

The IoT concept includes many personal technologies, services, and standards and perceives the cornerstone of the information market. Information communication technologies (ICTs) are forecasted to be at the edge of the for at least the next 10 years. From a logical perspective, the IoT system can be represented as a combination of and intelligent devices. From a technical perspective, the IoT can be used in different ways of data processing and communication technologies and methodologies in accordance with a purpose [2]

The term “fog computing” was introduced as a new model that can facilitate wireless data transfer to distributed devices in the IoT network paradigm. Fog computing is a new platform that extends the cloud computing paradigm to the edge of the network[3], that is, the entry point to the core network [25].

Fog computing provides an additional advantage given its proximity to customers, dense geographic coverages, and mobility supports, although IoT and fog computing provide a similar set of services in terms of computation and storage [4]. The fundamental element of the fog computing architecture is called a “fog node,” which is the extra layer between an IoT device/data generating node and a remote cloud server. These fog nodes are used to accelerate time-critical applications. Services are hosted away from the cloud, close to the devices, and at the fog node devices, such as routers, set-up-boxes, or access points. Data generator nodes, which are typically sensor nodes, generate data. The data from the data generator nodes proceed to the cloud via intermediate fog node(s) [25], and users can access the data from the fog nodes rather than from the cloud [5].
We must prevent unauthorized users, that is, people and systems must be authenticated for security, confidentiality, and integrity of personal data, to secure the access to IoT devices. In terms of personal user data and information, protection and confidentiality are crucial primarily because devices can access and can manage these data and information (for example, information on the habits of users) [6] . Authentication verifies a claim. Identity authentication verifies the claim of a user as the owner of a given identity, and proximity authentication verifies the claim that two given devices are proximate. Authentication is a fundamentally important security mechanism that provides a security base for many security applications. In particular, many security applications grant user services or privileges on the basis of the authentication result. For example, identity authentication helps applications recognize users to provide personalized services. Therefore,

authentication is the first step to service access. Many applications reject providing services when authentication fails [7] [26] . IoT devices require user authentication. If the user is not an expected user, then the IoT device will not allow the user to access computing. Therefore, authentication is an important security mechanism [8] [25].
Therefore, protecting the IoT against unauthorized usage is significant in safeguarding user privacy and network security. An IoT device can alert the owner and lock itself when unauthorized usage is detected, thereby inhibiting most IoT device thefts [9] [22]. In preventing the unauthorized usage of IoT devices, a location-based authentication system is more suitable than a user authentication system. A user authentication system verifies a user once during login to access fog computing [10].

The capabilities of hackers are continuously increasing. In the traditional adversary model, attackers can monitor/record the communication, modify the transmitted messages, and initiate authentication requests to the server or forge a response to the authentication request from a legitimate user. Attackers can execute more than those prescribed in the traditional adversary model with the rapid development of computer and electronics technologies. Thus, we use the term "strong adversary model" to reflect the evolving capabilities of computer hackers. In the strong adversary model, attackers can compromise the security features [11]. A location-based authentication system is aimed at continuously authenticating the current user during the entire system execution. In the absence of location-based authentication, an attacker can easily access a system. An attacker can log in to the system even if the system uses a username and password. The location-based authentication system invokes an authentication system that requires the location of the computer before authorizing a log in.

2. RELATED WORK

Communications security (COMSEC) refers to preventing unauthorized process to verified telecommunications traffic or to any written information that is transmitted or transferred from the sender, whereas the IoT is a computing concept that describes the connection of physical objects to the Internet and their capability to identify themselves to other connected devices [12],Fog computing is an alternative to cloud computing that places several types of transactions and certain resources at the edge of a network, rather than deterring channels for cloud capacity and utilization [13] ,A dual-encryption system is based on authenticating the server to provide high-performance security to existing fuzzy keyword-searching concepts. In the present research, we integrate symmetric and asymmetric encryption algorithms to enhance data security [14].

An unauthorized person is any person who is prohibited to access specific information. An individual is unauthorized to process classified information of any

Table 1::Comparison Related works of Authentication Fog Computing

Methods / Authors	Secure communication	Fog computing	IOT	Dual encryption	Unauthorized person	Authentication	Master secret key	Validation of location	User level	IDS	Monitor user behavior
[19]	√	√	√						√		
[15]		√	√	√	√	√			√		
[21]	√	√	√	√					√		
[8]		√	√			√	√		√		
[17]		√	√						√	√	
[18]		√	√			√			√		√
[7]	√	√	√			√			√		
[20]	√		√			√					

degree without a determined need-to-know depending on the degree of clearance [15] ,Authentication in the context of computer systems is a process that ensures and confirms the

identity classes of a user. Authentication is a pillar of information assurance (IA). The four other pillars are integrity, availability, confidentiality, and non-repudiation [12] .A security key is generated by the main secret server when an enterprise single sign-on (SSO) monitor requests for this key. This secret key is stored in the registry as a local security authority (LSA) secret on the main secret server. Only SSO administrators may access the secret key [8].

User-level security in the context of Microsoft Access is a fine-grained level of restrictions and permissions to users of a database. User-level security allows the database administrator to group users with the same requirements into common pools called workgroups. Permissions may then be granted to workgroups rather than individual users, to facilitate the administration of permissions. Two default groups, namely, admin and user groups, are provided with permissions [16]. Intrusion detection system (IDS) is a kind of security software that is designed to automatically alert administrators when an individual or a program is attempting to compromise the information system by malicious activities or by security policy violations [27] [17],User behavior monitoring is focused on behavioral monitoring at the user level and rapidly responds to abnormal behavior [18] [29].

[19] proposed a basic monitoring that focuses on overcoming the security problems encountered through data outsourcing from a fog client to a fog machine. These authors added Shibboleth, which is a security and cross-domain access control protocol between the fog client and the fog machine, to improve and verify the secure communication between them.

[15] proposed the dual encryption of data by using the emoticon technique that compared cryptography and steganography. In this method, data are first encrypted between fog computing and low level. Then, the encrypted data, such as emoticons, are hidden with a cover text. Dual encryption enhances the data security and reliability. If the cover text is accessed by unauthorized users, then only the encrypted data can be viewed and not the real data.

[21] implemented the idea of process encryption by using an AES algorithm for checking its functions for fog computing. The AES algorithm is the most secured process of encryption.

[8] proposed a secure and efficient mutual authentication concept for an edge-fog-cloud network architecture to mutually authenticate fog client computing at the edge of the network, with the fog servers at the fog layer. This author required a client in the network to hold only one long-term master secret key, which allows verifying a communication with any client in the fog server of the network, with a fully authenticated direction [24].

[16] presented new distribution and lightweight IDS-based ideas on an artificial immune system. The IDS is distributed in a three-layered IoT structure, including the cloud, fog, and edge layers. In the cloud layer, the IDS clusters and trains the detected primary network traffic. In the fog layer, the authors exploit a smart data concept to analyze the intrusion alerts. In the edge layer, the authors deploy the detection of edge devices. Smart data are promising approaches to enabling lightweight and efficient intrusion detection, thereby providing a path for detecting silent attacks, such as botnet attacks in the IoT-based systems.

[18] proposed to monitor client behavior or data access patterns in the cloud systems and identified abnormal data access patterns. If an unauthorized data access pattern is suspected, then decoy data are provided to the unauthorized client. This mechanism ensures the protection against misusing real client data. In this case, if the real client is trapped in this system, the client must be challenged by the system through a one-time password for verification.

[7] focused on security considerations for IoT from the perspectives of cloud tenants, end-users, and cloud providers in the context of extensive IoT proliferation that is effective across the range of IoT technologies (whether things or the entire IoT subsystems). Our goal is to analyze the current state of cloud-supported IoT to generate explicit security considerations [23].

[21] described multi-factor authentication (MFA) systems, which are inapplicable to the field of IoT but provides extensive security to user credentials. The MFA system is followed by a brief description of the working mechanism of interaction of third-party clients with private resources over the OAuth protocol framework and a study of the delegation-based authentication system in an IP-based IoT [21].

We observe several of the mechanisms of security and authentication between fog computing and low-level users and focus on the validation mechanism of the location in the security between fog computing and low-level users [28].

The protection from all measures is designed to deny unauthorized persons from accessing valuable information that

could be derived from possessing and studying telecommunications or mislead unauthorized persons in interpreting the results of certain possession and study. This system is called Location-based Authentication, which includes transmission, emission, and physical securities of communication materials and information.

3.PROPOSED METHOD

We assume that our methodology will be implemented in every organization in the communication of fog computing systems, that each device has a GPS to determine its location, and that the devices in the login system are heterogeneous. The proposed methodology should be implemented in conjunction with other security services, such as encryption of data and session. Our methodology does not cancel other methods, such as encryption of data, but adds new factors, such as location-based authentication. We assume that all devices are connected to fog computing and require authentication to log in to the fog system. We assume that the implemented system will work in the application layer, as illustrated in figure 1 In the user side, the user logs in through the browser and enters the required username and password to access the fog computing. At the fog side, the proposed methodology in the application layer of fog computing decides and replies to the user with either an authorized or blocked access.

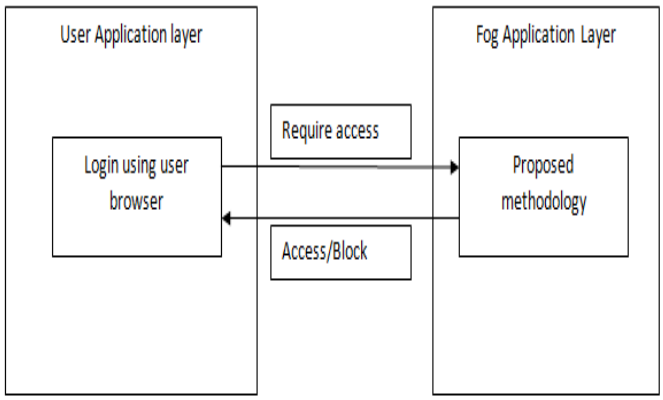

Figure 1: login authentication is required to access fog computing .

A secure system for login authentication is required to access fog computing, and security can be strengthened by adding a location factor to the login process. Thus, in this research, we add a location to the fog login factor to increase the access security. The proposed methodology is represented by a set of steps, which are depicted in figure 2. The first step involves logging in to the fog through the username and password that is unique for each employee who has access to the system. In the first step, a decision is made after comparing the password and username with those stored in the database, which contains all usernames and passwords. If the password does not match any of the stored passwords for a specific user, then the user is allowed to retry a specific number of attempts. The user is temporarily blocked after a certain number of failed login attempts, and details of the login attempts will be stored in a log file, including the IP address, time and date, the type of operation (login failed), and the decision taken (block). In the case of a successful login, the user is authorized to access the fog.

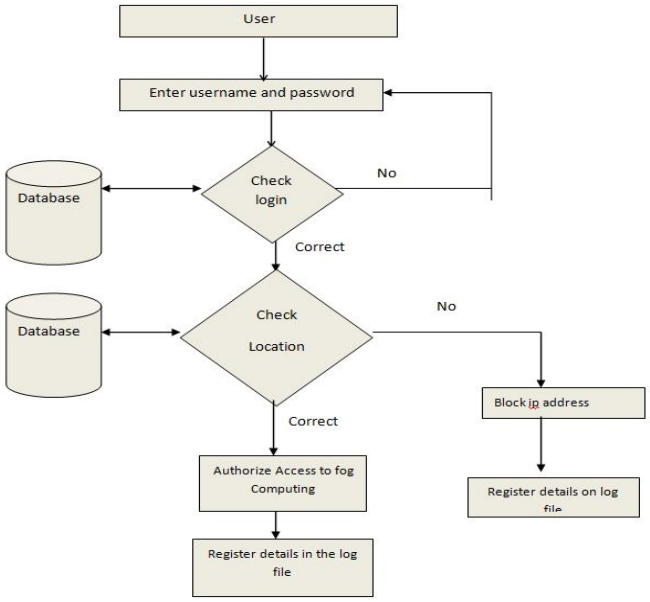

Figure 2: Proposed Methodology

In the second step, the location of the accessed device will be checked by comparing it with the database that contains the location coordinates (Latitude and longitude) of the devices that can access the fog. Furthermore, every username and password correspond to a device location. If the accessed device location is the same as the one stored in the database, then the access to the device is authorized. If the location is different from the location stored in the database, then the access from this device at the specified location is blocked. Subsequently, the details of the illegal access are stored in the log file, including the IP address, time and date, the type of operation (login failed), the decision taken (block), and the location of the user). If the location of the user matches the location that is stored in the database, then the access to the fog is authorized, and the details of the successful login are stored in the log file.

The location-based authentication in fog computing addresses the breach that may occur because of stolen passwords that are used at different locations to access the fog from outside the

organization. Furthermore, we confirm the user identity by matching the stored location with the location where the user is accessing from. The breach is handled by storing the location and details of the illegal access in a log file.

4. EVALUATION THROUGH A CASE STUDY

This section examines the results of the simulation through the proposed methodology. The simulation is performed using the LabVIEW simulator. The evaluation is conducted by creating different network scenarios.

LabVIEW offers a graphical programming approach for a visual representation of our application, including the hardware configuration, measurement data, and debugging. These visualizations can be simplified to integrate measurement hardware from any users, represent complex logic on the diagram and experiments, develop data analysis algorithms, design custom engineering client interfaces, and devise distributed tests, measurements, and control systems, thereby reducing the consumed time. These visualizations can be combined with verified, standard, customizable hardware, which has been used by engineers for over 30 years, from NI to develop and deploy traditional large-scale industrial and production systems and experiments.

4.1 Case Study

In this case study, we assume that four devices (PC1–PC4) are connected to the fog, and every device has a PC1 Mac address, an IP address, and a location, as listed in Table 2.

Table 2: Specifications and details PC .

	Mac address	IP address	Location	
			Lat	Lon
	15222223425	255.255.255.425	425	11
	7412345750	255.255.255.750	750	244
	15EF486438	255.255.255.438	438	510
	1314151100	255.255.255.100	100	233

Figure 3: demonstrates the distribution of the PCs that are connected to the fog in the LabVIEW simulator, and each device has its own information.

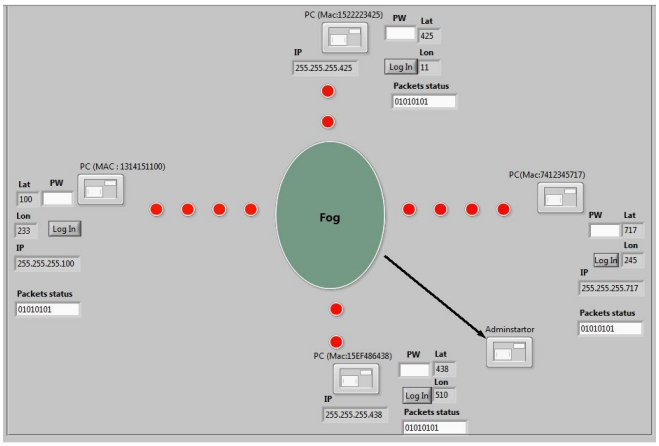

Figure 3::Distribution of the PCs in the LabVIEW simulator

The information on the PCs are stored in the database, and every PC has its own username, password, and location, as exhibited in Figure 4.

```
PC(Mac:1522223425)  ,  PW = 1234  , Lat = 425  , Lon = 11   , ip = 255.255.255.425
PC(Mac:7412345750)  ,  PW = 5678  , Lat = 750  , Lon = 244  , ip = 255.255.255.750
PC(Mac:15EF486438)  ,  PW = 4321  , Lat = 438  , Lon = 510  , ip = 255.255.255.438
PC(MAC:1314151100)  ,  PW = 8765  , Lat = 100  , Lon = 233  , ip = 255.255.255.100
```

Figure 4: Information on the PCs

The proposed methodology installed at the fog will compare the username, password, and location with those stored in the database when PC1 attempts to access the system with the given username and password to send information (username, password, and location) to the fog computing. If the information is correct, then the user is authorized to access the fog. The simulation of the results is presented in Figure 5.

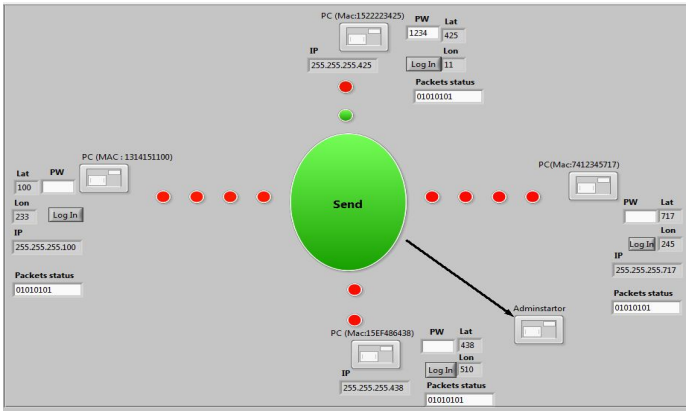

Figure 5: Legal access to fog computing

The log file of the legal access to fog computing is displayed in Figure 6.

Figure 6:: Log file of a legal access to fog computing

In the second scenario, we change the location of the PC (MAC 1522223193). The device obtains a new location in the LabVIEW simulator when the device is moved. The device will also identify the new location with a different MAC address, IP address, and specification after adding a new device. The PC is provided with the correct username and password but a different location. The methodology responds by preventing the access to fog computing and blocking the IP address when it attempts to log in. The results of the simulation are illustrated in Figure 7, and the log file, which contains the IP address, location of the illegal access, time and date, and activity, is depicted in Figure 8.

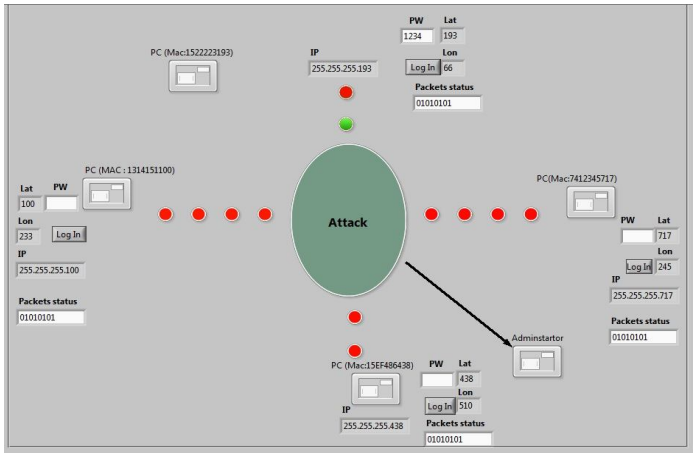

Figure 7 : LabVIEW simulation with illegal access

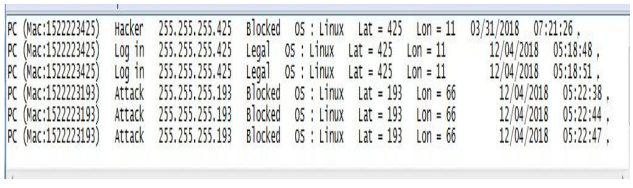

Figure 8 : Log file with illegal access

5. CONCLUSION

In this research, a location-based authentication methodology for accessing fog computing is proposed and described. The proposed methodology provides enhanced protection for authorization and login access to the fog computing using the location information. This methodology improves the verification confidence in accessing fog computing. The methodology is simulated and applied to different case studies. The results show that using location-based authentication for fog computing improves the security of authentication for access to fog computing.

REFERENCES

1. M.Farooq, M. Waseem and S. Mazhar,(2015) , **A Review on Internet of Things (IoT)** , International Journal of Computer Applications, Vol. 113 - No. 1 PP.1-7. https://doi.org/10.5120/19787-1571
2. S. Sicaria ., A. Rizzardia , L.A Griecob , G. Pirob , Coen-Porisinia A. ,(2017) , **A policy enforcement framework for Internet of Things applications in the smart health, Elsevier journal**, Vol. 3 ,No. 4 .pp. 39–74
3. F. Bonomi , P. Milito, P. Natarajan and J. Zhu,(2014) , **Fog Computing: A Platform for Internet of Things and Analytics**, Big Data and Internet of Things: A Roadmap for Smart Environments ,VOl. 546. Springer, Cham , pp. 169-186.
4. A. Munir, P. Kansakar and. S. Khan ,(2017), I**FCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things**, IEEE Consumer Electronics Magazine,vol.4 ,p12-22. https://doi.org/10.1109/MCE.2017.2684981
5. B. Bashari Rad and Shareef A. ,(2017) , **Fog Computing: A Short Review of Concept and Applications**, International Journal of Computer Science and Network Security, VOL.17 No.11, PP.68-74
6. M. Razzaq and M. Qureshi, (2017) , **Security Issues in the Internet of Things (IoT): A Comprehensive Study" , International Journal of Advanced Computer Science and Applications**, Vol. 8, No. 6, PP.383-388.
7. J. Singh , T. Pasquier, J. Bacon , Ko H., and Eyers D. ,(2016) , **Twenty security considerations for cloud-supported Internet of Thing**, IEEE Internet of Things Journal Vol. 3, Issue: 3 .PP.1-16. https://doi.org/10.1109/JIOT.2015.2460333
8. M. Ibrahim , (2016), **Octopus: An Edge-Fog Mutual Authentication Scheme** , International Journal of Network Security, Vol.18, No.6, PP.1089-1101,

9. M. Abomhara and . G. Køien ,(2015), **Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks** , Cyber Secur Journal ,Vol. 4 ,PP. 65-88 .
10. S. Khan, S. Parkinson and Y. Qin, (2017) , **Fog computing security: a review of current applications and security solutions** , Journal of Cloud Computing: Advances, Systems and Applications ,Vol.6, N.19, PP.1-22.
11. M. MUKHERJEE , L. SHU, R. MATAM, L. MAGLARAS, A. FERRAG, N. CHOUDHURY and V. KUMAR,(2017) , **Security and Privacy in Fog Computing: Challenges** , IEEE Access , Vol.5 , PP. 19293-19304. https://doi.org/10.1109/ACCESS.2017.2749422
12. J. Kumar and D. Patel, (2014), **A Survey on Internet of Things: Security and Privacy Issues**, International Journal of Computer Applications Vol 90 , No 11, PP.20-26.
13. K. Fakeeh, (2014), **Privacy and Security Problems in Fog Computing** , Communications on Applied Electronics , Vol.4 ,N.6 PP.1-6. https://doi.org/10.5120/cae2016652088
14. T. Tariq and P. Agarwal, (2017) , **Secure Keyword Search Using Dual Encryption in Cloud: An Approach**. International Journal of Computational Intelligence Research, Vol. 13, N.5, PP. 1271-1281.
15. H. Kumar, S. Shinde and P. Talele, (2017), **Secure Fog Computing System using Emoticon Technique** , International Journal on Recent and Innovation Trends in Computing and Communication ,Vol 5 Issue: 7,PP.801-808.
16. F.Pour, P. Amoli , J. Plosila, T. Hämäläinen and H. Tenhunen, (2016), "An Intrusion Detection System for Fog Computing and IoT based Logistic Systems using a Smart Data Approach", JDCTA (International Journal of Digital Content Technology and its Applications, Vol.10 , NO.5, PP.34–46.
17. F. Hosseinpour, , T. We.sterlund, , Y. Meng, (2016).: **A review on fog computing systems**. 1M. J. Adv. Comput. Technol. 8(5), 48-61 .
18. S Sangle ., R. Deshmukh, R. Ghodake, A. Yadav and J. Musale, (2017) , **Data Security System in Cloud by Using Fog Computing and Data Mining**, International Journal of Advanced Research in Computer Science and Software Engineering , Vol. 7 , No.5 ,PP.88-96.
19. S, Zahra Alam M. and Javaid Q. , (2017) , **Fog Computing Over IoT: A Secure Deployment and Formal Verification**, IEEE Access, Vol.5 , https://doi.org/10.1109/ACCESS.2017.2766180
20. A. Vishwanath , R. Peruri and J. He ,(2016) ,**Security in Fog Computing through Encryption,Information** Technology and Computer Science, 2016, 5, 28-36.
21. T. Borgohain , A. Borgohain and U. Kumar, () , **Authentication Systems in Internet of Things** , Int. J. Advanced Networking and Applications, Vol: 6,No. 4, PP. 2422-2426.
22. J. Bhanu1 ,J. Sastry,P.Kumar,B.Sai and K.V.Sowmya,(2019),**Enhancing Performance of IoT Networks through High Performance Computing ,**International Journal of Advanced Trends in Computer Science and Engineering ,Vol.8 ,No.3,PP.432-442. https://doi.org/10.30534/ijatcse/2019/17832019
23. S.Bunawan ,(2019),**Architecture Internet of Things Based on Cluster Housing Security System Using Fog Computing ,** International Journal of Advanced Trends in Computer Science and Engineering ,Vol. 8 ,No.(6),PP.3087-3090 https://doi.org/10.30534/ijatcse/2019/68862019
24. S.Karimunnisa and V. Kompalli ,(2019),**Cloud Computing: Review on Recent Research Progress and Issues** ,International Journal of Advanced Trends in Computer Science and Engineering vol. 8, No. 2,PP.216-223. https://doi.org/10.30534/ijatcse/2019/18822019
25. A. Al Hwaitat, S. Manaseer, &R. Al-Sayyed,. (2019). A Survey of Digital Forensic Methods under Advanced Persistent Threat in Fog Environment, Journal of Theoretical and Applied Information Technology , Vol.97. No 18,PP. 4934-4954.
26. A. Al Hwaitat, S. Manaseer ,(2018), Centralized Web Application Firewall Security System, Modern Applied Science; Vol. 12, No. 10; PP.164-170. https://doi.org/10.5539/mas.v12n10p164
27. A. Al Hwaitat, S. Manaseer and R. Jabri ,(2018) ,**Distributed Detection and prevention of Web Threats in Heterogeneous Environment** , Modern Applied Science; Vol. 12 ,No10 ,PP.13-22. https://doi.org/10.5539/mas.v12n10p13
28. A. Al Hwaitat, S. Manaseer ,(2017), **Validation and Integrity Mechanism for Web Application Security,** International Journal of Engineering Research & Science , Vol. 3, No.11,PP.34-38.
29. O. rababha , A. Al Hwaitat , S. Manasser ,(2016) **Web Threats Detection and Prevention Framework**, communications and Network, Vol. 8, No.8, PP. 170-178. https://doi.org/10.4236/cn.2016.83017