Data and Programming Security Issues in Fog Computing

Pranav Vyas, Dharmendra Patel
CMPICA, Charotar University of Science and Technology
Changa, Gujarat
India
pranavvyas.mca@charusat.ac.in
dharmendrapatel.mca@charusat.ac.in

ABSTRACT: *IOT devices suffer from the drawbacks of limited computational resources at local level. IOT devices are required to gather and process large quantity of data with limited resources. One solution is to upload data from IOT devices to cloud based systems, which can process data and send results back to devices. This technique suffers from delay in processing and results in delayed response from the cloud in real time scenarios. Another technique to solve the problem is to introduce a middleware processing node also called edge node. The processing of data from edge nodes is known as edge computing or fog computing. In this paper, the authors discuss the security aspects of fog computing. After careful study of related literature, the authors identified several challenges related to security of data processing at edge nodes. The authors identified challenges such as data security and programming related security. The authors present several solutions to the challenges.*

Keywords: IOT, Fog Computing, Edge Computing, Security, Data Security, Programming Security, Data Encryption, Trust Establishment, No-sql Databases, Procedural Language, Markup Language

Received: 17 November 2018, Revised 3 January 2019, Accepted 11 January 2019

DOI: 10.6025/jisr/2019/10/2/67-76

©2019 DLINE. All rights reserved

1. Introduction

Fog computing (Dastjerdi & Buyya, 2016) (Bonomi, Milito, Zhu, & Addepalli, 2012) ascertains by providing an intermediate layer between users and cloud servers in the form of fog servers in order to minimize access latency of the computations. Fog Computing acts similar as cloud computing in terms of services such as resource utilization, security, storage, computation, etc. The security in fog computing plays a vital role as it deals with real time data. Fog computing is derived from cloud computing so the security threats of cloud computing (Hashizume, Rosado, Medina, & Fernandez, 2013) (Gonzalez, et al., 2012) are innate to Fog Computing (Garcia Lopez, et al., 2015). Security issues related to virtualization (Luo, Lin, Chen, Yang, & Chen, 2011) (Wei, et al., 2009), network, data, segregation (Rittinghouse & Ransome, 2016) (Alliance, 2011), etc. are common in Fog Computing.

These security threats exists in Fog Computing due to developer's carelessness. Another important issue in Fog computing arises from data security. Security of heterogeneous data during communication suffers from lack of generic encryption algorithm where as data exchange between IOT devices and fog nodes suffers from an efficient mechanism for trust establishment. This issue is especially important if an IOT node is mobile and moves between networks.

In this paper, the authors have carried out an extensive literature survey on security challenges prevalent in Fog Computing. The authors have identified that very little research has been done on security issues related to the coding part of Fog Computing based application. Any software application has three fundamental viewpoints: (a) Database; (b) Front End where Procedural Language is utilized and (c) Documentation part. In this paper, the authors have recognized security threats of all these three viewpoints. After systematically studying all perspective security threats, the authors have outlined the possible solutions of every threat. The goals of the paper are as follows:

- To discern the existing security threats of Fog Computing.
- To distinguish Programming based Security threats in all viewpoints.
- To outline conceivable ideal solutions of all programming based security threats.

This paper is organized as follows: Section 2 will present the related work. In section 3 the data and programming based security challenges in Fog Computing are discussed. Section 4 will present the ideal solutions of the above mentioned threats. Finally, the paper will end with the concluding part.

2. Related Work

In their paper (Stojmenovic, Wen, Huang, & Luan, 2015), the authors propose a technique to detect intrusion by using signature. In this method, the researchers compare the behavior pattern against the database of possible misbehavior. They also propose anomaly based method where the researchers compare behavior against expected behavior. According to the paper, it is possible to achieve this by monitoring input rate of power flow for anomalies that are a result of modification by the attackers. The paper also highlights issues of authentication issues with IOT devices in an environment where the connection is fragile. The authors present a conceptual solution of this problem in our paper.

Wang et al. (Wang, Chen, & Wang, 2015) present authentication, authorization and data integrity as core security aspects in their paper. The authors state that the authentication should be a bi-directional process and researchers should focus on techniques for bi-directional authentication from cloud to the device. It is in this regard that the fog computing can play a vital role.

The authors also raise issues of data integrity. According to the authors, the device needs to make sure that the code running on the cloud is the same as the one submitted by the device. The edge computing nodes can use digital signatures to verify data integrity of application code from the device.

In his article on Bring Your Own Device (BYOD) Morrow (Morrow, 2012) highlights security challenges that an organization faces with movable devices. The author discusses challenges that comes with untrusted devices accessing the network. The author delibrates challenges such as mobile device security, data breach security, mobile data security, integration with corporate systems, cost of support, local regulations, industry specific security requirements.

In their article Roman et al. (Roman, Lopez, & Mambo, 2016) categorize various security threats for fog computing. They also present threat models for the fog-computing paradigm. The authors propose a variety of security mechanisms to overcome threats discussed earlier in the paper.

Lee et al. (Lee, Kim, Ha, Rajput, & Oh, 2015) present variety of issues and challenges in fog computing in their paper. The authors divide fog-computing security in security technology for IOT network, security technology for fog node and security technology for IOT node. The authors also discuss potential security and privacy problems related to fog computing. However, the authors do not present any solution to the problems discussed earlier.

Zhao and Ge (Zhao & Ge, 2013) present number of security problems with the internet of things that are related with fog computing. The authors analyze security problems from 3 perspectives: 1) Perception layer and data transmission related problems; 2) Network layer related problems and 3) Application layer related problems.

Stojmenovic and Wen (Stojmenovic & Wen, The Fog Computing Paradigm: Scenarios and Security Issues, 2014) present authentication and intrusion detection as possible security issues in fog computing. The authors of this paper provide generic solutions to the problems. The authors also discuss privacy issues. The authors review man-in-middle attack and examines it for depth analysis of the attack. The authors also offer several techniques based on CPU and memory usage to detect the attack.

Wang, Uehara and Sasaki (Wang, Uehara, & Sasaki, 2015) discuss differences between the security issues in cloud computing and fog computing. The authors identify several challenges that are out of scope for current discussion. The authors mention of intrusion of a rogue node and man in the middle attack as one of the most sensitive issues in fog computing.

Vaquero and Merino (Vaquero & Merino, 2014) raise issues of privacy and trust in fog computing. The authors argue that fog computing is an excellent technology to alleviate privacy concerns by applying innovative privacy protection techniques on data. On the issue of trust, the authors argue about introducing a sandboxing mechanism. The authors propose using this mechanism on new and unknown devices before larger networks can trust them.

Weber in his paper (Weber, 2010) presents security and privacy needs for IOT and fog computing technologies. The author elaborates on points such as resilience to attack, data authentication, access control and client privacy. The author also describes several privacy enhancing technologies such as Virtual Private Network (VPN), Transport Level Security (TLS), DNS Security Extension (DNSSEC), Onion routing protocol and Private Information Retrieval (PIR) systems.

Yan et al. (Yan, Zhang, & Vasilakos, 2014) in their paper identify a number of trust-based issues that can have impact on fog computing scenario. The authors present issues such as trust establishment in a heterogeneous architecture of IOT devices, data fusion and a need for generic trust management mechanism.

Yi et al. (Yi, Li, & Li, A Survey of Fog Computing: Concepts, Applications and Issues, 2015) in their paper identify authentication, access control, intrusion detection, privacy as major security concerns in fog computing. The authors describe trusted execution environment technique for authentication. The authors mention several access control mechanisms proposed in the literature. The authors suggest designing access control mechanism that can consider resource constraints at level of device, fog node and cloud. The authors also raise issues of intrusion detection in geo-distributed and highly mobile fog based systems. The authors also bring up privacy concerns by suggesting a privacy preserving mechanism by using homomorphic encryption techniques that can provide protection to data between fog and cloud. This also allows data aggregation without decryption. The authors also suggest differential privacy techniques for other requirements.

Ibrahim (Ibrahim, 2016) proposes a new mutual authentication scheme to establish trust between the device and the fog node. They propose a long-term key with sufficient length. The user can apply this key to perform authentication with fog nodes before joining their network. The key benefit of this system is that it does not need public key like infrastructure. Hence, it is much more efficient. One drawback of this scheme is if the key is expired or the device with the key is lost, it is not possible to retrieve the key.

Yi et al. (Yi, Qin, & Li, Security and privacy issues of fog computing: A survey, 2015) in their paper present several security and privacy issues related to fog computing. The authors refer to reputation-based system in order to establish a trusted relationship between the device and the fog node. The authors also touch upon intrusion detection by commenting on detection of rogue node with the help of network traffic analysis and round trip time. The authors also mention several authentication schemes including NFC and location limited channel for pre-authentication. As most of the authentication schemes are based on ad-hoc wireless network authentication schemes, the authors also suggest implementing a biometric based authentication scheme. On the issue of privacy in fog environment, the authors suggest data encryption techniques that are also searchable. The authors also raise several valid concerns regarding usage privacy and location privacy challenges.

3. Data and Programming Based Security Challenges

Data security issue deals with various aspects of security with regard to data collected by IOT devices and being processed in the fog nodes. This aspect deals with issues such as secure transmission of data considering the heterogeneous nature of data collected by IOT devices, absence of efficient encryption algorithms, authentication of new devices to name a few. The authors begin this section with description of data security issues in fog computing in detail. Later in this section the authors discuss programming security challenges in fog computing.

3.1 Security in Transmission of Hetrogeneous Data

There are different types of IOT devices and these devices are used for various purposes. These devices collect data of various nature. For example, an IOT device monitoring temperature of the room will be collecting numerical data, a device with light sensor will be collecting data in either video format or in the form of pictures. Some devices may be monitoring data from multiple sources at the same time. An example of such device is a baby monitor which may be monitoring a baby through audio and video link.

Due to this wide variety of data being captured by a variety of devices and absence of a standard encryption algorithm it is difficult to securely transmit data from IOT node to fog node on the edge.

3.2 Establishing Trust Based Relationship

The trust based relationship between an IOT device and an edge node can be established to reduce communication overhead taking place due to encryption and decryption process. This frees up the resources of IOT device and improves its performance further. A traditional trust based relationship techniques of certificate authorities and digital signatures can be used in case the IOT device is not mobile.

But since most IOT devices are highly mobile and can be moved around freely, they can move in different networks. For example, IOT systems located in the car or wearable gadgets. This characteristic of mobility of devices raises several issues. There are several techniques which can be used by a roaming node to establish trust based relationship with local edge node in swarm.

Programming based security is major point of focus in fog computing. Following are the main threats of programming in terms of fog computing:

3.3 Non-Relational Database Threats

The fog computing needs to store large amount of data in a distributed manner to deal with availability and scalability issues. Non-relational databases such as MongoDB and Cassandra are heavily used in fog computing as they handle large amount of data in unstructured form such as documents, sensor data, e-mail, multimedia, social media, etc. However, such databases have three main problems in terms of security such as:

3.3.1 Unencrypted Data in the Storage

In most of non-relational databases, the data is kept unencrypted. Inter cluster communication among devices happens freely without any kind of encryption or authentication. Hence, these the information stored in these databases is not secure unless encrypted.

3.3.2 Vulnerable to Injection Attacks

Non relational databases use the query languages similar as SQL, and they support unstructured data as well. Most of non relational databases use the parsed language that is vulnerable to injection attacks.

3.3.3 No Auditing

Generally, non relational databases do not provide any facilities for auditing transactions performed in the database.

3.3.4 Procedural Language Threats

For fog computing, the procedural language is used to communicate with the databases for the fog servers. It is used to store the data in the database, fetch the data from databases or any file system for analysis and prediction purpose. If the code is poorly written in the procedural language, it is vulnerable to several security threats:

3.3.5 Denial of Service Attack (DOS)

In fog computing, the procedural languages use the simple mathematical hashing to speed up storing and retrieving data. This kind of hashing is vulnerable to attack. The attacker can precompute a set of values in such a way that all hashes will be the same. Comparing these hash values creates a very heavy load on the fog server and as a result, there is a Denial of Service (DOS).

3.3.6 Cross Site Scripting Attack (XSS)

In most of procedural languages, there is no control over the output and this characteristic leads to this attack. Non-persistent XSS is common in a procedural language as the server reads the data directly from the HTTP request and imitates it back in the reply. DOM based XSS attack is also very common that simply modifies the client side script so several DOM features are to be compromised.

3.3.7 Lightweight Directory Access Protocol Attack (LDAP)

In procedural languages, LDAP protocol provides a means for accessing and modifying data directories. LDAP protocol is common in Internet of Things (IoTs) based applications where internet is dominant. Malicious intruder can send LDAP statements with code injection and steal sensitive information.

3.3.8 Operating System Command based Attack (OSC)

In this type of attack, the intruder uses the system level commands of Operating Systems and attack the vulnerable application. These commands bypass the administrative privileges and execute malicious Operating System commands to steal the sensitive information.

3.3.9 Extensible Markup Language based threat (XML)

Extensible Markup language describes the document of an application rather than stream of real data. The major attack in this category is XPath injection. XPath is used for querying XML. When user supplied information is used to construct the XPath, the attacker can find out how the XML data is structured in the document. The attack can take sensitive data from this document.

4. Solutions of Security Threats in Fog Computing

In this section the authors present several possible solutions to the challenges described in the previous section. The authors first describe data security challenges and then move towards proposing solutions of programming challenges.

4.1 Solution To Securely Transmit Heterogeneous Data

A possible solution to this problem can be a generic encryption algorithm that can work efficiently with a variety of data. An ideal encryption algorithm should also consider the limitation of IOT devices in terms of processing and storage capacity and should be resource friendly. Possible category of encryption algorithm for this can be symmetric key encryption algorithm that is easy to implement and resource friendly.

An alternative to encrypting data is to establish trust based relationship between IOT devices and the fog node. Once such a relationship is established, encryption before information transfer may not be required.

4.2 Solution To Establishing a Trust Based Relationship Between Device and Edge Node

One technique to establish trust between device and edge node is through Internet service providers. The mobile IOT devices would be required to be registered with ISPs and will be assigned a unique identifier similar to mobile phones. The network where they initially register with ISP can be considered home network and other networks can be considered as roaming networks. The ISPs can provide a gateway for the mobile device to communicate with its home network which in turn authenticates it. The home network can then issue an authentication token that can be used by the IOT device for a period of time before it can expire. This token can be presented at roaming networks as a token to the establish of trust based relationship between edge node in roaming network and mobile IOT device. In this technique it is assumed that a trust based relationship already exists among different networks. Hence, a device authenticated by one network need not to be authenticated by other swarm.

Alternatively, a reputation based model can be developed for IOT device. The IOT device can be initially assigned a default score and its reputation can increase or decrease based on its interaction with edge node. A device with a reputation below certain threshold can be declined service by edge node. However, usage of this model can result in several issues. One of the main issues when using this model is regarding identity and authenticity of the IOT device. Another issue that is presented by this model is the ability of an edge node to differentiate between intentional and accidental misbehavior of device which can affect its reputation score.

The first issue can be solved by group authentication protocols. There are many such protocols proposed by researchers. Mahalle (Mahalle, Prasad, & Prasad, 2014) in their paper propose a group authentication scheme based on threshold cryptography.

According to the authors the proposed scheme is lightweight and overcomes the battery exhaustion attack on certain IOT devices. The proposed scheme is efficiently tested only for the Wi-Fi environment. While most IOT devices are Wi-Fi enabled, this does not hold true for all IOT devices. There are large number of devices that use Bluetooth or infrared signals for communication. Hence, the proposed scheme by the authors is not generic for all devices.

In their paper Kalra and Sood (Kalra & Sood, 2015) propose a cookie based mechanism of authentication of IOT devices. In this paper the authors assume that most IOT devices are built in with a browser based interface. This makes it possible to interact with devices using HTTP and hence propose encrypted cookies for authentication. The scheme only considers authentication by a central authority. Here, the authors do not consider devices with high mobility. The IOT devices installed in the cars have high mobility and may not be able to keep constant contact with central authority to be authenticated using the proposed scheme.

Another issue is ability of edge node to detect misbehavior. Machine learning techniques can be helpful for this. In their paper Meidan et. al (Meidan, et al., 2017) propose one such scheme to detect an unauthorized node by monitoring traffic data. In the proposed scheme the authors install various IOT devices and monitor their traffic data. The authors extract features from the stored traffic data and train the machine with the extracted data. However, this scheme may not give accurate results when there is a high volume of traffic on the network. It may also not be accurately able to predict the rogue node if the node is able to mimic the traffic pattern familiar to the monitoring system.

An alternative concept can be to actively monitor node behavior and categorizing it in accidental or intentional. This data can be collected and analyzed for patterns and features. CPU usage, memory usage, network usage are some of the parameters to look out for in order to find patterns in behavior of the device. It is possible to train a classifier to monitor for patterns determining the behavior of the device.

4.3 Solutions of Non-Relational Databases Challenges

4.3.1 Solutions for Unencrypted Data in Non-Relational Databases

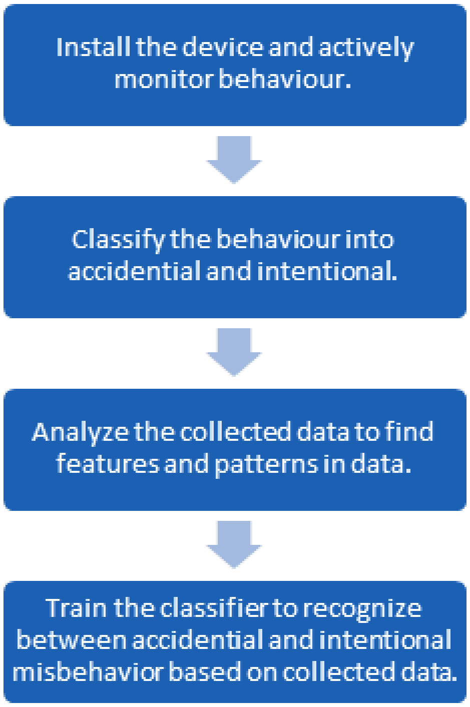
Install the device and actively monitor behaviour.
Classify the behaviour into accidential and intentional.
Analyze the collected data to find features and patterns in data.
Train the classifier to recognize between accidential and intentional misbehavior based on collected data.

Figure 1. Behavior monitoring using machine learning

As discussed in the previous section, the one of the major security threat in the fog computing is unencrypted data in the storage. The main reason for this is to achieve speedy performance at the edge node. However, security is also the main concern in several applications where data is very sensitive. Light weight encryption algorithms (Katagi & Moriai, 2008), (Ebrahim, Khan, & Mohani, 2014), (Lim & Korkishko, mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors, 2005), (Lim, Crypton: A new 128-bit block cipher, 1998) are best suited for the fog computing. The majority of algorithms are designed by keeping only one parameter, either security or performance, in mind. However, several other parameters are essential while designing encrypted algorithms of fog computing. Lightweight block cipher, lightweight hash function and high performance system are essential in the fog computing to achieve security as well as performance. The figure-2 describes the components of fog computing based encryption.

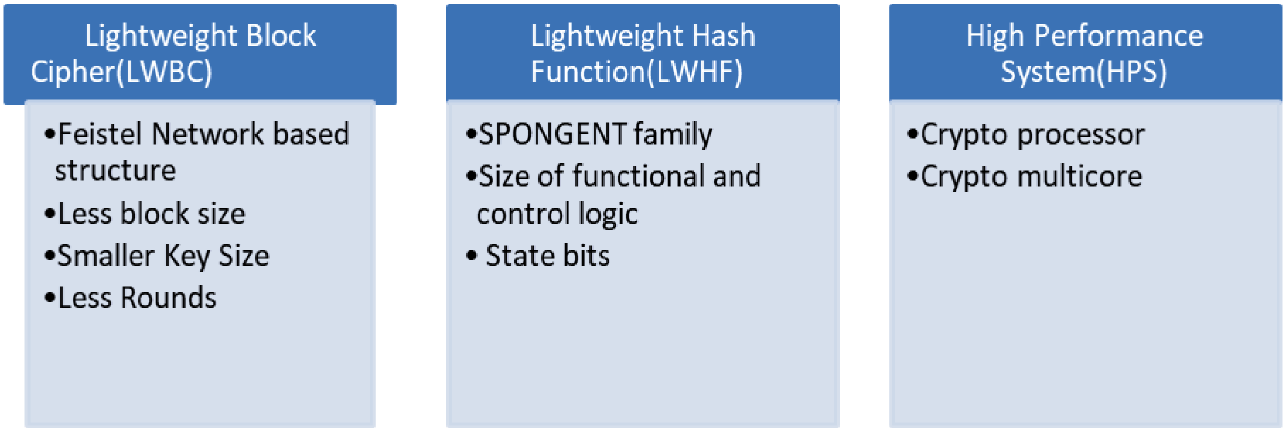
Lightweight Block Cipher(LWBC)
•Feistel Network based structure
•Less block size
•Smaller Key Size
•Less Rounds
Lightweight Hash Function(LWHF)
•SPONGENT family
•Size of functional and control logic
• State bits
High Performance System(HPS)
•Crypto processor
•Crypto multicore

Figure 2. Components of Fog Computing based Encryption

The Feistel Network (Schneier & Kelsey, 1996) based structure is very simple and secure. ARX (Dinu, et al., 2016) based ciphers of this category are designed using addition, rotation and XOR. Algorithms designed in this way are faster and exhibit inherent security. Light Weight Hash function with SPONGENT family needs less size for functional and control logic and contains fewer bits. In addition to LWBC and LWHF, if the system has high performance capacity, like crypto processor and crypto multicore, then it gives an optimum performance.

4.3.2 Solution of Injection Attacks in Non-Relational Databases

Fog computing based applications are also vulnerable to an injection attack. The attacker can falsify a malicious NoSQL based query. Data Validation is an ideal solution for this kind of problem. Data Validation Middleware can be implemented that automatically check the user requested data. The code of Middleware comes before the controller code. Middleware describes the functions shown in Figure-3.

4.3.3 Solution of Auditing Issue in Non-Relational Databases

Auditing is another major problem in the NoSQL type of databases due to performance reasons. However, auditing is essential in the context to the security aspect in fog computing. The column oriented storage technique (COST) is best suited for the auditing in databases due to their high performance. It is not necessary to maintain a log for Read operation as it is not so affected to security reasons, so the authors can skip such operations and can only focus on IUD (Insert, Update and Delete) operations.

4.3.4 Solution Of DOS Attack In Non-Relational Databases

DOS attack is very common in Fog Computing. DOS attack in Fog Computing can be prevented by proactive means rather than reactive means. Several strategies were presented in the literature to prevent DOS attack: (Mirkovic & Reiher, 2004), (Feinstein, Schnackenberg, Balupari, & Kindred, 2003), (Iyengar, Kumar, & Kannammal, 2013), (Vissers, Somasundaram, Pieters, Govindarajan, & Hellinckx, 2014). The Challenge response (*CR*) is an ideal strategy for the Fog Computing. It is an easy strategy to implement. It addresses most common attacks such as automated, bot and rate based. Cookie based puzzle mechanism can be integrated with this strategy to make an effective solution of this category.

4.3.5 Solution of XSS Threat in Non-Relational Databases

XSS threat is another well-known security threat of procedural programming language of fog computing. The most common

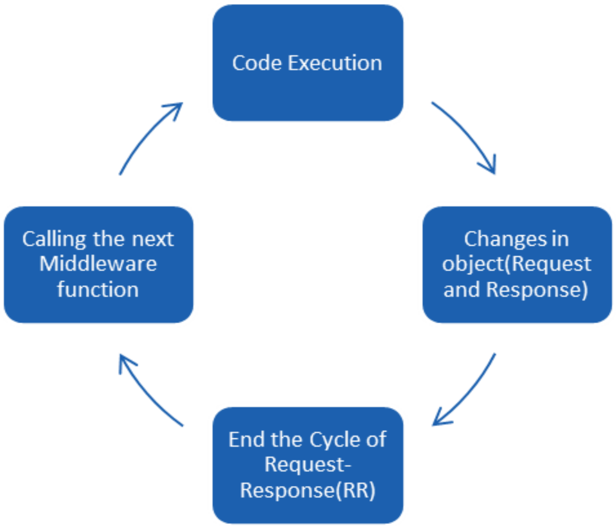
Code Execution
Changes in object(Request and Response)
End the Cycle of Request-Response(RR)
Calling the next Middleware function

Figure 3. Middleware Architecture for injection attack solution in NOSQL

solution is to turn off scripting in the browser from the user side, but it is not an ideal solution as client side scripting is essential in most of applications. The best solution from the point of view of the language aspect is to establish a filter that is able to identify trusted and an untrusted scripting code dynamically.

4.3.6 Solution of LDAP in Non-Relational Databases

Lightweight Directory Access Protocol Attack (LDAP) is common now days. There are two main entities that lead this attack (a) Input and (b) Meta Characters used in the query. If the developer can prevent these two situations, the developer is able to prevent LDAP attack. Input validations are required at both client and server side. To do this the developer must assume expected input in the system. The system must reject the input, which does not meet the criteria set by the developer. It is possible to prevent misuse of the meta characters such as (,), *, &, %, #, @, Etc. by preceding them with the appropriate character with regards to the operating system.

4.3.7 Solutions of Procedural Language Based Challenges

Fog Computing based applications need an interface where users can read a file, send an email, execute an OS command to perform certain tasks and such an interface leads the attack of OS based commands. There are several possible solutions that need to be incorporated in modern programming languages to prevent this attack. The possible solutions are described in Table 1.

Sr.No	Probable Solution	Description
1.	Use of API	Instead of allowing users to enter the OS commands directly, use API when it is possible to avoid this attack.
2.	Scrub Input	When the API is not possible, scrub the input value to avoid malicious character input especially for the alphanumeric value.
3.	String Literal	Instead of allowing commands from user, construct the commands using string literal.
4.	Whitelist or Enumerated Input	When a command input is compulsorily required, use only items in whitelist or enumerate them in conditions.
5.	Principle of least privilege	In coding, give the appropriate privilege to every user to do their job to prevent this situation.

Table 1. Probable solutions for the OS Command based attack

4.3.8 Solution Of Markup Language Based Challenges

The XML based attack is common in modern applications as it is extensively used for documentation and database development. XPath attack is the well known in this category. The best and feasible solution for these challenges is the creation of XPath expression with a parameter instead of string concatenation. Here instead of passing the user input, parameters are passed that reduce the risk of this attack.

5. Conclusion

In this paper, the authors have presented various security challenges faced by edge nodes in fog computing environment. The authors have concentrated upon data and programming based security challenges. The authors have identified data security challenges such as heterogeneous data exchange and challenge of trust establishment between an IOT device and an edge node. As far as programming challenges are concerned, the authors have identified challenges in applications of non-relational databases, applications of procedural aspects and markup language based challenges. The authors have also suggested the solutions to the above mentioned challenges as theoretical concepts. The authors concluded that the research is scarce from the point of view of applications in edge computing. The authors also concluded that if certain security parameters are stressed during programming, several security challenges may have least impact or can be avoided altogether.

References

[1] Alliance, C. (2011). *Security guidance for critical areas of focus in cloud computing v3. 0.* Cloud Security Alliance.

[2] Bonomi, F., Milito, R., Zhu, J., Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, (p. 13-16).

[3] Dastjerdi, A. V., Buyya, R. (2016). Fog computing: Helping the Internet of Things realize its potential. *Computer,* 49 (8) 112-116. (August).

[4] Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., Biryukov, A. (2016). Design strategies for ARX with provable bounds: Sparx and LAX. *International Conference on the Theory and Application of Cryptology and Information Security,* Springer, Berlin, Heidelberg.

[5] Ebrahim, M., Khan, S., Mohani, S. S. (2014). Peer-to-peer network simulators: an analytical review. *arXiv preprint arXiv:1405.0400.*

[6] Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D. (2003). Statistical approaches to DDoS attack detection and response. *In:* IEEE Proceedings of DARPA Information Survivability Conference and Exposition, 1, p. 303-314.

[7] Lopez, Garcia., P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A., Riviere, E. (2015). Edge-centric Computing: Vision and Challenges. *ACM SIGCOMM Computer Communication Review,* 45 (5) 37-42.

[8] Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Näslund, M., Pourzandi, M. (2012). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *Journal of Cloud Computing: Advances, Systems and Applications,* 1(1), 11.

[9] Hashizume, K., Rosado, D. G., Medina, E. F., Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications,* 4 (1) 5.

[10] Ibrahim, M. H. (2016). Octopus: An Edge-Fog Mutual Authentication Scheme. *International journal of Network Security,* 18 (6) 1089-1101.

[11] Iyengar, J. N., Kumar, N., Kannammal, A. (2013). An enhanced entropy approach to detect and prevent DDoS in cloud environment. *International Journal of Communication Networks and Information Security, 5*(2), 110-119.

[12] Kalra, S., Sood, S. K. (2015). Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile Computing,* 24, 210-223.

[13] Katagi, M., Moriai, S. (2008). *Lightweight cryptography for the internet of things.* Sony Corporation.

[14] Lee, K., Kim, D., Ha, D., Rajput, U., Oh, H. (2015). On Security and Privacy Issues of Fog Computing supported Internet of Things Environment. *IEEE 6th International Conference on the Network of the Future (NOF)*, (p. 1-3).

[15] Lim, C. H. (1998). *Crypton: A new 128-bit block cipher.* NIsT AEs Proposal.

[16] Lim, C. H., Korkishko, T. (2005). mCrypton-a lightweight block cipher for security of low-cost RFID tags and sensors. *In:* Lecture Notes in Computer Science 3786 (p. 243-258).

[17] Luo, S., Lin, Z., Chen, X., Yang, Z., Chen, J. (2011). Virtualization security for cloud computing service. *In:* IEEE International Conference on Cloud and Service Computing (CSC), (p. 174-179).

[18] Mahalle, P. N., Prasad, N. R., Prasad, R. (2014). Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (IoT). *In:* 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE).

[19] Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., Elovici, Y. (2017). Detection of Unauthorized IoT Devices Using Machine Learning Techniques. *Arxiv Preprint arXiv:1709.04647*.

[20] Mirkovic, J., Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review,* 34(2) 39-53.

[21] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, p. 5-8.

[22] Rittinghouse, J. W., Ransome, J. F. (2016). *Cloud Computing: Implementation, Management, and Security.* CRC Press.

[23] Roman, R., Lopez, J., Mambo, M. (2016). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*.

[24] Schneier, B., Kelsey, J. (1996). Unbalanced Feistel networks and block cipher design. *In:* International Workshop on Fast Software Encryption Springer, Berlin, Heidelberg.

[25] Stojmenovic, I., Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. *In:* Federated Conference on Computer Science and Information Systems. doi:10.15439/2014F503

[26] Stojmenovic, I., Wen, S., Huang, X., Luan, H. (2015). An overview of Fog computing and its security issues. *Concurrency and Computation: Practice and Experience,* 28 (10), 2991-3005. doi:10.1002/cpe.3485

[27] Vaquero, L. M., Merino, L. R. (2014). Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. *ACM SIGCOMM Computer Communication Review,* 44 (5) 27-32.

[28] Vissers, T., Somasundaram, T. S., Pieters, L., Govindarajan, K., Hellinckx, P. (2014). DDoS defense system for web services in a cloud environment. *Future Generation Computer Systems,* 1 (37) 37-45.

[29] Wang, Y., Chen, I.-R., Wang, D.-C. (2015). A Survey of Mobile Cloud Computing Applications: Perspectives and Challenges. *Wireless Personal Communications*, 80 (4) 1607-1623.

[30] Wang, Y., Uehara, T., Sasaki, R. (2015). Fog Computing:Issues and Challenges in Security and Forensics. *In:* 39th IEEE Annual International Conference on Computers, Software & Applications.

[31] Weber, R. H. (2010). Internet of Things - New Security and Privacy Challenges. *Computer Law and Security Review,* 26 (1) 23-30.

[32] Wei, J., Zhang, X., Ammons, Glenn, Bala, V., Ning, P. (2009). Managing security of virtual machine images in a cloud environment. *In:* Proceedings of the 2009 ACM workshop on Cloud computing security.

[33] Yan, Z., Zhang, P., Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Computer Network and Applications,* 42, 120-134.

[34] Yi, S., Li, C., Li, Q. (2015). A Survey of Fog Computing: Concepts, Applications and Issues, *In:* ACM Proceedings of the 2015 Workshop on Mobile Big Data.

[35] Yi, S., Qin, Z., Li, Q. (2015). Security and privacy issues of fog computing: A survey. *In:* Springer International Conference on Wireless Algorithms, Systems, and Applications. Cham.

[36] Zhao, K., Ge, L. (2013). A Survey on the Internet of Things Security, *In:* Ninth International Conference on Computational Intelligence and Security.