Security Challenges for IoT Based Applications & Solutions Using Fog Computing: A Survey

Miss. Sayali Karmode

Assistant Professor (CS & IT) at Satish Pradhan Dnyansadhana College, Thane

*Correspondence: sayalis.karmode@gmail.com

Abstract: The internet of things has taken the world by storm. According to prediction, there will be around 30 billion connected devices in the year 2020. This means that some or all our home applications might have the capability to be controlled remotely. Recently, the use of IoT devices and sensors has been rapidly increased which also caused data generation (information and logs), bandwidth usage, and related phenomena to be increased. To our best knowledge, a standard definition for the integration of fog computing with IoT is emerging now. This integration will bring many opportunities for the researchers, especially while building cyber-security related solutions. In this study, we surveyed about the integration of fog computing with IoT and its implications. Our goal was to find out and emphasize problems, specifically security-related problems that arise with the employment of fog computing by IoT.

Keywords: IoT, IoT Security, Security Threats, Cloud, Fog Computing

1. Introduction

The Internet of Things (IoT) is one of the spotlight innovations which has the potential to provide unlimited benefits to our society. The development of the IoT is about to reach a stage at which many of the objects around us will have the ability to connect to the Internet to communicate with each other without human intervention. The pace of connecting physical devices around us to the Internet is increasing rapidly. According to a recent Gartner report, there will be around 8.4 billion connected things worldwide in 2020. This number is expected to grow to 20.4 billion by 2022. The use of IoT applications is increasing in all parts of the world. The major driving countries in this include western Europe, North America, and China. The number of machine to machine (M2M) connections is expected to grow from 5.6 billion in 2016 to 27 billion in 2024. This leap in numbers itself declares IoT to be one of the major upcoming markets that could form a cornerstone of the expanding digital economy. The IoT industry is expected to grow in terms of revenue from $892 billion in 2018 to $4 trillion by 2025. M2M connections cover a broad range of applications like smart cities, smart environments, smart grids, smart retail, smart farming, etc [1].

In the future, the devices are not only expected to be connected to the Internet and other local devices but are also expected to communicate with other devices on the Internet directly. Apart from the devices or things being connected, the concept of social IoT (SIoT) is also emerging. SIoT will enable different social networking users to be connected to the devices and users can share the devices over the Internet. With all this vast spectrum of IoT applications comes the issue of security and privacy.

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

Without a trusted and interoperable IoT ecosystem, emerging IoT applications cannot reach high demand and may lose all their potential. Along with the security issues faced generally by the Internet, cellular networks, and WSNs, IoT also has its special security challenges such as privacy issues, authentication issues, management issues, information storage, and so on. Due to all these issues and vulnerabilities, the IoT applications create a fertile ground for different kinds of cyber threats.

The Internet of Things is poised to apply major stresses to the current internet and data center infrastructure. The popular current approach is to centralize cloud data processing in a single site**,** resulting in lower costs and strong application security. But with the sheer amount of input data that will be received from globally distributed sources, this central processing structure will require backup. Also, most enterprise data is pushed up to the cloud, stored and analyzed, after which a decision is made and action taken. But this system isn't efficient, to make it efficient, there is a need to process some data or some big data in IoT case in a smart way, especially if it's sensitive data and need quick action. To deal with this Fog computing is the best solution. In this paper, we are presenting various layers of IoT with challenges and solutions for it i.e fog computing working.

2. Review & Analysis

2.1 Sources of security threats in IoT applications

A. Security issues at the sensing layer

This deals with physical IoT sensors and actuators. Sensors sense the physical phenomenon happening around them. Actuators, on the other hand, perform a certain action on the physical environment, based on the sensed data. There are various kinds of sensors for sensing different kinds of data, e.g., ultrasonic sensors, camera sensors, smoke detection sensors, temperature and humidity sensors, etc. There can be mechanical, electrical, electronic, or chemical sensors used to sense the physical environment. Various sensing layer technologies are used in different IoT applications like RFID, GPS, WSNs, RSNs, etc

B. Security issues at the network layer

The key function of the network layer is transmitting the information received from the sensing layer to the computational unit for processing. The major security issues that are encountered at the network layer are as follows and which leads to the following attacks on applications.

- Phishing site attack
- Access attack
- Dos attack
- Data transit attack
- Routing attack

C. Security issues at the middleware layer

The role of the middleware in IoT is to create an abstraction layer between the network layer and the application layer. Middleware can also provide powerful computing and storage capabilities. This layer provides APIs to fulfill the demands of the application layer. The middleware layer includes brokers, persistent data stores,

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

queuing systems, machine learning, etc. Although the middleware layer is useful to provide a reliable and robust IoT application, it is also susceptible to various attacks [2]. These attacks can take control of the entire IoT application by infecting the middleware. Database security and cloud security are other main security challenges in the middleware layer. Various possible attacks in the middleware layer are discussed as follows.

- Man in the middle attack
- SQL injection attack
- Cloud malware attack

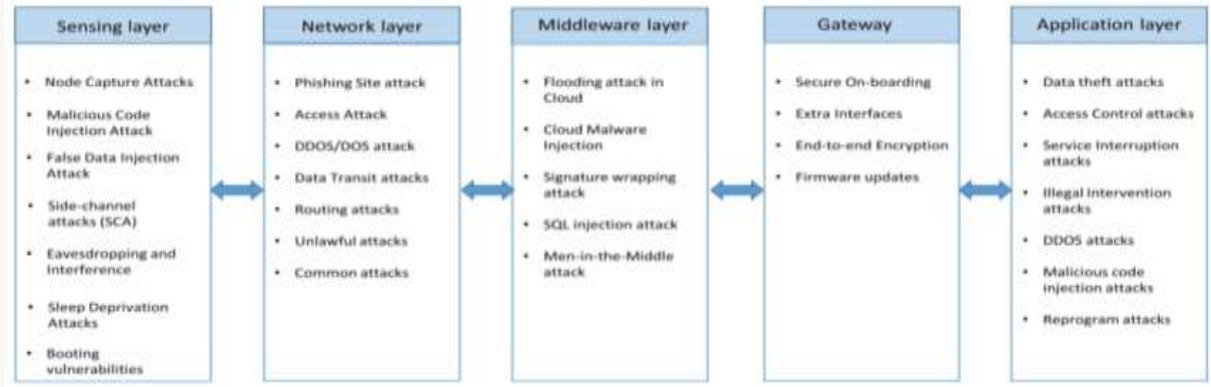

Fig. 1 Security issues in a layer of IoT application

D. Security issues at gateways

Gateway is a broad layer that has an important role in connecting multiple devices, people, things, and cloud services. Gateways also help in providing hardware and software solutions for IoT devices [3]. Gateways are used for decrypting and encrypting IoT data and translating protocols for communication between different layers. IoT systems today are heterogeneous including LoraWan, ZigBee, Z-Wave, and TCP/IP stacks with many gateways in between. Some of the security challenges for IoT gateway are as follows:

- Secure onboarding
- End to end encryption
- Firmware updates

E. Security issues at the application layer

The application layer directly deals with and provides services to the end-users. IoT applications like smart homes, smart meters, smart cities, smart grids, etc. lie in this layer. This layer has specific security issues that are not present in other layers, such as data theft and privacy issues. The security issues in this layer are also specific to different applications. Many IoT applications also consist of a sublayer between the network layer and application layer, usually termed as an application support layer or middleware layer [4][5]. The support layer supports various business services and helps in intelligent resource allocation and computation. Some security issues mostly encounter by this layer are as follows:

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

- Data theft
- Access control attack
- Service interruption attacks
- Sniffing attack
- Reprogram attack

2.2 Challenges in security:

Large-scale IoT deployments created situations that cloud computing could not handle efficiently and effectively. For instance, applications that require low latency while processing the data on the edge of the network. In real life, a massive amount of data is being collected by IoT from many different sensors in various environments such as factory production lines, vehicles, machines, elevators, etc. or individual purposes such as smart home systems, hobby-related sensors, etc. These sensing devices have different characteristics and features. They are connected via hardwire or WiFi. Large-scale device deployments in heterogeneous environments bring management issues. Hence, intelligent communications approaches are needed in which efficiency and robustness are prioritized.

The IoT promises to bring the connectivity to an earthly level, permeating every home, vehicle, and workplace with smart, Internet-connected devices. But as dependence on our newly connected devices increases along with the benefits and uses of a maturing technology, the reliability of the gateways that make the IoT a functional reality must increase and make uptime a near guarantee. Like every appliance, light, door, piece of clothing, and every other object in your home and office become potentially Internet-enabled; The Internet of Things is poised to apply major stresses to the current internet and data center infrastructure [6]. The popular current approach is to centralize cloud data processing in a single site**,** resulting in lower costs and strong application security. But with the sheer amount of input data that will be received from globally distributed sources, this central processing structure will require backup. Also, most enterprise data is pushed up to the cloud, stored and analyzed, after which a decision is made and action taken. But this system isn't efficient, to make it efficient, there is a need to process some data or some big data in IoT case in a smart way, especially if it's sensitive data and need quick action.

Using a cloud network to stream data and analyze data has its limitations such as bandwidth consumption and communication costs. If the user data are sensitive, securing the data is another important issue. The data are important for auditing purposes or controlling the assets to improve efficiency or preventing disasters etc. The data analysis could be done on-site by running the software at local stations. The cloud would be used as storing the analysis result for historical and audit purposes. The data aggregation will reduce the bandwidth and also bandwidth related cost. IoT security has always been a controversial issue. The CoT paradigm is not straightforward, it also introduces new challenges to the IoT system that cannot be addressed by the traditional centralized cloud computing architecture, such as latency, capacity constraints, resource-constrained devices, network failure with intermittent connectivity and enhanced security.

2.3 Solution

2.3.1 Fog Computing

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

Fog computing is an effective approach to solve the above-mentioned security threats that we face without fog computing.

It allows computing, decision-making, and action-taking to happen via IoT devices and only pushes relevant data to the cloud**,** Cisco coined the term "Fog computing "and gave a brilliant definition for Fog Computing: "The fog extends the cloud to be closer to the things that produce and act on IoT data. These devices, called fog nodes, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oil rig. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and video surveillance cameras."Large-scale IoT deployments created situations that cloud computing could not handle efficiently and effectively. For instance, applications that require low latency while processing the data on the edge of the network. In real life, a massive amount of data is being collected by IoT from many different sensors in various environments such as factory production lines, vehicles, machines, elevators, etc. or individual purposes such as smart home systems, hobby-related sensors, etc [7]. These sensing devices have different characteristics and features. They are connected via hardwire or WiFi. Large-scale device deployments in heterogeneous environments bring management issues. Hence, intelligent communications approaches are needed in which efficiency and robustness are prioritized.

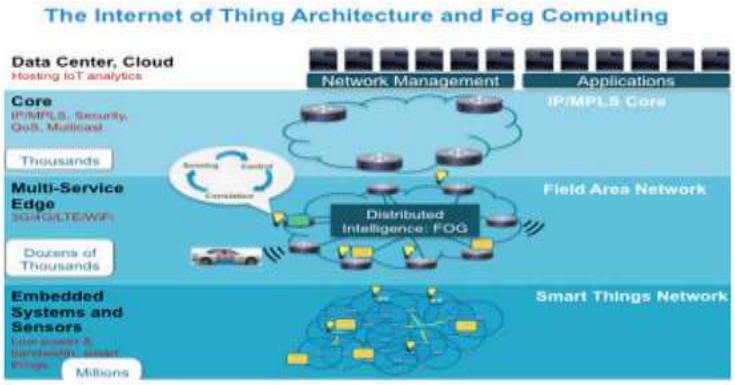

Fig. 2 Architecture of IoT & Fog computing

Using a cloud network to stream data and analyze data has its limitations such as bandwidth consumption and communication costs. If the user data are sensitive, securing the data is another important issue. The data are important for auditing purposes or controlling the assets to improve efficiency or preventing disasters etc. The data analysis could be done on-site by running the software at local stations [7] [8]. The cloud would be used as storing the analysis result for historical and audit purposes. The data aggregation will reduce the bandwidth and also bandwidth related cost. The fog computing architecture theoretically and mathematically while comparing the performance of fog computing paradigm with traditional cloud computing framework based on service latency and energy consumption. Fog computing reduces the data traffic between cloud and network edge by 90% and average response time for a user by 20% when compared with the cloud-only model.

2.3.2 Advantages of fog overcloud

IoT devices generate large volumes of data every day. Moving this data to the cloud in real-time for analysis is not feasible. Therefore, the concept of fog computing has been developed [9]. Fog computing refers to extending cloud computing and its services to the edge of the network. Fog computing is a decentralized infrastructure for analysis of data and computing and can be used to store and process time-sensitive data efficiently and quickly. Its main goal is to enhance security, prevent data thefts, minimize the data stored on the cloud, and to increase the overall efficiency of IoT applications. The latency in fog computation is less than cloud computation because the fog

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

layer is placed much closer to the devices than the cloud. Only the selected and important data is sent to the cloud for long-term storage. Fog computing applications include smart vehicles, smart homes, smart agriculture, health-care, smart traffic lights, smart retail, software-defined networks, etc. Sending the immense amount of data generated by IoT devices to the cloud for processing and analyzing would be costly and time-consuming [9][10]. Along with minimizing network bandwidth requirements, fog computing also reduces the frequency of two-way communication between IoT devices and the cloud. In fog architecture, the data is collected at devices called fog nodes which can analyze 40 percent of it. It offloads traffic from the core network minimizing the latency of IoT devices.

Fig. 3 Fog computing & IoT devices

A fog node can be any device like a router, switch, or a video surveillance camera that has computing, storage, and network connectivity. These fog nodes can be installed anywhere like on a factory floor or in a vehicle, provided it has a network connection. Data is directed to the fog node, aggregation node, or cloud-based on its time-sensitivity. Fog nodes make the communication in IoT application secure by providing cryptographic computations.

2.3.3 Solutions provided by fog computing to overcome IoT security threats

Regarding the attacks discussed in Section 2.1 , the solution that fog computing provides or can provide to overcome those security threats are discussed below.

1. Man-in-the-middle attack: Fog acts as a security layer between end-user and cloud or IoT systems. All threats or attacks on the IoT systems need to pass through the fog layer in between, and this layer can identify and mitigate unusual activities before they are passed to the system.

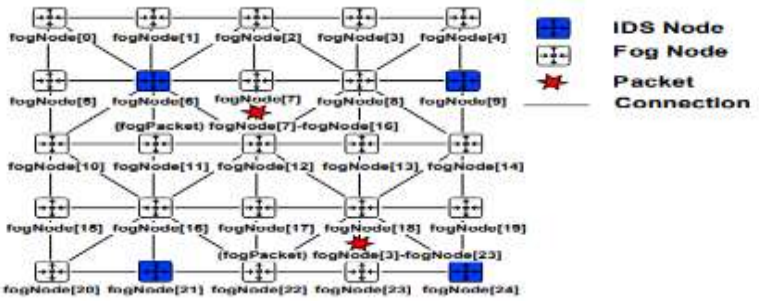

Fig. 4 Fog nodes

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

The symmetry and proximity (one-hop distance) to the fog nodes ensured in the deployment of the IDS nodes allows reduced latency. Each IDS is placed such that it is one hop away from the nodes it observes in a wheel spoke fashion. Whenever IDS node finds a compromised node or an intruder, it simply informs nodes close to it to cut off connection with the node. Also, packets are routed from source to destination by first moving the packets in a multi-hop fashion along the Y-axis (i.e. up or down). The packets move in this direction until they reach their destination's row [11]. Then the packets move along the X-axis (i.e. backward or forward) until they reach their destination.

2. Data transit attacks: Data storage and management are much better if performed on the secure fog nodes, as compared to the IoT devices. Data will be better protected if it is stored on the fog nodes as compared to storing the data on the end-user devices. Fog nodes also help in making the user data more available.

3. Eavesdropping: Using fog nodes, the communication takes place between the end-user and the fog node only, rather than routing the information through the entire network. The chances of an adversary trying to eavesdrop reduce a lot because the traffic on the network is reduced.

4. Resource-constraint issues: Most of the IoT devices are resource-constrained and the attackers take advantage of this fact. They try to damage the edge devices and use them as the weak links to enter the system. Fog nodes can support the edge devices and can prevent them from being affected by such attacks. A nearby fog node can perform the more sophisticated security functions necessary for protection.

5. Incident response services: Fog nodes can be programmed to provide real-time incident response services. Fog nodes can generate a flag to the IoT system or the end-users as soon as they encounter a suspicious data or request. Fog computing allows for malware detection and problem resolution in transit [12]. In many critical applications, it might not be possible to stop the entire system to resolve malware incidences. Fog nodes can help in such resolutions while the system is up and running.

3. Conclusions

Moving the intelligent processing of data to the edge only raises the stakes for maintaining the availability of these smart gateways and their communication path to the cloud. When the IoT provides methods that allow people to manage their daily lives, from locking their homes to checking their schedules to cooking their meals, gateway downtime in the fog computing world becomes a critical issue. Additionally, resilience and failover solutions that safeguard those processes will become even more essential. Throughout this article, we have discussed the implications of using fog computing as a backbone architecture for IoT, especially from the cybersecurity point of view. According to our finding, we have stated that usage of fog computing for cloud-based IoT system might have items of cost,

References

[1] Yousuf, Tasneem, et al. "Internet of Things (IoT) Security: Current status, challenges, and countermeasures." International Journal for Information Security Research (IJISR), vol. 5, no .4, 2015, pp. 608-616**.**

[2] W. Wang, P. Xu, and L. T. Yang, “Secure data collection, storage and access in cloud-assisted IoT," IEEE Cloud Computing, vol. 5, no. 4, pp. 77–88, 2018.

[3] Rose, Karen et al. "The Internet of Things: An Overview." The Internet Society (ISOC), vol. 1, 2015, pp. 1-50.

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143

[4] Albishi, Saad, Soh Ben, Ullah, Azmat, and Algarni, Fahad. "Challenges and Solutions for Applications and Technologies in the Internet of Things." Procedia Computer Science 124 (2017) 608–614.

[5] C. Li and C. Chen, "A multi-stage control method application in the fight against phishing attacks," Proceeding of the 26th computer security academic communication across the country, pp. 145, 2011.

[6] B. Zhang, N. Mor, J. Kolb, D. S. Chan, K. Lutz, E. Allman, J. Wawrzynek, E. A. Lee, and J. Kubiatowicz, "The cloud is not enough: Saving iot from the cloud." in HotStorage, 2015.

[7] I. Butun, B. Kantarci, and M. Erol-Kantarci, "Anomaly detection and privacy preservation in cloud-centric internet of things," in Communication Workshop (ICCW), 2015 IEEE International Conference on. IEEE, 2015, pp. 2610–2615.

[8] T. H. Luan, L. Gao, Z. Li, Y. Xiang, and L. Sun, "Fog computing: Focusing on mobile users at the edge," CoRR, vol. abs/1502.01815, 2015. [Online]. Available: http://arxiv.org/abs/1502.01815

[9] S. Forsstr¨om, I. Butun, M. Eldefrawy, U. Jennehag, and M. Gidlund, "Challenges of securing the industrial internet of things value chain," in 2018 Workshop on Metrology for Industry 4.0 and IoT. IEEE, 2018, pp. 218–223.

[10] "Fog computing and the internet of things: Extend the cloud to where the things are," Cisco White Paper, 2015.

[11] Z. Shae and J. J. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017, pp. 1972–1980.

[12] D. Koo, Y. Shin, J. Yun, and J. Hur, "An online data-oriented authentication based on merkle tree with improved reliability and fog computing," in 2017 IEEE International Conference on Web Services (ICWS). IEEE, 2017, pp. 840–843.

Received: Nov 15, 2019 Revised: April 21, 2020 Accepted: May 3, 2020

DOI: 10.5281/zenodo.3786143