International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 12; December 2017; Page No. 8139-8144
DOI: http://dx.doi.org/10.24327/ijcar.2017.8144.1297

Research Article

A STUDY ON FOG COMPUTING BASED IOT ENVIRONMENT: SECURITY ISSUES AND CHALLENGES

Veerraju T*., Sai Ganesh S and Murthy G.S.N

Department of CSE, Aditya College of Engineering, Surampalem, Andhra Pradesh, India

A R T I C L E I N F O

Article History:
Received 9th September, 2017
Received in revised form 12th October, 2017
Accepted 6th November, 2017
Published online 28th December, 2017

Key words:

Cloud computing, Internet of Things, attacks, Security challenges.

A B S T R A C T

Cloud computing is one among the most prominent technologies for present users, which provides elastic recourses for utilizing services. Cloud computing may possibly facilitate by contribute on-demand and scalable storage, along with the processing services that preserve scale to IoT necessities. Fog computing evolved at resources close to IoT sensors for local storage space and groundwork data processing at the edge of the network. The major problem in the Fog computing is security due the limited resources. In this paper, we investigate explores the security issues and challenges of Fog and provides a different attacks and countermeasures on security. We focused the future security directions and challenges to address in fog networks.

INTRODUCTION

In the present scenario of the user needs are relying on the cloud computing technology. The cloud built with physical and virtualized resources over the internet. Cloud provides on demand services to store the user data as well as to use the elastic resources based on their user needs. Cloud provides us pay and use model. In current scenario, we felt that it is comfortable to us to store and retrieve the data. But, when the number of devices increased to be connected to the internet definitely there would be a major problem in storage as well as accessing the information retrieval. The IoT concept is come into the existence as a better choice to defeat the problem (M.Friedemann and C. Floerkemeier, 2010).

Internet of Things allows RFID, sensor nodes and GPS in our daily life environment to be active participants by getting and sharing information with other members of the network. The traditional internet connects device to device, device to human. In the year 1999, the IoT concept was introduced at MIT. The IoT refers to the interconnection of networked objects, sensors, tools or devices. The above mentioned things can be small or large irrespective with the size and are varied with respect to the place and time where we use (Lu, Xinjiang, Zhiwen Yu, Bin Guo, and Xingshe Zhou, 2014). In the IoT era, every object and devices are not only interconnected but also interacted with each other, which making it possible to recognize events and changes in their surroundings.

Corresponding author:* **Veerraju T
Department of CSE, Aditya College of Engineering, Surampalem, Andhra Pradesh, India

The advantages of IoT are unlimited and its applications are altering based on the way we live and work by saving the time and resources, and offering the new opportunities for growth, innovation, and the exchange of information between different entities. By 2020, it is envisage that Internet of Things will significantly expanded with more than 50 billion outstandingly specialized devices (excluding PCs, tablets and smart phones), which is an remarkably large number. As a result, the extinction of the interconnected entities of an outsized network will definitely cause new security, privacy, and trust threats that put all those devices at a high risk, thus harming the affiliated users (D. Singh, G. Tripathi, and A.J. Jara, 2014).

Fog computing is the only new paradigm which can address the security threats in the rapid development and ampler adoption of IoT devices in our lives. In view of the fact that the devices which are interconnected have a direct impact on the lives of users and there is an urgent need for a well-defined security threat classification and a proper security infrastructure with the new systems and protocols which can alleviate the security confront in Fog.

We define the security most well known attacks on Fog systems. It introduces the category of the attacks based on the layers in the IoT. We focused mainly attacks on the network layer of the IoT. It suggests future security directions to cover the diversity of challenges in IoT-Fog based networks.

This paper presents various sections as follows: In section 2, provides an overview of Fog computing. The goals of the Fog security are explained in Section 3. In Section 4, the related work done on security of Fog is given. Section 5, provides a classification of the security challenges in Fog Systems. Then section 6, establishes a new security directions to

countermeasure these threats and finally section 7 conclusions are given.

Fog Overview

The users will be notified before storing the data into the cloud, analyzed and preprocessed to generate a new kind of patterns from the collected data. A new paradigm is required for this is which is referred to known as Fog computing. In the fog computing process, application comes to the data, not the data to the applications (W. Shi and S. Dustdar, 2016). Fog computing is supposed to be an extension of the cloud but not a complete replacement of it. When the number of devices connected to the internet has been increased at a rapid speed and even development in the Internet of things has led this number to increase drastically. In near future, we may predict that it is very much difficult to storing of the data and retrieving it from the cloud because, it is a full of sensors and there would be huge amount of data produced by these devices.

Characteristics of Fog computing

Fog computing is a distributed architecture which provides cloud-like services to edge of the network. It influences IoT and fog/edge resources along with its own infrastructure as shown in Fig 1. In quintessence, the technology deals by utilizing the clients or fog devices nearby users to carry out a considerable amount of storage, communication, control, configuration, and management with the help of IoT. This approach benefits from edge devices which are close proximity to nodes or sensors, at the same time as changing the on-demand scalability and service of cloud resources. The involvement of the Fog computing are the components of data-processing or analytics applications running in IoT structure and edge of the devices. It also facilitates the services and programming of computing, networking, and storage services between data centers and fog devices. In addition, it supports location mobility, resource management and interface heterogeneity, and distributed data analytics to address the requirements of widely IoT applications that need low latency (R. Buyya and A. Dastjerdi 2016).

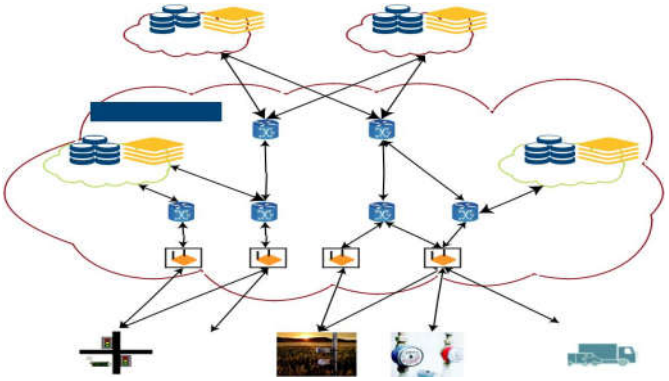

Fig 1 A fog-computing environment

Components of Fog computing

The architecture of the fog-computing is depicted in Fig 2. Fog systems generally use sensing the data and actuate then, processing various patterns. The Sensors streams the data to the IoT networks, other applications running on fog devices subscribe to and process the information, and the obtained in-sights are translated into actions sent to actuators. Fog systems use programming interfaces to make composite functionalities. Where the components at the resource-management layer use information from the resource-monitoring service to track the state of available cloud, fog, and network resources and process incoming tasks to identify the best one. With multiuser applications, the resource-management components prioritize the tasks of the various participating users or programs. Fog and cloud resources communicate using device-to-device (D2D) standards such as MQTT (formerly MQ Telemetry Transport) and the Constrained Application Protocol (CoAP). Software-defined networking (SDN) architecture helps with the well-organized management of heterogeneous fog networks.

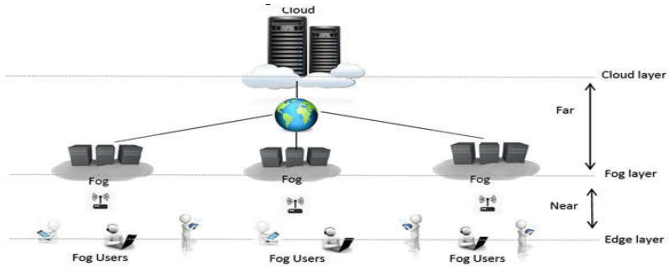

Fig 2. Fog computing architecture

Software systems of Fog computing

Fog computing based IoT environments utilized to build various prominent software systems for applications. Cisco IOx provides device management and enables D2D services in fog environments (F. Bonomi *et al*, 2014). Using device abstractions provided by Cisco IOx APIs, applications running on fog devices can communicate with other fog devices via D2D protocols. Cisco Data in Motion (DMo) enables data management and analysis at edge of the network and is built into products that Cisco Systems and its partners provide. Local Grid's fog-computing platform is software installed on network devices in smart grids. It provides reliable D2D communication between devices and data-processing services without going through the cloud. Cisco Par Stream's fog-computing platform enables real-time IoT applications.

Fog computing applications

The Fog computing IoT based environment provides various applications to the cloud. Fog computing, one of the key research area in recent years, together with IoT bring rapid advancements in various applications. Some of them are discussed below:

Healthcare Monitoring

In Healthcare sector, where a real-time processing and event response is more and more critical, then the Fog computing could be useful. One of the proposed systems utilizes fog computing to detect, predict, and prevent falls by stroke patients (Y. Cao *et al* 2015). The fall-detection learning algorithms are dynamically deployed across fog devices and IoT resources. Many of the researches proved that the system had a lower response time and consumed less energy than cloud-only approaches. A prominent fog computing–based smart-healthcare system needed which enables the mobility support, low latency, and location and privacy awareness.

Smart utility services

The smart utility services such as smart grid, smart transportation and smart cities, etc., are most of the real-time applications implemented by using Fog computing, whose

focus is improving energy generation, delivery ,transportation, traffic control and smart utility services in cities and billing. In those environments, fog/edge devices can report more fine-grained energy-consumption details (for example, hourly and daily, rather than monthly, readings) to user's mobile devices than traditional smart utility services. These edge devices calculate the cost of power consumption throughout the day and advise which energy source is most cost-effective at any given period of time or when home appliances should be turned on to minimize utility use. Similarly, connected vehicles in the smart transportation system have to know the current traffic system.

Other applications such as augmented reality, cognitive systems, and gaming

The augmented reality applications are latency sensitive, which are computing for low latency technologies like Fog. It plays major role in enhanced application. For example, the EEG Tractor Beam augmented multiplayer, online brain–computer-interaction game performs continuous real-time brain-state classification on fog devices and then tunes classification models on cloud servers based on electroencephalogram readings that sensors collect (J. Zao *et al*, 2014). A wearable cognitive-assistance system which uses Google Glass devices to help people with less psychological acuteness performs different tasks including telling them the names of people they meet but don't remember. For time-sensitive tasks, the system streams video from the Glass camera to the fog devices for processing. In this application, devices communicate with the cloud for delay-tolerant jobs such as error reporting and logging. The system reveals the way the fog devices greatly decreases the end-to-end latency.

Security goals in Fog network

Fog is a relatively new paradigm. There is a need to identify its security goals. To successfully achieve this, we need to understand that Fog is an implementation of network layer in IoT and edge devices and an integration of existing network infrastructures (e.g. wireless sensor networks, RFIDs based sensor networks, Cloud Computing, IoT, and the Internet etc.). Therefore, all of the security challenges and threats of each layer are passed by default onto the IoT system that utilizes these technologies. Further, adversaries can easily capture the nodes, which is in edge then there is the possibility of additional security threats which can arise from the coexistence and collaboration of the different technologies. The most enviable security objective of Fog is to protect the collected data, because the data collected through physical devices may also include sensitive user information. For this purpose the security of any Fog system needs to be flexible regarding data-related attacks and provide trust, data security and privacy. We study typical attacks which are in different levels in Fog Infrastructure.

Security and Privacy in Fog

The data security and privacy refers to the guard of any collected or stored information in any Fog system. The confidentiality and privacy information can be easily available to adversaries. Thus, Fog system needs efficient security mechanisms that can preserve data privacy and to provide data confidentiality, integrity, and availability. This can be achieved by utilizing authentication, access control, data encryption, data availability and redundancy through back-ups and etc.

Related work

We have been widely studied on security challenges and security issues in various fields like Wireless sensor network security and cloud security. The security mechanisms in cloud are not sufficient and suitable for Fog environment. Security in Fog research has not comprehensively investigated how to provide a proper classification of security challenges. However, most of the research papers address only specific types of threats based on specific security objectives (D. Singh *et al*, 2014;H. Suo, J. Wan *et al*, 2012;Y. Song, 2013). Most of the authors address various attacks like man in the middle attack, sink-hole attack, node capture attack etc. Compared to the previous work after investigation of Good number of papers, our paper focuses to provide a more extensive list of attacks and countermeasures. We also aim to provide various security challenges at the different levels of IoT architecture. Finally, (D. Chen, G. Chang *et al*, 2011; F. Bao and I. Chen, 2012; F. Bao, I. Chen and J. Guo, 2013) number of papers have focused on the security and privacy issues in Fog on different applications and expanded future directions in Fog infrastructure.

Classification of Security Challenges

This paper attempts to capture attacks in Fog systems. Our classification is unique compared to other classifications as it divides the different attacks under three distinct classes: Physical, Network, and Software attacks. A Fog network can be attacked physically, or attacked from within its network, or from applications on the system. Fog is implemented using various existing network technologies (e.g. wireless sensor networks, RFIDs based sensor networks, Cloud Computing, IoT, Fog, and the Internet etc.). Thus, there is a need for a proper categorization of the attacks such that it encapsulates all of the different types of threats, so that better counter measurements can be developed and implemented for securing it. A summary of the classification of the attacks is shown in Table 1 which is given below.

Table 1. Classification of Attacks

Physical Attacks	Network Attacks	Software attacks
Node capture Attacks	Traffic analysis Attacks	Virus and Worms
RF Interference	RFID Spoofing	
Node Jamming	RFID cloning	Spyware
Malicious node Injection	Unauthorized access	
Physical damage of the node	Sinkhole Attack	Trojan Horse
Social Engineering	Man in the Middle Attack	
Malicious code Injection on the node	Sybil Attack	Denial of service

Physical Attacks

These kinds of attacks are focused on the lower layer of the architecture which is edge of the network very near to the users in the Fog system. The attacker needs to be physically close to the network and attempt to get the information within the devices like sensors, RFIDs, etc. These kinds of attacks that harm the lifetime or functionality of the hardware are also included in this category. Now, we will explore these attacks (Ioannis Andrea *et al*, 2015).

Node-Capture attack

Sometimes, it is possible to the attacker by physically changing the entire node or some part of its hardware can be scratched or even electronically passing the messages and gain the access from the nodes and alter sensitive information to a sensor node. These kinds of attacks can have serious implications on the structured network. To detect,

cryptographic algorithms are needed to study against the node capture attack.

RF Interference on RFIDs

A DoS attack can be implemented on any RFID tag by creating and sending malicious and noisy signals over the RF signals which are used by the RFIDs for communication. The noisy signals will obstruct with the RF signals delayed communication. Fog has to define against such malicious signals.

Node Jamming in WSNs

This is similar to the Radio Frequency Interference physical attack explained earlier for the RFIDs with the difference that these kinds of attack are based on the Wireless Sensor Networks. The adversary can obstruct with the radio frequencies of the wireless sensor nodes, blocking the signals and refused the communication to that kind of nodes. If the attacker can succeeded to squeeze the sensor nodes, he can successfully deny the service of the Fog network. Fog also needs to define the cryptographic algorithms.

Malicious Node Injection

The adversary can physically placing a new malicious node between two or more communicating nodes of the Fog network, hence controlling all data flow to and from the nodes and their operation. This is known as Man in The Middle Attack. For the fog networks, the major issue to develop cryptographic algorithms is to defeat such kind of attacks.

Physical Damage

The adversary can physically damage devices of the Fog network for his own gain. This kind of attack is an attack that deals with security of the area or building that hosts the Fog system. It differs from Node Tampering attack. As in this situation, the adversary tries to directly damage the Fog system with the purpose of impacting the availability of the service.

Social Engineering

The attacker manipulates users of a Fog system, to extract private information or to execute certain actions that would serve up his goals. This kind of attack is put under the physical attacks category because the attacker needs to be physically interacting with the Fog network users to attain the goals.

Malicious Code Injection

The attacker compromises a node by physically injecting it with malicious code that would give him access to the Fog system. For example imagine an attacker inserting a USB stick with harmful software (i.e. virus) onto the node. This would mean that the attacker could gain full control of the node or even control of the whole system.

Attacks on the Network

These attacks are centered on the Fog network resources. In the Fog environment, most of the devices are connected wireless network but attacker does not necessarily need to be close to the network for the attack to work.

Traffic Analysis Attacks

An attacker can inhale out the secret information or any other information flowing from the RFID technologies because of their wireless characteristics. Also, in almost all of the attacks an attacker first tries to gain some network information before he employs his attack. This is done using inhaling applications like port scanning application, packet sniffer applications etc.

RFID Spoofing

During the data transmission from RFID tags, signals are spoofed by the attacker. Then the adversary can send the data containing the original tag ID and get the full access to the system making it is to be valid from the original source.

RFID Cloning

An attacker clones an RFID tag by copying data from the victims RFID tag, onto another RFID tag. Although, the two RFID tags have identical data, this method does not reproduce the original ID of the RFID, making it possible to distinguish between the original and the compromised, unlike the event in the RFID spoofing attack.

RFID Unauthorized Access

The most of the RFID systems may not have proper authentication. Because of that, tags can be accessed by anyone. In such circumstances, the attacker can read, modify or delete data from the RFID node. For this reason, The Fog networks are needed authentication mechanisms against these attacks.

Sinkhole Attack

The attackers decoy all traffic from WSN nodes, hence creating an allegorical sinkhole. This type of attack breaches the confidentiality of the data and also denies the service to the network by dropping all the packets instead of sending them to the required destination.

Man in the Middle Attack

The attacker over the Fog network manages to interfere between two communicating sensor nodes, accessing restricted data, violating the privacy of the two nodes by monitoring, eavesdropping and controlling the communication between the two sensor nodes. Unlike the Malicious Node Injection from the Physical Attacks category, the attacker does not necessarily need to be physically there for this kind of attack to be successful, but relies solely on the network communication protocols of a Fog system.

Software Attacks

The main sources of security vulnerabilities in any computer system are the kind of attacks known as software attacks. Software attacks exploits the system by using Trojan horse programs, worms, viruses, spyware and malicious scripts which can pinch information, alter with data, deny service and even harm the devices of a Fog system.

Phishing Attacks

The spoofing and authentication credentials of a user can be accessed by attacker through phishing attacks. The phishing attacks can be mitigated by secure authentication and identification.

Virus, Worms, Trojan horse, Spyware and Aware

An adversary can infect the system with malicious software resulting in a variety of outcomes such as stealing information, tampering data or even denial of service.

Denial of Service

An attacker can execute DoS or distributed denial of service DDoS attacks on the affected IoT network through the application layer, affecting all users in the network. This kind of attack can also block the legitimate users from the application layer giving full application layer access to the attacker to the databases and private sensitive data.

Security Directions

In this part we will provide future directions for security mechanisms based on the classifications presented earlier. A Fog network of IoT system consists of three different layers each with vulnerabilities and security attacks. To address these attacks and to successfully protect the Fog network in IoT system, this section presents a multi-layered security approach that should be structured to give an optimal layered protection at each layer in an IoT system as shown in the Table 2. A detailed description of the table is explained below.

Physical Layer Security

Secure Booting: Authentication and the integrity of the software on the device should be verified using cryptographic hash algorithms, which would provide digital signatures. However, because of the low processing power on most of the devices and their need for ultra-low power consumption most cryptographic hash algorithms cannot be implemented. Apart from NH and WH cryptographic hash functions that are optimal for ultra-low power consumption devices.

Device authentication*:* When a new node is introduced to the network, it should authenticate itself before receiving or transmitting data, to ensure it is identified correctly before authorization and keeping malicious devices out of the system. Various authentication mechanisms are used to authenticate the user identity such as digital certificates or certificate authorities.

Data integrity*:* Integrity mechanisms should be provided at each node, to ensure no modifications occurred on sensitive data. Integrity mechanisms like SHA-1, HMAC are used to calculate the digest value and verified at the receiver domain which is equal the only allow the node, but for more secure Cryptographic hash function should be applied.

Data Confidentiality*:* All RFID Tags, IDs and data should be encrypted on each device before transmission of data to ensure confidentiality. Strong encryption algorithms like ECDH, ECC are implemented. Some of the algorithms implemented on physical layer which have lower power consumption and less processing power. Furthermore, various algorithms need to be implemented to provide the confidentiality to the node.

Anonymity*:* In some cases hiding sensitive information like the location and identity of the nodes is crucial. Although Zero-Knowledge approach would be the optimal solution for anonymity. It cannot be implemented on low power devices as it is a very strong algorithm and needs a lot of processing power. Hence K- anonymity approach best fits the job for low power devices such as the devices used in a Fog system.

Network Layer Security

Data privacy*:* Illegal access to the sensor nodes can be prevented, using authentication mechanisms and point to point encryption.

Routing security*:* Secure routing is very important to the acceptance and use of sensor networks for many applications, but the majority of used routing protocols are insecure. However, security of routing can be ensured by provided that multiple paths for the data routing which improves the ability of the system to detect an error and keep performing upon any known of failure in the system. Also, encryption and authentication mechanisms increase the security level of routing data.

Data integrity*:* Using cryptographic hash functions, the integrity of the data received on the other end is confirmed. In case of prove of tampering of data, error correction mechanisms could be introduced to mitigate the problem.

Application Layer Security

Data security*:* Authentication Encryption and Integrity mechanisms are critical at this level for insuring the privacy of the whole system and protecting against data theft. It prevents unauthorized access to the system and ensures the confidentiality of the system data.

Access Control Lists *(ACLs):* Setting up policies and permissions of who can access and control the Fog system, is a crucial part as this ensures the privacy of the data and the well being of the system. ACLs can block or allow the incoming or outgoing traffic, and give or block access to requests from different users inside or outside of the network.

Firewalls*:* This is an extra effective layer of security that will help block attacks that authentication, encryption and ACLs would failed to do so. Authentication and encryption passwords can be broken if weak passwords were selected. A firewall can filter packets as they are received, blocking unwanted packets, unfriendly login attempts, and DoS attacks before even authentication process begins.

Anti-virus, Anti-spyware *and* ***Anti-adware****:* Security software like antivirus or anti spyware is important for the reliability, security, integrity and confidentiality of the Fog system.

Table 2. Security countermeasures

IoT Layer	Counter Attacks for the Specific Layers	Counter Attacks for All Layers
Physical Layer	1) Secure Booting for all IoT devices a) Low power Cryptographic Hash Functions 2) Device Authentication using Low Power Techniques a) Data Integrity b) CRC – Cyclic Redundancy Check c) Checksum d) Parity Bit e) WH Cryptographic Hash Function 3) Data Confidentiality a) Encryption Algorithms like Blowfish and RSA 4) Data Anonymity a) K- Anonymity	1) Risk Assessment b) Finding New Threats c) Applying Updates d) Applying Patches e) Providing Improvements f) Upgrading Systems
Network Layer	1) Secure Communication between the devices a) Network Authentication – challenge-response mechanisms b) Point-to-Point Encryption for the confidentiality of the transmitted Data c) Cryptographic Hash Functions for the Integrity of the transmitted Data 2) Implementation of Routing Security a) Use of Multiple Paths b) Encrypting Routing Tables c) Hashing Routing Tables 3) Secure User Data on the Devices a) Data Authentication b) Data Confidentiality; Encryption Schemes of encrypting the data c) Data Integrity; Cryptographic hash functions	2) Intrusion Detection Mechanisms specific to Fog Systems 3)Securing the Fog Premises a) Physical Barriers b) Intrusion Detection Alarms c) Monitoring Devices d) Access Control Devices e) Security Personnel
Application Layer	1) Data Security a) Authentication; biometrics, passwords, etc. b) Confidentiality; Strong Encryption Schemes (AES) c) Integrity, Cryptographic Hash Functions 2) Access Control Lists (ACLs) 3) Firewalls 4) Protective Software a) Anti-virus b) Anti-adware	4) Trust Management a)Trust relation between layers b)Trust of Security and Privacy at each layer c)Trust between Fog and User

CONCLUSION

Fog Computing has been one of the major research area for the last decade, IoT can be classified different layered architecture, where interconnected with different objects using existing technologies. In the direction of many research attempts security and privacy issues then require a reconfigurable Fog architecture for the applications that can multiple scenarios, Fog devices that allow storage, communication and

computational resources to be efficiently used at the edge of the network .This paper explores the various security goals required Fog environment and classified security attacks and their countermeasures based on the IoT architecture. We investigate the many papers to provide confidentiality, integrity and authentication services to implement trusted environment. Fog the Future directions, To implement trusted and security mechanisms to interact between the fog devices and provide secure communication over the fog network in IoT environment.

References

D. Singh, G. Tripathi, and A.J. Jara. "A survey of Internet-of-things: Future vision, architecture, challenges and services." In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pp. 287-292. IEEE, 2014.

D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang "TRM-IoT: A trust management model based on fuzzy reputation for internet of things." Computer Science and Information Systems 8, no. 4 (2011): 1207-1228.

F. Bonomi *et al*., "Fog Computing: A Platform for Internet of Things and Analytics," *Big Data and Internet of Things: A Roadmap for Smart Environ-ments*, N. Bessis and C. Dobre, eds., Springer, 2014, pp. 169-186.

F. Bao and I. Chen, "Trust management for the internet of things and its application to service composition", in Proc. of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012, pp.1-6.

F. Bao, I. Chen and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems", in Proc. of IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISAD), (2013), pp.1-7.

H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648-651. IEEE, 2012.

Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", 2015 IEEE Symposium on Computers and Communication (ISCC), 6-9 July 2015.

J. Zao *et al*., "Augmented Brain Computer Interaction Based on Fog Computing and Linked Data," *Proc. 10th IEEE Int'l Conf. Intelligent Envi-ronments* (IE 14), 2014, pp. 374–377.

Lu, Xinjiang, Zhiwen Yu, Bin Guo, and Xingshe Zhou. "Predicting the content dissemination trends by repost behavior modeling in mobile social networks", *Journal of Network and Computer Applications*, 2014.

M. Friedemann, and C. Floerkemeier. " From the Internet of Computers to the Internet of Things." In From active data management to event-based systems and more, pp. 242-259. Springer Berlin Heidelberg , 2010.

R. Buyya and A. Dastjerdi, *Internet of Things: Principles and Paradigms*, Morgan Kaufmann, 2016.

W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer*, vol. 49, no. 5, 2016, pp. 78-81.

Y. Song, "Security in Internet of Things." (2013).

Y. Cao *et al*., "FAST: A Fog Comput-ing Assisted Distributed Analytics System to Monitor Fall for Stroke Mitigation," *Proc. 10th IEEE Int'l Conf. Networking, Architecture and Storage* (NAS 15), 2015, pp. 2-11.

How to cite this article:

Veerraju T *et al* (2017) 'A Study on Fog Computing Based Iot Environment: Security Issues And Challenges ', *International Journal of Current Advanced Research,* 06(12), pp. 8139-8144. DOI: http://dx.doi.org/10.24327/ijcar.2017.8144.1297

****