Fog Computing Security Challenges and Future Directions

A bottom-up view to the fog system hierarchy

By Deepak Puthal, Saraju P. Mohanty, Sanjivani Ashok Bhavake, Graham Morgan, and Rajiv Ranjan

The perception of the fog computing is to bring the virtual presence in day-to-day objects. The lowest layer of fog architecture is Internet of Things (IoT), which brought revolution by changing ordinary objects to smart objects that will automatically sense and process data to provide better solutions. In an IoT the smart objects connected over the Internet communicate with each other and exchange data with fog server to improve services that will benefit humanity. There are some challenges to achieve these benefits of IoT. This article discusses a three-layered fog architecture and highlights potential security threats and solutions at each layer. Finally, open research issues are discussed at all three layers of fog hierarchy.

1. Fog Computing Architecture

Fog computing decentralize the computing infrastructure without depending on centralize computing such as cloud computing. Fog computing is a paradigm proposed to integrate IoT and cloud concept to support user mobility, low latency and location awareness [1]. Fog computing (also known as edge computing) deploys datacenters in the network edges, it offers location awareness, low latency, and improves quality-of-services (QoS) for near real-time applications. Typical examples include transportation, industrial automation, agriculture and other smart cities applications [2]. Fog infrastructure supports heterogeneous devices, such as end device, edge devices, access points, and switches. Fog servers are considered as micro datacenter by inheriting cloud services to network edges. The datacenters positioned for near real-time applications, big data analytics, distributed data collection, and offers advantages in various applications in smart cities.

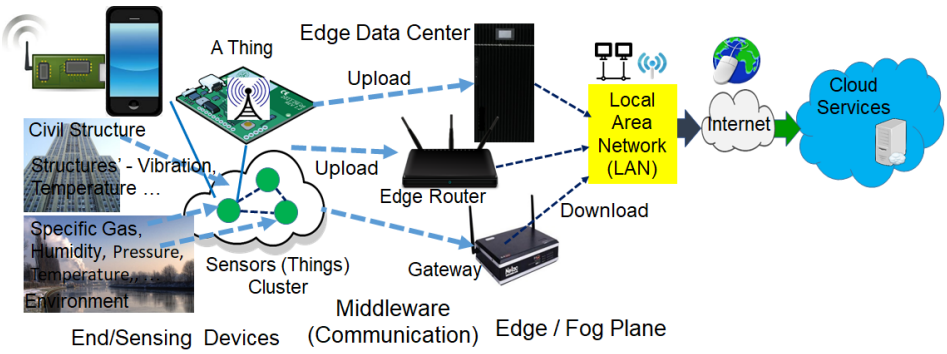

FIGURE 1. Three-layer architecture of fog/edge computing.

Fog computing is deployed to overcome latency issues. However, Fog computing completely ignore the cloud due to the limited sources at the fog server and always relies on the cloud for complex processing. Many research issues relating to Fog computing are emerging due to its ubiquitous connectivity and heterogeneous organization. In the Fog computing paradigm, key issues are the requirements and the deployment of Fog computing environment. This is because the devices that exist in Fog environments are heterogeneous: therefore, the question that arises is how will Fog computing tackle the new challenges of resource management and failure handling in such a heterogeneous environment? Hence, it is necessary to investigate the very basic requirements for other related aspects including deployment issues, simulations, resource management, fault tolerance, and services. Security issues in fog hierarchy is a key issue, where this article highlighted existing security challenges and solutions of different layer of Fog hierarchy. This article does not consider cloud as the part of fog hierarchy. The computing aspect of 3-layer fog hierarchy (Figure 1): (1) sensing layer, (2) middleware (communication medium), and (3) fog server. The Fog hierarchy is divided as into various communication layers (Figure 2). Security challenges of three-layer fog hierarchy can have both computing and communication prospective.

2. Fog Computing Properties

The working model of Fog computing can be explained with three-layers architecture (Figure 1 and 2).

2.1. Sensing layer

Sensing layer is the bottommost layer in the 3-layered architecture. Physical layer and Datalink layer of communications stack together forms the sensing layer (Figure 2). The sensing layer is made up of numerous sensing technologies such as Radio Frequency Identification (RFID) tags, Wireless Sensor Networks (WSN), Near-Field Communications (NFC) to build IoT infrastructure [3, 4]. Following listed functions performed in the sensing layer:

- Uniquely Identify physical objects as a part of IoT to collect data on these objects.
- Convert the sensed data to digital signals.
- Send data collected from the surrounding objects to upper layers for network transmission and processing.

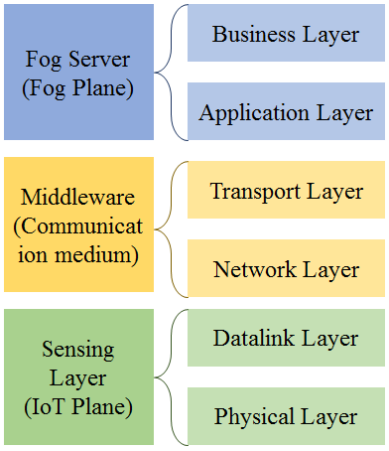

FIGURE 2. Fog Hierarchy in terms of network communications layers.

2.2. Middleware

The Network layer and Transport layer together forms Middleware of Fog hierarchy. The data received from bottom layer processed at middleware and transmit to fog server for further evaluation. Abundant amount of data is processed using network technologies such as LAN, wireless/wired networks and transmission medium such as Wi-Fi, Bluetooth and Zigbee [5]. The following functions performed in the middleware:

- Sensing layer information is processed with network support.
- Processed sensing data is received and transmitted to upper layer.
- Secure data transmission assign IPV6 addressing to the physical objects.

2.3. Fog server

The fog server layer can be further divided in to application layer and business layer. This layer acts as a front end to users. The main function of this layer is to facilitate management of different applications. IoT application deployment platforms are used to differentiate between various applications such as transportation, health, banking [2, 10]. The business sub layer manages the end data its security.

3. Fog Computing Security Threats

Potential security threats and existing solutions of three-layer fog hierarchy (Figure 3).

3.1. Sensing Layer

The sensing layer of fog architecture is also known as object layer. The sensing technologies used to sense data from physical objects include WSN, RFID tags, and NFC. As the number of new objects connected to IoT are increasing rapidly, data senses are abundant, and security of this data is at risk [4, 6, 7].

A. Security threats in sensing layer

Potential security threats of fog computing sensing layer are listed as follows.

- Node Capture/ Device Tampering: Things at the IoT gateway are weaken and important data is leaked which puts the security of entire network into danger.

- Spoofing Attack: In this attacker's masquerades the data and send fake data to the network. The things take the false identity of the original source enabling full access of system to the attackers.
- Signal Jamming: Generates interference in communication between network devices with the radio frequencies.
- Malicious Data: A malicious node if added to the system infects the whole system by spreading malicious data.
- Denial of Service Attack/ Path based DoS: floods sensor nodes by injecting replayed and false packets. This attack results in exhaustion of batteries, network resources and cut down the system service availability.
- Node Outage: Most of the devices in the network are cut down which leads to loss of connectivity.
- Replay Attack: The original data packets are replaced by the false data packets and network trust, authentication is put to risk.
- SYBIL Attack: The aggregate message is changed to a false message as a result of malicious node present in the network which give negative reinforcements. The ability of selecting most effective link is blocked.

B. Security solutions in sensing layer

Existing solutions to overcome security threats of fog computing sensing layer includes authorization, cryptography, steganography, image processing, spread spectrum communication, jamming report, error correcting codes, collision detection.

- Cryptographic processing includes encryption, decryption, key and hash generation, verify hashes used to guarantee privacy of data [9].
- Image data is secured using image compression and Cyclic Redundancy Check [9].

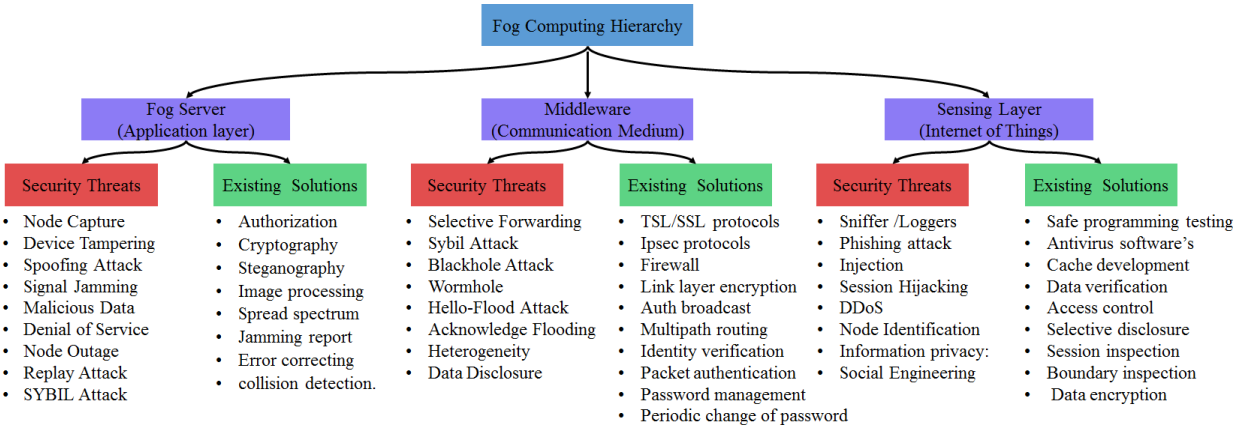

FIGURE 3. Security threats and solutions classifications in fog computing.

3.2. Middleware

At middleware, secure transmission of sensed data and its storage is of main concern. Thus storage, processing of data is involved this layer deals with confidentiality, integrity and availability issues. It could be classified as the CIA triode of security mechanism. Some of the common attacks that might occur in this layer are DoS, eavesdropping and many more [4, 6, 7].

A. Security threats in middleware

Potential security threats of fog computing middleware are listed as follows.

- Selective Forwarding: Some data packets are blocked and selectively dropped by malicious node. The major two types of selective forwarding attacks are dropping data packets and the infected node randomly skips routing data packets.
- Sybil Attack: In this attack device takes multiple identities. A single node is given multiple identities reducing the efficacy of fault tolerant schemes.
- Blackhole Attack: An unfaithful routing information is created, and all the data packets are diverted to the sink hole. This may cause network congestion and packet drop.
- Wormhole: The bits of data are relocated in the network by tunnelling the bits of data [4].
- Hello-Flood Attack: The attacker floods the channel with false data packets to create network congestion. Also persuade every node that the malicious node is their neighbor to participate in packet transmission.
- Acknowledge Flooding: Similar to DoS attack, attackers send fake information to neighboring nodes using acknowledgment.
- Heterogeneity: Numerous technologies and security protocols involved makes it difficult to maintain and coordination thus making the system vulnerable.
- Scalability: The untraceable number of devices connecting and disconnecting from the system, and which leads to lack of authentication, congestion and depletion of resources.
- Data Disclosure: Attackers use data retrieval techniques to extract information form node, which can lead to privacy risks.

B. Security solutions in middleware

Existing solutions to overcome security threats of fog computing middleware includes TSL/SSL protocols (secure transport layer), IPSec protocols (secure network layer), IPS, PPSK, firewall.

- Link layer encryption, authenticated broadcast, multipath routing, identity verification and packet authentication.
- Password management, policies and periodic change of password.

3.3. Fog Server

Fog server is the front end of the Fog hierarchy and therefore needs different security standards as per specific applications. As different applications have different requirements, and the task of making this level secure gets very complicated and hard. The security threats vary as per the protocols used depending on the suitable protocol and use in network. The protocols involved are MQTT, AMQP, CoPA and XMPP which face the risk of threats as listed follows [4, 7, 8].

A. Security threats in fog server

Potential security threats of fog server layer are listed as follows.

- Sniffer /Loggers: The attackers use sniffing to extract important data such as password, email and FTP files. Many protocols in the network are vulnerable to sniffing.
- Phishing attack: The email address of the main authority is used to gain credentials and damage data.
- Injection: It is a common attack by injecting infected codes into the application executed on the server. This attack can result in to loss of data, and accountability on application [8].
- Session Hijacking: This attack is basically hijack someone else's identity. Then further gains access to personal identities due to flaws in authentication management.
- DDoS: Multiple infected systems are used to damage the single system.
- Node Identification: Each application has different set users at different phases, attacker gains illegal access and harm the application [4].

- Information privacy: When data protection techniques are vulnerable, the results in loss of data and long-term damage to the system.
- Application Specific Vulnerabilities: The vulnerabilities left during the development of the application ant it can be later exploited by attackers. When programmer writes non-standard software's then hackers can easily hack in to the system.
- Social Engineering: Attackers gain vital application information form users by befriending them and later misusing their information.

B. Security solutions in fog server

Existing solutions to overcome security threats of fog server layer includes.

- Safe programming testing, Antivirus software's, Cache development, Data verification.
- Access control list, Selective disclosure, IPS, firewall, IDS, Session inspection [9].
- Boundary inspection and Data encryption to avoid the risk of primary leakage [9].
- Risk Assessment to identify threats in the network it involves: situation analysis and checks for risk acceptance levels.

4. Open Research Challenges

The Fog computing is a consequence of diverse physical objects and technologies where user's data is sensed, stored, managed and used at different layers of hierarchy. Due to limited research done on the Fog framework there are many research challenges to be addressed at various layers of its architecture (Figure 4).

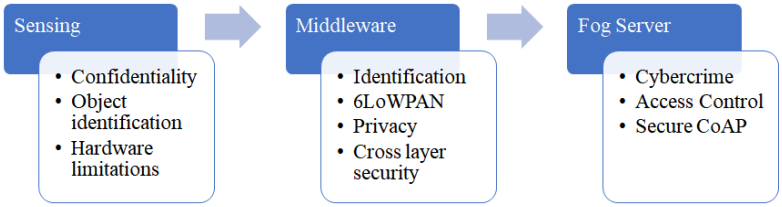

FIGURE 4. Open security research issues in fog computing.

4.1. Sensing layer

Most of the security vulnerabilities associated with the sensing layer, where IoT devices deployed in an unattended area. Some of the open security challenges are the following.

- IoT is an emergent platform formed by integration of millions of computing devices and massive amount of real time data is sensed form these devices. These devices are globally used and are powerful, compact and costly. Thus, some objects can contain malicious data and risk the security of IoT. Keeping a track on objects adding to IoT network is one of the biggest challenges.
- Limitations of sensing layer security with IEE.802.15.4 standards are another vital research challenge [4, 9]. Developed IEE.802.15.4 standard do not completely support the security of sensing layer thus limited secure communications are identified.
- Current IEE.802.15.4 standard does not completely support keying models and fail to protect acknowledge messages from confidential issues. This also highlights that existing end to end security mechanisms designed are not completely compatible with new objects adding to IoT platform.
- Hardware limitations for low cost devices with restricted range of Analog to Digital converter. In future migration of IoT system to non-orthogonal transmission scheme can be challenging due to ADC and device restrictions.
- Proper support and coordination between IoT devices are important to gain low power and reliable communication. Cooperative channel coding can be considered as an efficient sensing layer approach for IoT systems.
- Furthermore, research efforts should be made for the IoT system by checking the security updates and patches. Future research can be focused on making IoT layers to be trustworthy for data routing and processing.

4.2. Middleware

- The primary challenge at this level is designing an IoT middleware compatible for cloud and edge to support various IoT applications [4]. New devices in the sensing infrastructure makes the communication process faster.
- Low Power Wireless Area Networks (6LoWPAN) support end-to-end internet communications between sensing objects and other internet units in IoT fog communications [9]. Even though the suitable security mechanisms in regard to this technology are clearly acknowledged, the 6LoWPAN specifications only focuses on general security issues [9].
- Use of 6LoWPAN in IoT have several advantages for middleware security, but there are no proper mechanisms implemented. The research done in this technology is limited general security issues and security approaches like IPSec are yet to be explored completely [9].
- Restrictions of wireless sensing platform have made the adoption of middleware security mechanisms with 6LoWPAN challenging.
- There is a need to develop IoT compatible network and transport layer security schemes and mechanisms to guarantee IoT security and user data privacy protection.

4.3. Fog Server

- Existing Fog application protocols do not completely support security and therefore cannot protect system from security thefts. More research is required in developing protocols to protect fog systems form cybercrime issues.
- In Fog server with CoAP, security is supported using DTLS discussed various issues and limitations of DTLS with IoT security and need for further investigation [8].
- With DTLS limitations it is difficult to protect great amount of information processed in IoT and end up making the IoT network more complex and costlier.
- Improvement of DTLS to protect CoAP communications is one of the major challenges [9].
- Where further research can be focused to support the public key cryptographic as viability of cryptography sensing platforms in CoAP setting is currently restricting.

5. Conclusion and Future Scope

This article presents the current status of Fog computing research regarding its architecture security threats, existing solutions and open research challenges. The Fog system holds the potential to make better decisions and automatically improvise service experience in future. The constantly evolving technology and with various protocols, security mechanisms used to keep IoT secure becomes a priority. This update in technology and security issues question the sustainability of IoT, whether or not it will be a secure and sustained technology for the future. The complexity of the internet of things, it is essential that future IoT standards should be developed and implemented to ensure secure Fog system.

A fully holistic security solution is yet to be developed to determine all the security mechanisms required can work on constrained objects including to IoT platform. As the new devices add up their security at every stage should be guaranteed in various day to day application. The Fog system needs focus to decentralize the security model and best solution in current time in Blockchain. However, Blockchain needs substantial research contributions to make it suitable for Fog system [11].

ABOUT THE AUTHORS

Deepak Puthal (deepak.puthal@uts.edu.au) is a lecturer (assistant professor) in the Faculty of Engineering and Information Technology at University of Technology Sydney, Australia.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the University of North Texas, USA.
Sanjivani A. Bhavake (sanjivaniashok.bhavake@student.uts.edu.au) is a master student at University of Technology Sydney, Australia.
Graham Morgan (graham.morgan@ncl.ac.uk) is a senior lecturer at Newcastle University, UK.
Rajiv Ranjan (raj.ranjan@newcastle.ac.uk) is a Chair Professor of Computing Science and Internet of Things at Newcastle University, UK.

References

[1] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing", *IEEE Communications Magazine (COMM)*, Volume 56, Issue 5, May 2018, pp. 60--65.

[2] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine (CEM)*, Volume 5, Issue 3, July 2016, pp. 60--70.

[3] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review", in *Proc. of IEEE International Conference on Computer Science and Electronics Engineering*, 2012, 648-651.

[4] A. Tewari, and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework", *Future Generation Computer Systems*, 2018, in Press https://doi.org/10.1016/j.future.2018.04.027.

[5] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges", *Ad hoc networks*, vol. 10, no. 7, pp. 1497-516.

[6] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the internet of things", *IEEE Cloud Computing*, vol. 3, no. 3, 2016, pp. 64-71.

[7] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)", *International Journal of Computer Applications*, vol. 111, no. 7, 2015.

[8] S. N. Swamy, D. Jadhav and N. Kulkarni, "Security threats in the application layer in IoT applications," in *Proc. International Conference on IoT in Social, Mobile, Analytics and Cloud*, 2017, pp. 477-480.

[9] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues", *IEEE Comm. Surveys & Tutorials*, vol. 17, no. 3, 2015, pp. 1294-1312.

[10] Li Da Xu, Wu He, and Shancang Li, "Internet of things in industries: A survey", *IEEE Transactions on Industrial informatics*, vol. 10, no. 4, 2014, pp. 2233-43.

[11] D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Volume 38, Issue 1, January 2019, pp. 26--29.