Fog Computing Security Challenges and Future Directions

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

The perception of fog computing is to bring a virtual presence into day-to-day objects. The lowest layer of the fog architecture is the Internet of Things (IoT), which created a revolution by changing ordinary objects into smart objects that automatically sense and process data. In the IoT, smart objects connected over the Internet communicate with each other and exchange data with the fog server to improve services to customers. There are some challenges to achieving the benefits of the 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 the fog hierarchy.

FOG COMPUTING ARCHITECTURE

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

Fog computing is deployed to overcome latency issues. However, fog computing completely ignores the cloud because of 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 because of its ubiquitous connectivity and heterogeneous organization. In the fog computing paradigm, the key issues are the requirements and the deployment of the 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 handling failure in such a heterogeneous environment?

As a result, 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 the fog hierarchy are a key issue, and this article highlights existing security challenges and solutions of different layers of the fog hierarchy. We do not consider the cloud as the part of the fog hierarchy. The computing aspect of a three-layer fog hierarchy (Figure 1) is as follows:

1) the sensing layer
2) the middleware (communication medium)
3) the fog server.

The hierarchy is divided into various communication layers (Figure 2). Security challenges of the three-layer fog hierarchy can be in both computing and communication.

FOG COMPUTING PROPERTIES

The working model of fog computing can be explained with the three-layer architecture (Figures 1 and 2).

SENSING LAYER

The sensing layer is the bottommost layer in the three-layered architecture. The physical layer and datalink layer of communications stack together to form the sensing layer (Figure 2), which is made up of numerous sensing technologies, such as radio-frequency identification (RFID) tags, wireless sensor networks (WSNs), and near-field communications (NFCs), to build IoT infrastructure [3], [4]. The following is a list of functions performed in the sensing layer:

- uniquely identify physical objects as a part of the IoT to collect data on these objects

Digital Object Identifier 10.1109/MCE.2019.2893674
Date of publication: 8 April 2019

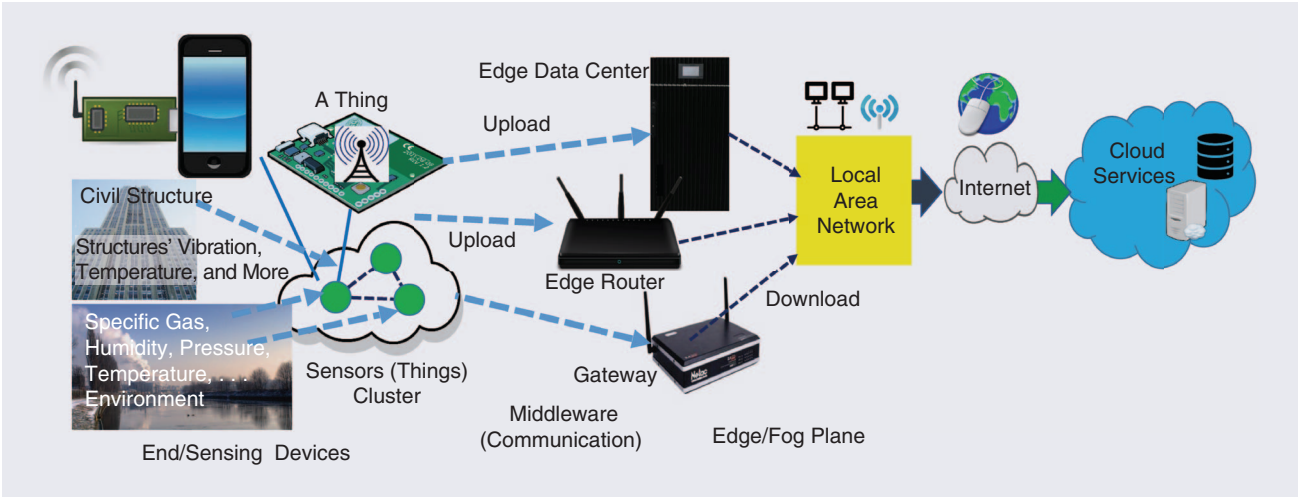

FIGURE 1. The three-layer architecture of fog/edge computing.

- convert the sensed data to digital signals
- send data collected from the surrounding objects to upper layers for network transmission and processing.

MIDDLEWARE

The network and transport layers together form the middleware of the fog hierarchy. The data received from the bottom layer are processed at the middleware and transmitted to the fog server for further evaluation. Abundant data are processed using network technologies, such as local area networks, wireless/wired networks, and transmission medium, such as Wi-Fi, Bluetooth, and Zigbee [5]. The following functions are performed in the middleware:

- Sensing layer information is processed with network support.
- Processed sensing data are received and transmitted to the upper layer.
- Secure data transmission assigns Internet Protocol version 6 addressing to the physical objects.

FOG SERVER

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

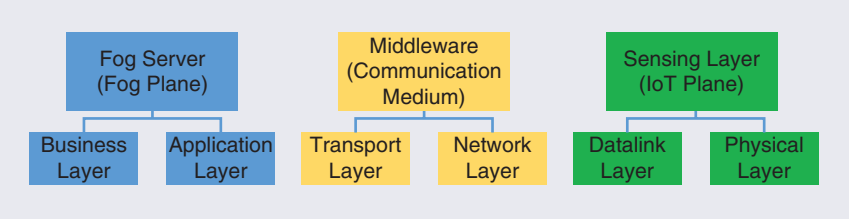

FIGURE 2. The fog hierarchy in terms of the network communications layers.

FOG COMPUTING SECURITY THREATS

Next, we present the potential security threats and existing solutions of the three-layer fog hierarchy (Figure 3).

SENSING LAYER

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

SECURITY THREATS IN THE SENSING LAYER

Potential security threats in the sensing layer are listed as follows.

- *Node capture/device tampering*: Things at the IoT gateway are weakened, and important data are leaked, which puts the security of the entire network in danger.
- *Spoofing attack*: In this, the attackers conceal data and send fake data to the network. The things take the false identity of the original source, giving the attackers full access of system.
- *Signal jamming*: Jamming generates interference in the communications between network devices using radio frequencies.
- *Malicious data*: A malicious node, if added to the system, infects the whole system by spreading malicious data.
- *Denial of service (DoS) attack/path-based DoS*: This attack floods sensor nodes by injecting replayed and false packets. It exhausts batteries and network resources and cuts down the service availability of the system.
- *Node outage*: Most of the devices in the network are cut down, which leads to a loss of connectivity.
- *Replay attack*: The original data packets are replaced by false data packets, and network trust and authentication are put at risk.
- *Sybil attack*: The aggregate message is changed to a false message as a result of a malicious node that is present in the network, which gives negative reinforcement. The ability of selecting the most effective link is blocked.

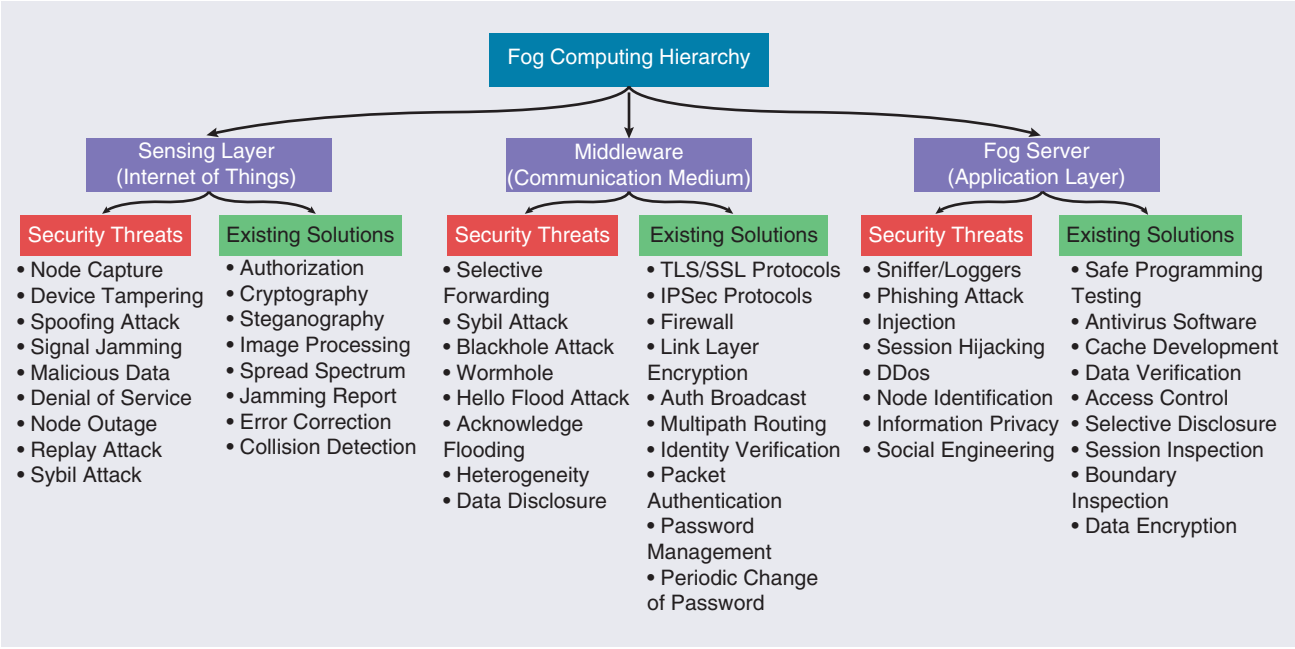

FIGURE 3. The security threats and solutions classifications in fog computing. DDoS: distributed DoS; TLS: transport layer security; SSL: secure sockets layer; IPsec: Internet Protocol security.

SECURITY SOLUTIONS IN SENSING LAYER

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

- Cryptographic processing includes encryption, decryption, key and hash generation, and verification of hashes used to guarantee privacy of data [9].
- Image data are secured using image compression and a cyclic redundancy check [9].

MIDDLEWARE

At the middleware level, the secure transmission of sensed data and its storage are the main concerns. Thus, storage and processing of data are involved, and this layer deals with confidentiality, integrity, and availability issues. It could be classified as the U.S. Central Intelligence Agency triad of security mechanisms. Some of the common attacks that might occur in this layer are DoS, eavesdropping, and many more [4], [6], [7].

SECURITY THREATS IN MIDDLEWARE

Potential security threats of fog computing middleware are as follows.

- *Selective forwarding*: Some data packets are blocked and selectively dropped by a malicious node. The two major types of selective forwarding attacks are the dropping of data packets and the infected node randomly skipping the routing of data packets.
- *Sybil attack*: In this attack, the device takes multiple identities, reducing the efficacy of fault-tolerance schemes.
- *Blackhole attack*: 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 tunneling to a different storage location [4].
- *Hello flood attack*: The attacker floods the channel with false data packets to create network congestion. They also persuade every node that their neighbor is a malicious node when participating in packet transmission.
- *Acknowledge flooding*: Similar to a DoS attack, attackers send fake information to neighboring nodes using acknowledgment.
- *Heterogeneity*: The numerous technologies and security protocols involved make it difficult to maintain and coordinate transfers, thus making the system vulnerable.
- *Scalability*: An untraceable number of devices connect and disconnect from the system, which leads to a lack of authentication, congestion, and depletion of resources.
- *Data disclosure*: Attackers use data retrieval techniques to extract information from a node, which can lead to privacy risks.

SECURITY SOLUTIONS IN MIDDLEWARE

The existing solutions to overcome the security threats of fog computing middleware include transport layer security (TLS)/secure sockets layer protocols (secure transport layer), Internet Protocol security (IPSec) protocols (secure network layer), intrusion prevention system (IPS), private preshared key, and firewalls. Other solutions include link-layer encryption, authenticated broadcasting, multipath routing, identity verification and packet authentication as well as password management and policies and periodic password changes.

FOG SERVER

The fog server is the front end of the fog hierarchy and needs different security standards according to the specific application. Because 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 its use in the network. The protocols involved are Message Queuing Telemetry Transport, Advanced Message Queuing Protocol, Constrained Application Protocol (CoAP), and the Extensible Messaging and Presence Protocol, which face the following threats [4], [7], [8].

SECURITY THREATS IN FOG SERVER

Potential security threats to the fog server layer are 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 when infected codes are injected into the application that is executed on the server. This attack can result in a loss of data and accountability for the application [8].
- *Session hijacking*: This attack basically hijacks someone else's identity. Then, the attacker gains further access to personal identities because of flaws in authentication management.
- *Distributed DoS*: Multiple infected systems are used to damage a single system.
- *Node identification*: Each application has a different set of users at different phases, and the attacker gains illegal access, harming the application [4].
- *Information privacy*: When data protection techniques are vulnerable, the result is a loss of data and long-term damage to the system.
- *Application-specific vulnerabilities*: The vulnerabilities left during the development of the application can later be exploited by attackers. When a programmer writes nonstandard software, then hackers can easily hack into the system.
- *Social engineering*: Attackers gain vital application information from users by befriending them and later misusing their information.

SECURITY SOLUTIONS IN THE FOG SERVER

Existing solutions to overcome the security threats of the fog server layer include the following.

- safe programming testing, antivirus software, cache development, and data verification
- access control lists, selective disclosure, IPS, firewall, intrusion detection system and session inspection [9]
- boundary inspection and data encryption to avoid the risk of primary leakage [9]
- risk assessment to identify threats in the involved network: situation analysis and checks for risk acceptance levels.

OPEN RESEARCH CHALLENGES

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

SENSING LAYER

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

- The IoT is an emergent platform formed by the integration of millions of computing devices and a massive amount of real-time data that are sensed from 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 the IoT. Keeping track of objects added to the 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]. The developed IEEE 802.15.4 standard does not completely support the security of the sensing layer, and thus, limited secure communications are identified.
- The current IEEE 802.15.4 standard does not completely support keying models and fails to protect acknowledgment messages from confidential sources. This also highlights that existing end-to-end security mechanisms are not completely compatible with new objects that are added to the IoT platform.
- Hardware limitations for low-cost devices with a restricted range of the analog-to-digital converter. In the future, the migration of IoT systems to nonorthogonal transmission schemes will be challenging because of analog-to-digital converters 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 an efficient sensing layer approach for IoT systems.
- Research efforts should be made regarding checking security updates and patches for the IoT system. Future research can be focused on making IoT layers trustworthy for data routing and processing.

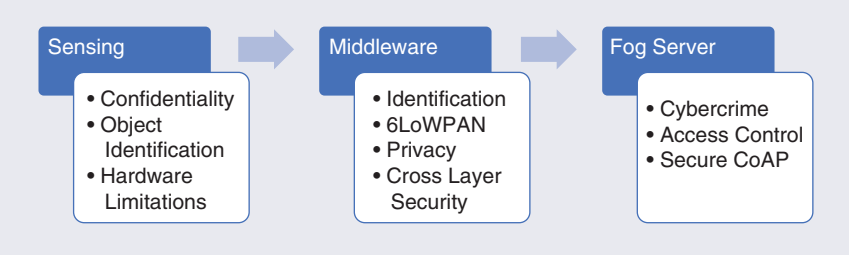

FIGURE 4. Open security research issues in fog computing. LoWPAN: Low-power wireless area networks.

MIDDLEWARE

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

FOG SERVER

- Existing fog application protocols do not completely support security and cannot protect the system from security threats. More research is required in developing protocols to protect fog systems from cybercrime issues.
- In a fog server with CoAP, security is supported using Datagram Transport Layer Security (DTLS), and research must discuss the various issues and limitations of DTLS with IoT security, which need further investigation [8].
- With DTLS limitations, it is difficult to protect the great amount of information processed in the IoT, which will end up making the IoT network more complex and costlier.
- Improving DTLS to protect CoAP communications is one of the major challenges [9].
- Further research can be focused on supporting public-key cryptography as a viable cryptographic sensing platform in the CoAP setting, which is currently restricted.

CONCLUSION AND FUTURE SCOPE

This article presented the current status of fog computing research regarding its architecture security threats, existing solutions to those threats, and the open research challenges. The fog system holds the potential to make better decisions and automatically improve the service experience in the future. Constantly evolving technology and security mechanisms with various protocols are used to keep the IoT secure, which is a priority. This update in technology and security issues questions the sustainability of the IoT and whether or not it will be a secure and sustainable technology for the future. Because of the complexity of the IoT, it is essential that future IoT standards be developed and implemented to ensure a secure fog system.

A fully holistic security solution has yet to be developed to determine all of the security mechanisms required that can work on constrained objects, including on the IoT platform. As the number of new devices adds up, security at every stage should be guaranteed in various day-to-day applications. The fog system needs focus on decentralizing the security model, and the best solution currently is blockchain. However, blockchain needs to be substantially researched to make it suitable for the 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, University of Technology Sydney, Australia.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a professor at the University of North Texas, Denton.

Sanjivani Ashok Bhavake (sanjivaniashok.bhavake@student.uts.edu.au) is a master's degree student at the University of Technology Sydney, Australia.

Graham Morgan (graham.morgan@ncl.ac.uk) is a senior lecturer at Newcastle University, Newcastle on Tyne, United Kingdom.

Rajiv Ranjan (raj.ranjan@newcastle.ac.uk) is a chair professor of computing science and the Internet of Things at Newcastle University, Newcastle on Tyne, United Kingdom.

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 Commun. Mag.*, vol. 56, no. 5, pp. 60–65, 2018.

[2] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, 2016.

[3] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: a review," in *Proc. IEEE Int. Conf. Computer Science and Electronics Engineering*, 2012, pp. 648–651.

[4] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, 2018. doi: 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. 1497–1516,

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

[7] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Applicat.*, vol. 111, no. 7, pp. 1–6, 2015.

[8] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IoT applications," in *Proc. Int. Conf. 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," *Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 2015.

[10] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, 2014.

[11] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, Jan. 2019.