A Fog-Based Security Framework for Large-Scale Industrial Internet of Things Environments

Hejia Zhou, Shantanu Pal, Zahra Jadidi, and Alireza Jolfaei

Abstract

The Industrial Internet of Things (IIoT) is a developing research area with potential global Internet connectivity, turning everyday objects into intelligent devices with more autonomous activities. IIoT services and applications are not only being used in smart homes and smart cities, but they have also become an essential element of the Industry 4.0 concept. The emergence of the IIoT helps traditional industries simplify production processes, reduce production costs, and improve industrial efficiency. However, the involvement of many heterogeneous devices, the use of third-party software, and the resource-constrained nature of the IoT devices bring new security risks to the production chain and expose vulnerabilities to the systems. The Distributed Denial of Service (DDoS) attacks are significant, among others. This article analyzes the threats and attacks in the IIoT and discusses how DDoS attacks impact the production process and communication dysfunctions with IIoT services and applications. This article also proposes a reference security framework that enhances the advantages of fog computing to demonstrate countermeasures against DDoS attacks and possible strategies to mitigate such attacks at scale.

Introduction

The Industrial Internet of Things (IIoT) triggered the fourth industrial revolution (known as Industry 4.0) based on Cyber Physical Systems (CPS), which defines various use cases from connected digital technology, mobile cloud computing and Internet of Things (IoT) to promote the efficiency, effectiveness, support for varied data, higher manufacture, mechanization, and wide-ranging knowledge [1]. IIoT has the potential to enhance traditional IoT communications in a new way (with a large-scale deployment), which allows all devices to share and use the same data in the same environment. Some characteristics of the IoT are [2]:

- The IoT cannot simply be seen as an extension of the Internet. IoT is built on a unique infrastructure and will be a new set of independent systems, although some of the underlying facilities will still be dependent on existing Internet technologies.
- The IoT could be accompanied by new business development to a single network to automate operational control and optimize the workflow.
- The IoT includes a variety of different communication modes, object-to-person communication and object-to-object communication, with particular emphasis on machine-to-machine communication (M2M).

Based on the characteristics mentioned above, the IoT can be seen as a distributed system connecting many information sensing devices and applications through the Internet and uniquely identifying entities within a broad network area.

The IIoT systems integrate the features of an IoT system. Therefore, it is essential to examine the basic building blocks of an IoT system. Several potential architectures discuss the layer view of an IoT system. These are composed of three to seven layers. However, in this article, we consider a basic IoT architecture consisting of four layers (as shown in Fig. 1). We argue that a four-layer architecture can efficiently distribute the various components of an IoT architecture. The bottom layer is called the *perception layer*, which is used for sensing the physical world. The perception layer includes smart sensing devices represented by sensors, actuators, location tracking devices, e.g., GPS (Global Positioning System) and smart terminals, etc. The perception layer is the basis for the IoT to obtain information and data, and its purpose is to achieve data sensing on a large scale. The next layer is the *network layer* used for data transmission. The network layer includes the access network and the core network. The network layer is the transmission layer for collected data. The collected data is stored on the *data storage layer* (also known as the cloud layer) located above the network layer. Finally, the top layer is the *application layer*, where the users use various data to achieve their business or manufacturing goals [3].

A similar layered architecture can be considered for an IIoT system for efficient data processing locally and improved response time. For instance, in an IIoT system, the perception layer collects data and transmits it to the data storage layer through the network layer for further processing. The data storage layer then analyzes and processes the data and sends it to the application layer to furnish users with a wealth of specific services, for example, smart transportation, smart home, smart health, and smart city.

Roadmap of the Article: Next, we discuss the concept of an IIoT architecture with more granularity with the inclusion of "fog computing." Towards this, we discuss a fog-based reference framework for IIoT systems that can efficiently address DDoS (Distributed Denial of Service) attacks at scale. We also provide a list of mitigation strategies for DDoS attacks in an IIoT system based on the discussed reference framework. We also discuss a security analysis of the proposed architecture.

The Concept of Fog-Based IIoT Architecture

The design of an IIoT framework incorporates the concept of a fog layer. The fog layer situates between the perception and cloud layers (i.e., the data storage layer) and is responsible for data transmission, encryption, and area management [4]. As an extension of the cloud layer, the fog layer helps the cloud layer to take on some of the data processing, distributed area management, distributed signature authentication, data re-encryption and critical management responsibilities. The fog layer interfaces upwards to the cloud layer, where it is managed and receives data sets from the cloud layer, and downwards to the perception layer, where it regionalizes and addresses the various sensors that access the IIoT, receives data requests

Hejia Zhou is with Queensland University of Technology, Australia.
Shantanu Pal is with Deakin University, Australia.
Zahra Jadidi is with Griffith University, Australia.
Alireza Jolfaei is with Flinders University, Australia.

Digital Object Identifier: 10.1109/IOTM.002.2200195

2576-3180/23/$25.00 © 2023 IEEE

from devices, authorizes the requests and establishes the data transmission links. Significantly, the use of the fog layer can perform some of the basic functions of the network layer, e.g., data transmission from the perception layer to the cloud layer.

As Fig. 2 shows, a general IIoT architecture can consist of the basic elements of an IoT architecture but with a fog layer, which we discussed above. The IoT and the IIoT are very similar in that they are related to a network of intelligent devices, machines, and sensors. The most common difference between the IoT and IIoT is that IoT is derived from conceptual terms, e.g., creation, concatenation of acts, manipulation of posters and other instances of constructive expression. Since the IIoT is extremely forgiving of others and is very powerful, it has a high degree of language, which means that the data and ideas generated in the reproductive community are likely to be more sophisticated and sensitive [5].

Although we find that the layering of the IIoT architecture can be three layers, four layers or even seven layers, it is more challenging to implement and requires consideration of its security, privacy, and trust issues between these layers. Moreover, because of the instability of network protocols and less human intervention, it becomes increasingly vulnerable to various security threats in an IIoT system. The additional specialist reason is that technicians have found that the cloud-only network layer is becoming challenging to support the large number of devices accessing and transmitting data. Hence the introduction of the concept of a fog layer is pivotal. Next, we analyze the advantages of including fog layers in an IIoT architecture and demonstrate whether using them can lead to more secure and efficient information processing, enhancing storage capabilities, security, privacy, and trust.

Security Challenges

IoT and IIoT have some common characteristics, and according to those common factors, it is hard to distinguish different attacks individually for each system, especially the DDoS attacks [6]. Therefore, an attack that impacts an IoT system can easily affect an IIoT system. Some concerns regarding emerging security issues in IIoT systems are [7]:

Threats Built into the IIoT: IIoT threats, including the threat of attacks on databases, are intertwined with other trends in 2021. In a world of increasing automation, many attacks are focused on supply chains and manufacturing. There are many applications of IIoT in these areas, and updating devices is not always a priority. As we experience more new types of attacks against the IIoT (for example, Mirai botnets and WannaCry), one fundamental question is whether we can update aging firmware to give it the defence it needs.

Threat of Artificial Intelligence (AI) in the IIoT: In recent years, it is likely to be the challenges of AI-driven threats to the IIoT. AI-based attacks have been occurring since 2007, mainly against social engineering attacks (simulating human chatter) and augmented DDoS attacks. AI systems are better than humans at performing many elements of IoT threats, e.g., repetitive tasks, interactive responses, and processing extensive data sets. In general, AI helps attackers amplify the IoT threat. In 2021, we not only envision new AI-based IoT threats but also realize the magnitude of such attacks. We should look for the usual cyber breaches and other attacks, but they are deployed faster, on a larger scale, and more flexible, automated, and customized than in the past.

Data Protection Challenges: In an IIoT-connected world, data protection becomes significant because it can be transferred between multiple devices in seconds. It can store on a mobile device, and in the next second, it may be stored on the web and then in the cloud. All this data is transferred over the Internet, leading to data leakage due to this high mobility of data. Once the data is compromised, attackers can make unauthorized use of this sensitive data to other organizations that violate the privacy and security rights of the data (and, in the long turn, the reputation of the organizations). In addition, even if the attackers do not compromise data, service providers may not comply with laws and regulations, leading to data privacy breaches.

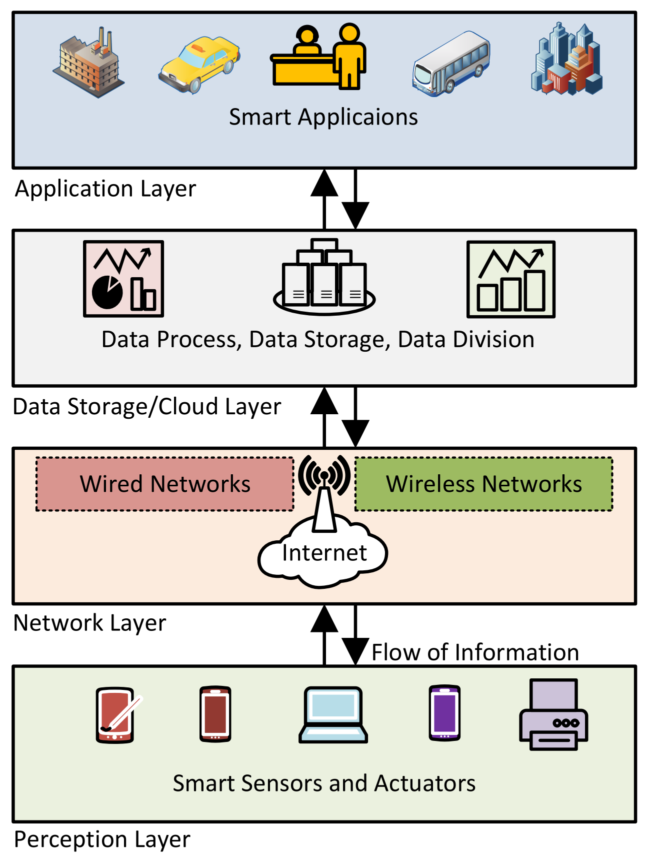

FIGURE 1. A simple IoT architecture consists of four layers.

Impact of DDoS Attacks on IIoT

In terms of the motivations used to deploy DDoS attacks, they can be seen into the following areas [8]:

- *Abuse of a Reasonable Request for Service:* The attacker excessively requests the normal services of the system, taking up too many service resources and causing the system to be overloaded. These service resources include network bandwidth, file system space capacity, and a number of open processes or connections.
- *Creating High Volumes of Unwanted Data:* Maliciously creating and sending large amounts of random and useless data packets to occupy network bandwidth with this high volume of useless data, causing network congestion.
- *Exploiting Flaws in the Transport Interest Protocol:* Constructing and sending malformed packets that cause errors or crashes that cannot be processed by the target primary server.
- *Exploit a Vulnerability in the Service Program:* This behavior targets a specific vulnerability in the service program on the host and sends some targeted data in a special format that causes the service to process it incorrectly and deny service.

Compared with other security attacks, DDoS attacks are more concealed and harmful due to the resource-constrained nature of the IIoT (and IoT) devices. Once a DDoS attack affects any device in the IIoT production line, it may cause the communication failure of the device and fail to connect to other devices in the IIoT system. The setting of interconnected IIoT leads to the immobility or loss of connection of the automated production line and leads to a system failure at scale.

It is noted that DDoS attacks against the IIoT can cause unimaginable consequences. The following two cases illustrate the impact of DDoS attacks in large-scale IIoT systems [9]:

- In February 2018, the target of a DDoS attack was GitHub, a popular online code managing service used by millions of developers. At this peak, the attack transmitted traffic at a

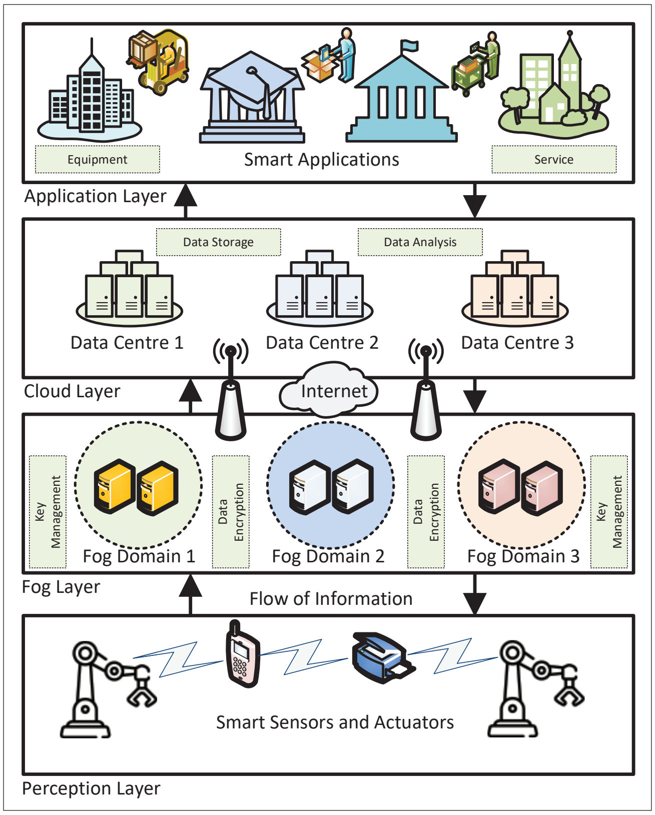

FIGURE 2. A simple overview of a fog-based IIoT architecture.

rate of 1.3 Terabytes per second (TBps) and sent data packets at a rate of 126.9 million per second. The attacker benefits from the amplification consequence of a widespread database storing system called Memcached. By overflowing the Memcached server with misleading requests, the attacker was able to scale his attack by about 50,000 times.

- Another noted cyber-attacks on manufacturing systems was the December 2015 attack on the Ukrainian power grid. The attack combined multiple hacking techniques, including DDoS attacks, malicious emails, Internet virus worms, and malware. The attackers managed to damage the whole power distribution company and caused more than 200,000 people in Ukraine to lose power for a certain period.

A Reference Security Framework

In this section, we discuss an overview of the proposed security framework against DDoS attacks for IIoT systems. In contrast to the IIoT framework mentioned earlier, the concept of the "regional aggregator" has been added to the framework. A regional aggregator can seamlessly execute distributed services on a single device. The structure of the proposed IIoT framework is composed of four layers, as the architecture discussed earlier. Recall, in this article, we try to take advantage of the underlying fog layers to mitigate DDoS attacks for the IIoT systems [10]. In Fig. 3 we illustrate a layered framework, which is composed of the following layers:

- ***Perception Layer:*** The perception layer is the bottom layer of the framework. It contains smart sensor devices, which perform data transmission and security authentication to the corresponding data collection.
- ***Fog Layer:*** The second layer is the fog layer. In contrast to other IIoT fog layers, our framework introduces the concept of adding regional aggregate processors. The framework assumes a structure where each firewall is responsible for managing only a fixed number of devices in a fixed area. Each firewall uses RSA encryption for authentication between the firewalls. It ensures the accuracy of data transmission and allows for quick identification of the area under attack in the event of a cyber-attack, thus narrowing the scope and improving remediation efficiency.
- ***Cloud Layer:*** Cloud layer is the third layer in the IIoT system. This layer is responsible for processing information and data storage in the cloud server and then distributing the data to the related devices and applications. The cloud layer is generally the same as secure storage, which could set the link between the application and fog layers.
- ***Application Layer:*** It is the top layer of the architecture. This layer contains users and smart applications to access the desired services. The functionality of this layer is to deliver applications, e.g., smart cities, smart transportation, and smart agriculture, just a name a few applications. In addition, this layer links the smart devices or smart user's surface that offer smart services to the IIoT system's users.

In the data-driven manufacturing environment, e.g., the IIoT, how to design a secure and distributed automation architecture has become a challenging task for technicians and designers. We argue that the balance control between fog computing and cloud computing will enable the IIoT to give more flexible and granular modularity to its applications and services at their highest potential. With this, many manufacturing organizations will benefit from automated systems that deploy sensors to measure, monitor, and analyze data through the IIoT to improve efficiency and increase revenue from operations. The volumes of data (e.g., big data) generated by these newly connected factories can be measured in petabytes - millions of streams of data from sensors connected to ICS (Industrial Control Systems) for both Operational Technology (OT) and Information Technology (IT) sides, SCADA (Supervisory Control and Data Acquisition) systems, and autonomous unattended machines, industrial robots effectively [11].

Larger autonomous systems are now more likely to adopt new architectural approaches and solutions that enable IIoT to realize its extreme potential through the fog layer (sometimes referred to as edge computing). Fog computing is designed for data-intensive computational tasks that can be performed inside the local devices without the need for requiring high-performance capability. Fog can be seen as a developing distributed architecture that connects the cloud to edge devices in the production line, eliminating the need for a fixed Internet connection in the field. By selectively shifting computation, storage, communication and control, fog computing allows decisions to be made close to the edge sensors and actuators where the data is generated and used locally. That is close to the edge nodes where the actual data resides. The involvement of fog is a valuable complement to cloud computing, rather than a complete replacement so that IIoT can be used its advantages more efficiently, economically, safely and constructively in large-scale manufacturing environments.

As stated above, the fog and edge layers can be seen interchangeably, but there are key differences between them. The fog layer can be seen as a superset of the edge functions of the cloud layer. The architecture of the fog layer is designed primarily to combine resources and data sources with layers that reside at the cloud-to-edge, function-to-function or point-to-point levels to gain maximum efficiency at the edge level. In other words, edge computing is often limited to a small number of cloud-to-edge layers, often associated with simple protocol gateway functions. Concerning the IIoT systems, fog can provide better utilization of resources that can be processed locally and easily mitigate DDoS attacks at the edge level. This will, in turn, enable the IIoT system to detect and take appropriate measures to prevent such an attack at the edge level [12].

The gateway nodes (e.g., a physical device or virtual platform) of the fog layer are the basic elements of the fog architecture. A fog node can be any device that provides the compute, network, storage, and acceleration elements of a fog architecture. Examples include industrial controllers, switches, routers, embedded servers, complex gateways, programmable logic controllers (PLCs), and smart IoT nodes (e.g., video surveillance cameras) used in IIoT automated production lines. The fog nodes result in the more reliable and faster data processing. Factories that can make use of the data flow from these fog node layers can not only make the devices more efficient but also interconnect data between factories. Fog nodes at lower levels of the overall IIoT architecture, e.g., individual computers, can be connected directly to local sensors and actuators to enable real-time data analysis and interpretation of anomalies. It can also respond and compensate for problems or solve them autonomously if authorized . In addition, a fog node can send appropriate service requests to providers with better technical resources, machine learning capabilities or maintenance services to obtain higher fog tiers.

When the environment in which they are located requires real-time decisions about data processing, e.g., raising an alert in case of equipment failure or adjusting parameter values at critical points in industrial production, fog nodes can provide millisecond delays for the process of data analysis and manipulation. This feature makes it unnecessary for plants to route such real-time decisions through cloud computing data centers. Helping to avoid potentially high latency events, queue delays, or network/server downtime could lead to engineering incidents, reduced productivity, or lower product quality. In addition, higher-level fog nodes in the factory allow for a broader view of industrial processes. Therefore, they can add extra functions, e.g., visualization of production line operations, monitoring the status of faulty machines, adjusting production strictures, modifying production schedules, ordering supplies, and sending alerts to the right people [13]. Adding a fog layer and placing local fog nodes in the hierarchy near the IIoT pipeline, allowing them to be connected to sensors and actuators with cheap and fast local network facilities. Fog nodes improve safety and reduce the chance of leaks. If authorized, they can respond to abnormal conditions in milliseconds and quickly close the valve, significantly reducing the severity of spills. Fog nodes can operate between wired, fiber optic, and wireless networks and within those networks, making them best suited for connecting to industrial components based on the SCADA systems. Fog node analysis on local sites reduces the need for cloud bandwidth and overall costs. A balance of control between cloud and fog computing yields better results across the entire business process (cost, control, and security). Moving most decision-making functions to fog nodes and occasionally using the cloud to report status or receive commands or updates can help organizations create a superior control system.

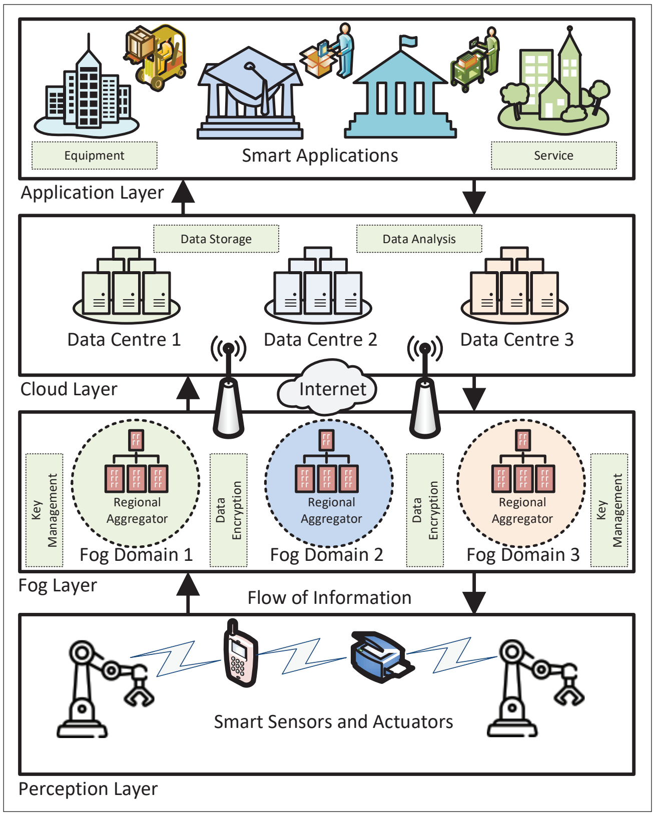

FIGURE 3. The proposed reference fog-based IIoT security framework.

Discussion

The significant finding of this article is how the overall security of the IIoT environment can be effectively enhanced by building a fog layer framework and strengthening the fog layer functionality to the core mitigation of DDoS attacks in an IIoT system [14, 15].

Mitigation Considerations

- ***Latency:*** Due to the dynamic nature of IIoT systems, more and more ICS require end-to-end data transfer delays in production lines to be kept to sub-milliseconds. However, this requirement is hard to be met by the leading providers of cloud services at present. In some cases, factories, the latency of up to 10 micro-seconds may be required to prevent production line shutdowns, avoid accidents, restore electrical service, or correct manufacturing errors. The creation of a fog node reduces latency because it eliminates the back-and-forth time delay from the sensor on the production line to the cloud and from the cloud back to the sensor. This latency includes transmission delays to the cloud (wireless or fiber optic devices), delays in waiting for data queues and delays in processing data by cloud servers, which can exceed 100 milli-seconds round trip even in a well-designed cloud network. We argue that using our framework, the local fog nodes can be able to react to conditions and make decisions within milli-seconds.
- ***Security:*** Traditional industrial security measures focus on providing peripheral-based threat detection, and defenses are not enough for IIoT systems. With fog computing, local security functionalities can be used in a more controlled and processed way for an organization. In general, fog nodes include a trusted hardware root, the foundation of a chain of trust that runs from the lowest sensors and actuators up the fog hierarchy to the cloud. Communications from the Internet to the distributed fog networks are monitored, and machine learning can be used to detect irregular activity in the local environment, allowing potential attacks to be detected and controlled in a timely manner. In future, blockchain technology can be an alternative to provide more secure storage that can easily be integrated with the proposed architecture.
- ***Cognition:*** The fog layer structure can control the optimal location of the cloud to the edge computing, storage, and control functions on individual edge devices. The fog layer can also be employed to make data processing decisions via nearby fog nodes on many edge devices to avoid excessive data consumption and reduce transmission processing efficiency by transferring data to the cloud locally. The use of a fog layer allows data to be processed and analyzed easily and efficiently, autonomously in the local fog layer. The processed information is then sent through the fog layer to a data center in the cloud for analysis. The addition of the fog layer enables the data processing performance of the IIoT system to support long-term planning and continuous system improvement in the future by monitoring local computation and processing at the edge devices.
- ***Flexibility:*** A common industrial production environment may result in excessive fluctuations in data output. By sequencing all fog nodes, the fog hierarchy can be empowered to manage some of the unpredictable requirements, e.g., zero-day attacks of the system and allocate bearers beyond compliance to other under-utilized machines providing flexibility to the attack mitigation. The hierarchy of fog nodes can form a dynamic group to exchange information and enable an efficient federation of the learning environment. For example, suppose an industrial plant discovers in advance that it is running short of capacity for its tasks. It can then transfer part of its production tasks to another organization's assets

and equipment for operation. That said, it can be easily performed with more flexibility than traditional approaches. The ability to change tasks dynamically also helps to coordinate and control information across the devices.

- **Real-World Implementation:** It is a key factor in the operational efficiency in real-world of the entire IIoT system. With the advent of Industry 4.0 and the evolution of Information and Communications Technology (ICT), from purpose-built and stand-alone systems to software-defined and modular interconnected operations, technicians are becoming aware that the cloud layer is gradually less productive to meet the need for efficiency. It is due to the complexity of connected edge systems and sensors and the integration of the various communication protocols and communication technologies. Fog nodes can, therefore, be added as an extension to traditional solutions or turned into an efficient protocol gateway by leveraging the computational efficiency of the edge devices in real-time. Recall that fog nodes collect and process data in different forms and use various protocols through the interconnection between the devices and the entire production pipeline so that devices and systems can be efficiently and uniformly connected without the need for different access methods for each component.

Security Analysis and Lessons Learned

The ability to analyze and process data at scale in real-time is considered to be one of the benefits of IIoT systems. In practice, the area of research on how to unify the data collected from various sources has been a potential challenge for individual developers, organizations, and users. This is because the devices may use different operating systems and complex communication protocols when sharing data. This is even more significant when considering the cross-domain data sharing between the nodes spread access to multiple jurisdictions. In addition, end-users are concerned about data security, and there are potential risks that industrial plants about sharing the sensitive information collected by the equipment with third parties outside the plant. We argue that fog architecture is beneficial where the locally computational performance can lead towards a direction where the various organizations can process such risks and their potential mitigation locally, particularly in avoiding DDoS attacks.

It is noted that the advent of fog architecture provides an interconnected layer to the overall IIoT systems. From the security aspect, it is to ensure the IIoT systems can communicate and operate safely and efficiently between the equipment and the cloud layer, as well as data processing and usage. Further, a fog architecture can help identify component failures before data aggregation, ensuring the data analysis security, reliability, confidentiality, integrity, and availability. Since the fog layer is closer to the perception layer, which involves a large scale of smart sensors, fog nodes can identify and process data faster. This helps increase the efficiency of device authorization and data responsibility speed and problem-solving speed with high efficiency.

In addition, in the fog layer, when analyzing data received, the fog nodes could detect whether the system should enter the maintenance period or not. The fog layer could generate signs that a fault has occurred in the system, immediately alert the operator, carry out equipment inspections, and adjust the production line schedule, thus minimizing the impact of the hazard on the manufacturing chain. Moreover, there may also be unconventional situations where uncertainty may cause due to the errors in sensor readings signal an imminent failure, the probability of which might be minimal and allows the system to fix it before the dreaded failure occurs.

To maintain security, privacy, and trust in the IIoT system, integrity and availability of data usage are essential. Therefore, the fog layer needs to determine the content of the data and the importance of encryption in a hierarchical manner, sending only the appropriate data to the required processor terminals with the appropriate applicability. The current mainstream approach uses data classification, encryption, and virtual private networks (VPNs) to provide more secure communications. Those methods significantly reduce the risk of inadvertent cross-leakage of exclusive information in some directions.

Conclusion and Future Work

Compared to traditional IoT, IIoT involves a more extensive system of connected devices and nodes, resulting in more data processing tasks, ensuring that this data can be processed and transmitted safely and efficiently. Since the IIoT system involves large-scale devices and data process demands, the cloud computing system currently used in the IoT can no longer meet the data processing needs of large IIoT. Fog layer computing is proposed to extend cloud computing to edge IIoT devices. This article presents a conceptual framework integrating the fog layer to mitigate DDoS attacks in IIoT systems. However, there are still several open questions and challenges related to authentication and trust issues, Energy consumption, location awareness, etc., which need to be addressed for a more secure and safe fog-based IIoT architecture.

References

[1] R. Huo *et al.*, "A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges," *IEEE Commun. Surveys & Tutorials*, 2022.

[2] S. Pal and Z. Jadidi, "Analysis of Security Issues and Countermeasures for the Industrial Internet of Things," *Applied Sciences*, vol. 11, no. 20, 2021, p. 9393.

[3] J. Lin *et al.*, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things J.*, vol. 4, no. 5, 2017, pp. 1125–42.

[4] P. Hu *et al.*, "Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues," *J. Network and Computer Applications*, vol. 98, 2017, pp. 27–42.

[5] G. S. Chalapathi *et al.*, "Industrial Internet of Things (IIoT) Applications of edge and Fog Computing: A Review and Future Directions," *Fog/Edge Computing for Security, Privacy, and Applications*, 2021, pp. 293–325.

[6] M. M. Salim, S. Rathore, and J. H. Park, "Distributed Denial of Service Attacks and Its Defenses in IoT: A Survey," *J. Supercomputing*, vol. 76, no. 7, 2020, pp. 5320–63.

[7] S. Pal, M. Hitchens, and V. Varadharajan, "On the Design of Security Mechanisms for the Internet of Things," *2017 11th Int'l. Conf. Sensing Technology (ICST)*, 2017, pp. 1–6.

[8] A. Bhardwaj *et al.*, "Distributed Denial of Service Attacks in Cloud: State-of-the-art of Scientific and Commercial Solutions," *Computer Science Review*, vol. 39, 2021, p. 100332.

[9] N. V. Patil, C. Rama Krishna, and K. Kumar, "Distributed Frameworks for Detecting Distributed Denial of Service Attacks: A Comprehensive Review, Challenges and Future Directions," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 10, 2021, p. e6197.

[10] P. Kumar, G. P. Gupta, and R. Tripathi, "Design of Anomaly-Based Intrusion Detection System Using Fog Computing for IoT Network," *Automatic Control and Computer Sciences*, vol. 55, no. 2, 2021, pp. 137–47.

[11] G. Falco, C. Caldera, and H. Shrobe, "IIoT Cybersecurity Risk Modeling for Scada Systems," *IEEE Internet of Things J.*, vol. 5, no. 6, 2018, pp. 4486–95.

[12] P. Kumar, G. P. Gupta, and R. Tripathi, "Tp2sf: A Trustworthy Privacy-Preserving Secured Framework for Sustainable Smart Cities by Leveraging Blockchain and Machine Learning," *J. Systems Architecture*, vol. 115, p. 101954, 2021.

[13] T. A. N. Abdali *et al.*, "Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues," *IEEE Access*, vol. 9, 2021, pp. 75,961–80.

[14] P. Kumar, G. P. Gupta, and R. Tripathi, "Toward Design of an Intelligent Cyber Attack Detection System using Hybrid Feature Reduced Approach for IoT Networks," *Arabian J. Science and Engineering*, vol. 46, no. 4, 2021, pp. 3749–78.

[15] Y. I. Alzoubi *et al.*, "Fog Computing Security and Privacy for the Internet of Thing Applications: State-of-the-Art," *Security and Privacy*, vol. 4, no. 2, 2021, p. e145.

Biographies

Hejia Zhou (hejia.zhou@connect.qut.edu.au) is associated with the School of Computer Science, Queensland University of Technology, Brisbane, Australia. Hejia has extensive research interests in machine learning, artificial intelligence, blockchain, the Internet of Things, Industry 5.0, and cyber physical systems.

Shantanu Pal [SM] (shantanu.pal@deakin.edu.au) is associated with the School of Information Technology, Deakin University, Melbourne, Australia. Shantanu has extensive research experience and knowledge in Internet of Things, big data and distributed applications, access control, trust management, blockchain technology, mobile and cloud computing, distributed networks, and policy enforcement.

Zahra Jadidi (z.jadidi@griffith.edu.au) is associated with the School of Information and Communication Technology, Griffith University, Gold Coast, Australia. She has extensive research interest in cybersecurity, security of cyber physical systems, machine learning applications in security analysis, and security of machine learning algorithms. She is a Fellow of the Higher Education Academy (FHEA), Australia.

Alireza Jolfaei [SM] (alireza.jolfaei@flinders.edu.au) is associated with the College of Science and Engineering, Flinders University, Australia. He has extensive research interest in cyber physical systems security, and analysis and design of safety-critical cyber-physical systems in the presence of cyber adversaries. He is a distinguished speaker of the ACM on cybersecurity.