J Inf Process Syst, Vol.16, No.4, pp.975~990, August 2020
https://doi.org/10.3745/JIPS.03.0144

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Comprehensive Analyses of Intrusion Detection System for IoT Environment

Jose Costa Sapalo Sicato*, Sushil Kumar Singh*, Shailendra Rathore*, and Jong Hyuk Park*

Abstract

Nowadays, the Internet of Things (IoT) network, is increasingly becoming a ubiquitous connectivity between different advanced applications such as smart cities, smart homes, smart grids, and many others. The emerging network of smart devices and objects enables people to make smart decisions through machine to machine (M2M) communication. Most real-world security and IoT-related challenges are vulnerable to various attacks that pose numerous security and privacy challenges. Therefore, IoT offers efficient and effective solutions. intrusion detection system (IDS) is a solution to address security and privacy challenges with detecting different IoT attacks. To develop an attack detection and a stable network, this paper's main objective is to provide a comprehensive overview of existing intrusion detections system for IoT environment, cyber-security threats challenges, and transparent problems and concerns are analyzed and discussed. In this paper, we propose software-defined IDS based distributed cloud architecture, that provides a secure IoT environment. Experimental evaluation of proposed architecture shows that it has better detection and accuracy than traditional methods.

Keywords

IDS, IoT, M2M, Security, Privacy

1. Introduction

The information technology age, Internet of Things (IoT) is known as the most exciting technologies. The internet allows connected devices to grow exponentially every day, and it has been announced that over 50 million devices will be connected via the internet by 2020 [1]. The IoT technology's purpose is to interconnect all objects in such a way as to make all computers, programmable, intelligent, and make it more secure to communicate with humans. Sensors and networks allow everything to communicate with each other directly for exchanging critical information. It is possible by machine to machine (M2M) communication in the future. Numerous practical of IoT applications can be used almost in many fields such as smart city applications (smart home, and smart grid, healthcare, and others), where those applications improve the quality of life [2]. The concept of the intrusion detection system (IDS) intends to detect a threat or intrusion into the network, and it actively tracks the network by detecting potential events and logging information about them by stopping incidents. Intrusion detection and prevention system (IDPS) which is a combination of two systems used to monitor events occurring in a network and

Manuscript received May 5, 2020; first revision June 26, 2020; accepted July 1, 2020.

Corresponding Author: Jong Hyuk Park (jhpark1@seoultech.ac.kr)

* Dept. of Computer Science and Engineering, Seoul National University of Science & Technology (SeoulTech), Seoul, Korea (josecostasicato@gmail.com, sushil.sngh001007@seoultech.ac.kr, rathoreshailendra2@gmail.com, jhpark1@seoultech.ac.kr)

evaluate them for possible violations or incidents in security policies and also the process of performing intrusion detection and stop to detect incidents.

Using the IoT system in many applications domains such as healthcare, smart home, smart industry, environmental monitoring, and others provides significant benefits to the IoT system. IoT security issues are a significant concern, which is confidentiality, integrity, availability, and authorization [3,4]. The integration of real-world objects with IoT, however, brings a range of cybersecurity threats in daily activities. Those possible attacks occur against critical infrastructure in IoT, such as denial of service (DoS), man-in-the-middle (MITM), and others [5]. They can compromise any device, the main server, if it's compromised by the attacker, the whole system to shut down. To solve these problems, IDS recognized as one of the key tools plays a crucial role in the IoT security framework used for information systems and conventional networks. It detects many known and unknown attacks not only to detect known attacks.

In this study, we provide brief overview research related to IDS for IoT security issues. Our research objective demonstrates state of the art from a different perspective, which includes the architecture of the layered IoT environment and security mechanism. We also focus on future recommendations and guidance related to cybersecurity issues in the IoT environment. Considering the development of IDS for the IoT environment presents significant challenges for security. Therefore, the study of our survey offers some key contributions as follows:

- First, we sketch relevant aspects of security issues, vulnerabilities, and attack surfaces on the IoT environment.
- Second a comprehensive discussion on open issues in IDS for IoT environment.
- Finally, evaluate the proposed architecture and shows that it is better than traditional methods.

The remainder of our research structured as follows: The literature review and related work are summarized in Section 2. Section 3 provides an overview of the IoT security environment; Section 4 describes problems and challenges relating to IoT security. Experimental results and analysis are shown in Section 5. Finally, Section 6 concludes our work.

2. Related Work

While IoT has been gaining popularity, security and privacy challenges pose significant barriers for deployment of these dives and widespread adoption. Intrusion detection has been a considerable field of work for more than three decades. Knowledge in network intrusion detection, along with security needs, has increased among researchers. Many researchers have studied and discussed the open-ended research issues of the IDS for the IoT environment, as it's shown in Fig. 1.

2.1 Detection Methods for Intrusion Detection System

In the IoT environment, the deployment of IDS can't succeed specified security issues. The IDS attempt to track either the device or the network events of potentially malicious attacks across the network [6,7]. Most of the research work based on intrusion detection and prevention system focused on cloud computing [8,9]. IDS's purpose is to detect unauthorized access from attackers. These systems are considered to include: wireless local area network (WLAN), clouds, wide area network (WANs), and

others [10]. Based on Jun and Chi [11] mentioned that effective IDS need to be simple and accurately detected for different security threats in the IoT environment. According to the deployment of IoT based IDS showed in Fig. 1, it can be categorized into anomaly-based IDS, host-based IDS, a network-based IDS, and distributed IDS.

- Anomaly based IDS (AIDS): In the case of AIDS, known as dynamic behavior-based detection, it creates significant false alarms and generates alerts, where unknown threats can be detected at various levels and vulnerabilities can be identified [12,13], and evaluated the appropriate actions to take. On the other hand, IDS continue to show a relatively high rate of false-positive [14]. Anomaly includes gathering data on authorized users' actions over a period to track device operation and to identify either normal or defect. These classifications are based on rules, rather than signatures, attempting to detect any attack in regular operation.
- Host-based IDS (HIDS): The HIDS is software installed host computer of the network capacity to monitor, analyze, and collect traffic activities on the network interfaces that are originated from the host of system application. IDS have limited views, and it can only detect malicious behaviors for a single host.
- Network-based IDS (NIDS): The NIDS makes anomaly detection and signature detection. For example, in Signature detection, list the types of attacks suitable for it, such as application layer reconnaissance, policy validation, transport layer reconnaissance, and network layer reconnaissance. The network-based intrusion detection system operates by monitoring the traffic as the network flows over the network infrastructure. Both NIDS and HDIS have capabilities for detecting and monitoring malicious activities [15].
- Distributed IDS (DIDS): It consists of multiple IDS on an extensive network, where all of which communicates and facilitates advanced network monitoring, instant attack data, and incident analysis. It incorporates information from the number of sensors, including both network and hose-based IDS. The central analyzer is best equipped to detect and respond to intrusion activities.

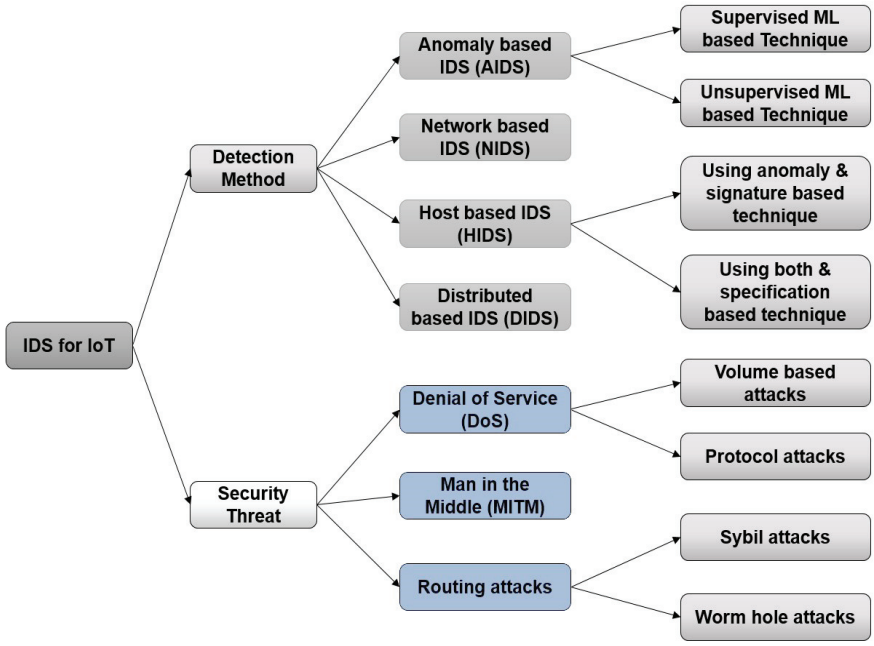


Fig. 1. Intrusion Detection System IDS for IoT.

2.2 Security Threats

The IoT security threats are vulnerable to various attacks, based on other research mentions different types of attacks that have been discussed in the IDS for IoT proposals. As a result, enabling IoT solutions will include various systems, facilities, and standards, each with its security and privacy criteria. Based on three aspects of exchanging data between users and objects: (1) limited power for the IoT environment, (2) a large number of interconnected devices have noted that conventional protection, and (3) privacy cannot be applied directly to such IoT technologies, some indication of how IoT devices are susceptible to attack has been identified [16,17].

According to Kollias et al. [18] mentioned the IoT technologies had been developed that could leave vulnerabilities attacks related to security and privacy issues in the IoT network. Some other research studies based on security threats that can affect entities in IoT is organized as the following categories shown in Fig. 1: routing attacks, MITM, DoS, eavesdropping attacks [19].

2.3 Existing Research Studies

In recent years many authors have been surveyed relevant to IoT and tend to focus on particular aspects of IDS. A survey-based on machine learning techniques which focusing on IDS for the wireless sensor network (WSN) and IoT [20]. Kasinathan et al. [21] proposed a network-based DoS detection for intrusion detection system architecture, where using the IDS probe approach to monitor 6LoWPAN traffic. Based on Buczak and Guven [22] survey mentions IDS on the general system regularly used for specific WSN and IoT, and highlights a certain number of issues with techniques in particular for the complexity of those which require acquisition. Abudaliyev et al. [23] mention a survey related on the characteristics of IDS in WSN, where the shortcomings for validation includes a low amount of data available, lack of universal attack detection and poor energy consumption. Another similar survey that focuses on IDS for WSN introduced [24]. In Table 1, we just mentioned a comparative overview survey on IDS for IoT security.

Table 1. Overview of IDS for IoT environment

	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	Our work
Architecture										
Centralized	×	×	×	×	✓	✓	×	×	✓	✓
Distributed	✓	✓	×	×	×	×	×	×	✓	✓
Hybrid	×	×	×	×	×	×	✓	✓	✓	×
Hierarchical	×	×	✓	✓	×	×	×	×	×	×
Detection technique										
Anomaly	✓	×	×	✓	✓	✓	✓	×	×	✓
Hybrid	×	✓		×	×	×	×	×	×	×
Signature	×	×	×	×	×	×	×	×	×	×
Specification	×	×	×	×	×	×	×	✓	×	×
Machine learning	×	×	×	×	✓	✓	×	✓	✓	✓
Types										
Network-based IDS	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Host-based IDS	×	×	×	×	✓	✓	×	×	×	✓
Technology focus										
Routing protocol for wireless	×	×	×	×	×	×	✓	✓	✓	✓
Wireless sensor network	✓	✓	✓	✓	×	×	×	×	✓	✓
Mobile devices	×	×	×	×	✓	✓	×	×	✓	✓

3. IoT Security

In this section, is reviewed an overview of current security issues within the IoT environment. IoT is known as the new generation of the internet; it consists of a large number of ad-hoc connected devices, and features highly limit these devices. The IoT architecture focuses on the core of three layers, as shown in Fig. 2.

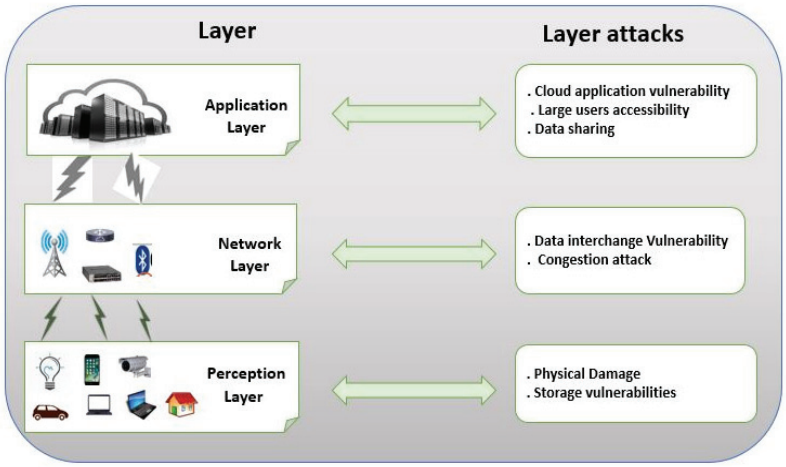


Fig. 2. IoT Architecture and attacks.

3.1 IoT Layer Architecture

- Perception layer, starting from this layer is the lowest level and input data gate for IoT, where communications occur between nodes and devices, it's critical to have security measures defending against any breach. The perception layer components are M2M, radio-frequency identification (RFID), and sensor network [34]. First, the M2M considered as one of the important elements of the IoT, which enables interconnection and interoperability between machines over the network [35]. Second, RFID allows the object to wirelessly communicate different types of communication over the IoT environment, leading to the ability to monitor data. The last sensor network, is considered important information in the perception layer and is another feature that feeds the signal database.
- The network layer forms one of the largest and is responsible for enabling IoT devices to communicate with other devices as well with the application services [36]. The network layer consists of a network interface, Wi-Fi, Ethernet, cellular, Zigbee, intelligent management, RIFD, and other devices. Network features are used for processing and transmit sensor data [37]. These sensors are small, with limit computing power and limited processing.
- Application layer includes an IoT infrastructure consisting of a network such as a cloud system for data storage and actuators. It is responsible for making sense of the data obtained and transmitted to another IoT layer. The IoT application layer method, filters and typically consists of those associated, often located by passing a message through all areas of the network from the perception layer [38]. Application is expected to present high-security requirements, but it presents common security issues such as related to data integrity, reliability, and privacy protection. Therefore, the security of IoT needs to be addressed.

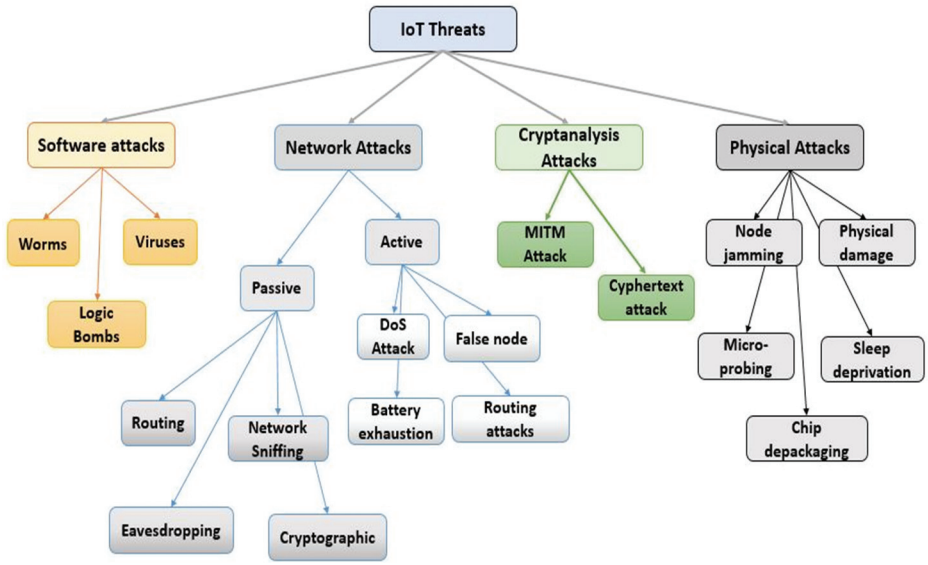


Fig. 3. Detailed taxonomy of threats in IoT.

3.2 IoT Cyber-Attacks

In cybersecurity, confidentiality, integrity, and availability are well known. Different types of attacks are exposed in the IoT network either from internal or external, Fig. 3 describes detailed taxonomy of threats in IoT, where these kinds of attacks are mainly classified as two types as outside and inside attacks. The outside attack is considered when the attacker is not part of the network, while in an inside attack, malicious nodes are part of the network, therefore we discuss some cyber-attacks in the IoT environment.

- Software attacks: It is the primary source of security vulnerability and it consists of various kinds of attacks in IoT, these attacks can replicate without human action and it exploits the system by using logic bombs, viruses, worms and other examples of software attacks that deliberately inject system code through its communication interface which can steal information and even damage devices on IoT system [39-41].
- Network attacks: It centered on the IoT environment, consists of two different types of attacks, passive and active, that might affect the IoT system environment. Passive attacks which are under intruders monitor a system is performed by several attacks allowing the attacker to collect information from the sensor, besides, by eavesdrop, an attacker could spy on a communication channel causing privacy violation (e.g., side chain, cryptographic, eavesdropping, routing) [42,43]. The active attack involves the use of information collected during the passive attack to compromise the network, and the attacker modifies the IoT system to change the configurations. Try to break the protection feature of data connected to the district or mess the network communication system. Attacks may include a sequence of medication, disruption, and many types of attacks (e.g., routing attack, DoS, false node, and battery exhaustion).
- Cryptanalysis attacks: This type of attack is a type of decryption and analysis of codes encrypted and cyphertext where they use some mathematics formulas for search vulnerabilities and beak into cryptography algorithms, and their purpose is to find encryption key used to breaking encryption. These types of attacks are known as well as implementation attacks, and it includes (MITM attack, chosen ciphertext attack) [44].

- Physical Attacks: Physical attacks know as a critical type of cryptanalysis used to discover hidden aspects of devices, and to identify IoT vulnerabilities focused on the hardware component, the attacker will try to get physical access before an attack is done by creating a false attack test. It exposes vulnerabilities such as (e.g., micro probing, node jamming, physical damage chip Re-packaging, and sleep deprivation), causing damage to the sensor node. The adversaries change the behavior of devices that involves the IoT environment system [45].

4. Proposed Distributed Cloud Architecture

In this section, we describe the design overview of proposed distributed cloud architecture, and experiment results and analysis.

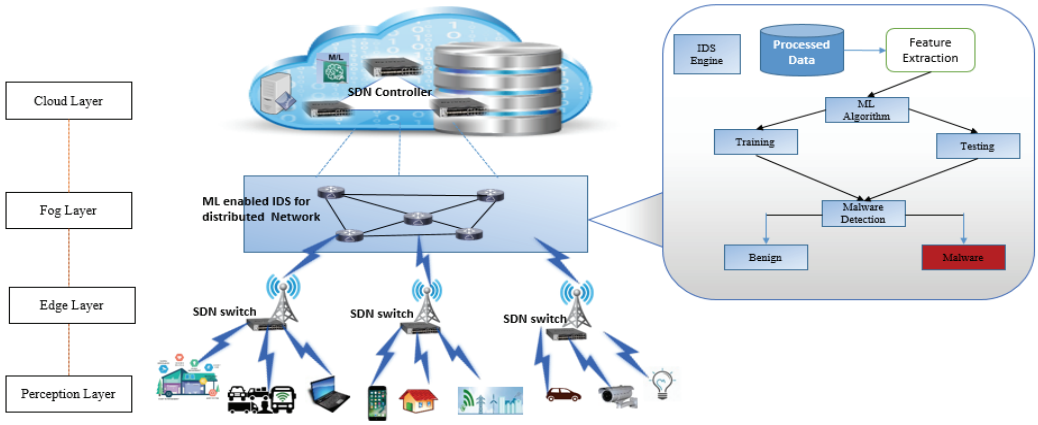


Fig. 4. Software-defined IDS based distributed cloud architecture.

4.1 Design Overview of Proposed Architecture

We discussed the fundamental security concerns and some safety measures related to the IoT architecture referred to in Section 3. To secure the IoT system inside, it is considered as four layers. In Fig. 4 presents our proposed method, we will review in-depth and security features of each level in detail.

Based on Patel et al. [46] research suggests the idea of a new Open Flow switch that involves IDS in it, making Open Flow protocol safer. The other author proposed a framework with the programmability benefits provided by SDN to include the IDS architecture to detect suspicious packets [47]. The authors present the definition in [48] to identify illegal activities carried out in the SDN setting. We suggest using SDN technologies and machine learning algorithms to track and detect malicious activities in the SDN data plane. We increase the performance and achieve the identification of U2R attacks.

Our proposed software-defined IDS for distributed cloud architecture specification consists of the following four components in different layers of the IoT environment: the first layer of perception consisting of IoT modules, second SDN-enabled switch, third cluster SDN controller and last SDN controller.

- *IoT devices in the perception layer*, end-users on other IoT devices should have their obligations. These IoT devices which are a collection of interconnected computing devices, mechanical, digital

machines, surveillance cameras, smart devices, wearable devices, and various other devices that are attached to an SDN switch with unique identifiers and the ability to transfer data over a network without the need for human-to-human or computer-to-computer interaction.

- *SDN-enabled switch in edge layer*, in this system, each end user is assumed to have a switch that is compatible with SDN and supports open flow protocol. The transition builds on security policies and guidelines. The switch is the endpoint of a service provider network. SDN allows switching to network service providers using a hybrid approach.
- *IDS controller in fog layer*, the end-users using in IDS controller which has the following key component. (1) Sensors able to collect data, for example, packets using TCP-dump or Wireshark, log files (for applications), system call traces (for the operating system). (2) Analyzer, the data obtained is received, evaluated, and decided whether it is intruded. And (3) user interface enables IDS performance and control actions to be interpreted by security experts, system administrators, and other users.
- *SDN controller in the cloud layer*, SDN controller remains with the telecommunication service provider at the highest level within the Soft Things system. This SDN controller manages all controllers in the IoT environment. This controller has a comprehensive overview of traffic flow and different events on the network.

Machine learning techniques have been used in conventional networks to improve SDN performance to avoid and prevent multiple IoT attacks. With intelligent attacks on the IoT framework layers, its resources, and computational constraints, it is important to explore the use of machine learning techniques to protect the IoT network and to detect anomalies against normal packets. It is understood that nowadays, however, machine learning is growing rapidly for SDN and IDS. For the edge and fog layer, which are processing, network devices capacity and storage, as fog layer have not to realize. Nevertheless, we suggest using a distributed, stable SDN controller network based on the IDS for the edge and fog layer to be virtual machines connected turn to the processing and storage unit seen as a different entity. Its use SDN for the enabled distributed cloud should not only operate the network but also track and effectively defend the network from external and internal attacks.

4.2 Experiment and Analysis

In this subsection, we run our experiment over the NLS KDD master dataset using and conducted on Ubuntu 18.10, with 6 GB of RAM and 100 GB of hard drive space on VMware. To train and test our Machine learning model, we use Weka (3.9.3) and TensorFlow, and for SDN, SDN emulator, and Maxi-Net.

4.2.1 Evaluation

The performance study of our work approach usually performed in terms of precision, recall, and accuracy. Software-defined IDS requires low false alarm high efficiency and high detection rate. The confusion matrix is used to measure those parameters; therefore, the evaluation results are the following.

- Precision indicates how many intrusions are predicted by and IDS. The higher the P, the lower alarm. The proportion of right positive classification for all positive classification.

$$P = \frac{TP}{TP+FN} \tag{1}$$

- Accuracy: Accuracy indicates the flow manifests exactly categorized around the entire traffic traces. The proportion of classifications, above all N cases, they were correct.

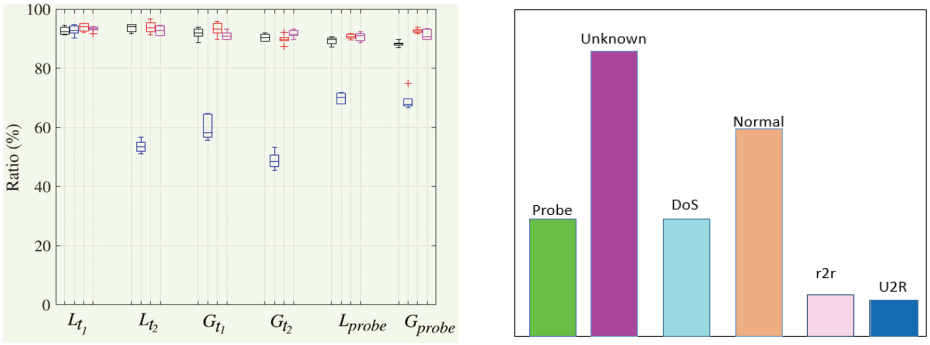
$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

- Recall shows the percentage number of expected intrusions versus any actual intrusion, its high R-value required. The proportion of positive examples which have been correctly classified.

$$R = \frac{TP}{TP+FN} \quad (3)$$

4.2.2 Graphical and tabular analysis

Accuracy was used for comparison because it calculates the ratio of correctly identified instances to the total number of instances. As shown in Fig. 5, it is clear that distributed fog solution in terms of accuracy, detection rate, recall in six separate attack scenarios. The proposed architecture is slightly lower in terms of detection rate because the device to share information to converge and make the most accurate decision.



(a) (b)

Fig. 5. Anomaly detection performance with accuracy: (a) accuracy and (b) different attack types predicted.

The performance of the proposed architecture using the NLS KDD master dataset was evaluated the combination of our chosen algorithms relative to several classes of standard feature selection and machine learning algorithms show in Table 2.

Based on the comparison and experimental evaluation, we can say that proposed architecture is beneficial for attack detection, showing that it offers better detection and accuracy than traditional methods.

Table 2. Detailed accuracy by class

TP rate	FT rate	Precision	Recall	MCC	RDC area	PRC area	Class
0.974	0.012	1.883	0.926	0.920	0.997	0.967	U2R
0.600	0.001	0.999	0.600	0.614	0.999	0.999	R2L
0.095	0.007	1.147	0.095	0.109	0.966	0.261	Probe
0.976	0.000	1.000	0.976	0.840	0.966	0.995	DoS
0.897	0.005	0.792	0.897	0.965	0.994	0.873	Normal
0.953	0.000	0.976	0.953	0.012	0.985	0.762	Unknown

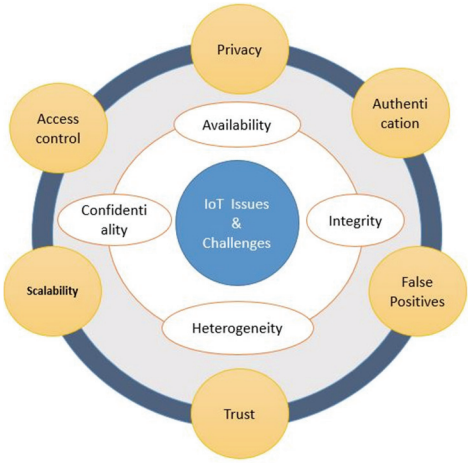


Fig. 6. IoT Issues and challenges.

5. IoT Security Issues

A great potential is provided by the IoT, where one of the main objectives is to transform the way we perform different activities and standard of living of people in the recent world. Wireless communication systems have been prone to security vulnerabilities from the very inception; therefore, it is crucial to highlight the security issues for IoT related to security and privacy that can be summarized based on Fig. 6 as confidentiality, availability, scalability, integrity, and heterogeneity.

- *Confidentiality* states that trust is a fundamental issue for IoT users sharing information by things and allows not to be compromised by an attacker. When an attacker can easily intercept messages that pass from the sender-receiver so that the privacy can be modified and leaked. Therefore, it's required a secure message for the IoT environment [49,50].
- *Availability*, as we come to rely on IoT security within our daily lives, it must consider the availability of IoT system, this potential for disruption as a result of connectivity devices failure, arising attacks such as DoS, DDoS, jamming attacks, which is considered as more than an inconvenience, therefore the impact of lack of availability could mean a loss [51].
- *Integrity*, ensuring the integrity data in an IoT network it's considered as another issue for security, due to the flow of big data generated by a large number of connected devices, it should guarantees that message has not to be altered by an attacker or unauthorized user while in transmission over the network to preserving the integrity of IoT [52]. Efforts have been made to ensure data integrity [53,54]. In near future data integrity in IoT should receive considerable attention.
- *Heterogeneity*, known as a diversity of different hardware performance over the IoT network such as an memory footprint, computation power, protocols, etc., attacks that occur on confidentiality, availability, and integrity, due to the IoT security heterogeneity issues to prevent types of attacks are too complex, the absence of common security service is the biggest problem [55].

5.1 SDN Based IDS

Enabling SDN is an evolving concept in the design and management of networks that allows optimization of network resources use. SDN is promising as a network technology that brings several advantages for IoT and provides more robust methods to improve the control of the network solutions as follows.

- Efficient network traffic management, as it provides direct and indirect control over the entire network traffic so that any suspicious traffic can potentially be detected. It is also desirable to significantly improve the use of resources for the optimal system output when it comes to the exponential growth of cloud computing and IoT devices. Enables the complex and timely control of the actions in network switches and work with each other.
- Vulnerability discovered in the near future: Operators will deal with any attacks as long as they discover the logic of the control system is instantly discovered to this type of attack, without waiting for software updates, be it an operating system or an application.
- Security, it cannot be based solely on host security, since these defenses are ineffective when the host is compromised.

Based on [56], research proposed the idea of a new Open Flow switch that includes the IDS, making the Open Flow protocol more secure. Another research was to propose a framework with the advantages of SDN programming capability to include IDS architecture for detecting suspicious packets [57]. Based on research also suggest the idea of using technology and machine learning algorithms for monitoring and detect malicious behavior in the SDN data plane. They increase the performance of attack detection and achieve higher true positive values (TPR) for DoS, U2R, Probe attacks compared with other approaches [58,59].

5.2 Challenges

In this subsection, we describe that the security and privacy of the IDS for the IoT environment are essential to maintaining and its primary concern. Knowing that IoT is relatively considered a new concept, it's needed to develop security goals. Therefore, as IoT grows because of the dynamic nature, several security challenges remain open in a various layer of the architecture shown in Table 3, which includes the following:

- Attack model: This model for IoT, since several smart devices are interconnected. Therefore, cyber attackers can conduct advanced and complicated attacks. Therefore, it is necessary to discover more realistic attack models and find a balance between detection rate and resource consumed.
- Secure alert traffic: The protection of IDS communication channels is another constant concern challenge for the IoT system. A variety of networks take over control to secure communication between IDS components and nodes across the network. As a consequence, in the IoT case, many difficulties in securing the IDS and poor protection methods are used to secure communication between nodes and sensors, so that allows the attacker to easily monitor and decrypt network traffic. The importance needs of protection with a strong IDS communication system for IoT.
- Trust: It is built on the premise that nothing is going to affect the desired individual. As a consequence, despite the IoT program, many heterogeneous networks can be compromised by being linked through the Internet. This connection with other systems brings lower security standards that can generate trust challenges. The trust system must meet and be updated with the growth of IoT devices [59]. Even though several researchers have been proposed to evaluate positive reputation and interaction, it's required further research.
- Malicious code attacks another challenge, which occurs various attacks in IoT that target application programs such as DoS, worms, it aims to attack security cameras, routers. These types of attacks can exploit the presence of software vulnerabilities. A common attack mechanism is an emerging computing system such as IoT security, a detection mechanism for IoT which focuses on individual detection threats.

- Privacy: It required special considerations for IoT to prevent user's information over the network [60]. Ensuring privacy in the IoT environment is considered as a challenge for establishing secure communication addressing related data. Privacy risk arises as the object in the IoT collect, which aggregate fragments of data.

Table 3. Security challenges in IoT layers

	DoS	Eavesdrop	Routing	Phishing	Malicious code
Application layer	×	×	×	✓	×
Network layer	✓	×	✓	×	✓
Perception layer	×	✓	×	×	✓

6. Conclusions

Today, it is believed that the number of IoT devices being connected worldwide tends to grow on daily basis; its application involves many projects. In this paper, we have identified attacks on IoT devices for which the number of recorded instances of malicious attacks continues to increase; information security experts and researchers regularly find vulnerabilities used by cybercriminals that could compromise privacy, security, and protection of consumers. As a result, the frequency and variety of security threats to these systems have increased in several ways, demonstrating the value of an effective intrusion detection system. Therefore, to summarize this paper, we presented a comprehensive survey about software-defined based IDS for IoT security environment, we provided a detailed study about each technology in a different chapter, and we studied the IoT security threats and the convergence. Experimental evaluation of proposed architecture shows that it has better detection and accuracy than traditional methods. Our future work aims to develop and implement a more reliable and secure SD-IDS technology for the IoT environment.

References

[1] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of things: challenges and opportunities," in *Internet of Things: Challenges and Opportunities*. Cham, Switzerland: Springer International Publishing, 2014, pp. 1-17.

[2] O. Vermesan and P. Friess, *Internet of Things-from Research and Innovation to Market Deployment*. Aalborg, Denmark: River Publishers, 2014.

[3] S. P. Anilbhai and C. Parekh, "Intrusion Detection and Prevention System for IoT," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 2, no. 6, pp. 771-776, 2017.

[4] S. Tanwar, S. Tyagi, and S. Kumar, "The role of internet of things and smart grid for the development of a smart city," in *Intelligent Communication and Computational Technologies.* Singapore: Springer, Singapore, 2018, pp. 23-33.

[5] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," in *Proceedings of 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, 2017, pp. 1-4.

[6] W. Meng, "Intrusion detection in the era of IoT: building trust via traffic filtering and sampling," *Computer*, vol. 51, no. 7, pp. 36-43, 2018.

[7] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naive Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5156-5170, 2018.

[8] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018.

[9] S. G. Kene and D. P. Theng, "A review on intrusion detection techniques for cloud computing and security challenges," in *Proceedings of 2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, India, 2015, pp. 227-232.

[10] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in *Proceedings of 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, 2016, pp. 84-90.

[11] C. Jun and C. Chi, "Design of complex event-processing IDS in internet of things," in *Proceedings of 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, Zhangjiajie, China, 2014, pp. 226-229.

[12] A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Junior, and C. Wills, "Autonomic agent-based self-managed intrusion detection and prevention system," in *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*, Port Elizabeth, South Africa, 2011, pp. 223-234.

[13] J. H. Lee, M. W. Park, J. H. Eom, and T. M. Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," in *Proceedings of 13th International Conference on Advanced Communication Technology (ICACT2011)*, Seoul, Korea, 2011, pp. 552-555.

[14] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, article no. 21, 2018.

[15] P. S. Kenkre, A. Pai, and L. Colaco, "Real-time intrusion detection and prevention system," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*. Cham: Springer, 2014, pp. 405-411.

[16] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.

[17] S. Notra, M. Siddiqi, H. Habibi Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in *Proceedings of 2014 IEEE Conference on Communications and Network Security*, San Francisco, CA, 2014, pp. 79-84.

[18] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things security 'Hands-On'," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 37-46, 2016.

[19] O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen, and R. Struik, "Security considerations in the IP-based Internet of Things: draft-garcia-core-security-06," Internet-Draft, Internet Engineering Task Force, 2013.

[20] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3496-3509, 2018.

[21] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based Internet of Things," in *Proceedings of 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Lyon, France, 2013, pp. 600-607.

[22] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2016.

[23] A. Abduvaliyev, A. K. Pathan, J. Zhou, R. Roman, and W. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223-1237, 2013.

[24] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," in *Proceedings of 2013 IEEE International Conference on Computational Intelligence and Computing Research*, Enathi, India, 2013, pp. 1-7.

[25] H. A. Arolkar, S. P. Sheth, and V. P. Tamhane, "Ant colony based approach for intrusion detection on cluster heads in WSN," in *Proceedings of the 2011 International Conference on Communication, Computing & Security*, Rourkela, India, 2011, pp. 523-526.

[26] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, Abu Dhabi, United Arab Emirates, 2017, pp. 31-38.

[27] T. Jiang, G. Wang, and H. Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks," in *World Automation Congress 2012*, Puerto Vallarta, Mexico, 2012, pp. 259-261.

[28] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1 & 2, pp. 1-9, 2009.

[29] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: a survey of common practices," *ACM Computing Surveys*, vol. 48, no. 1, Article no. 12, 2015.

[30] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in *Proceedings of 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2016, pp. 319-320.

[31] G. Han, J. Jiang, W. Shen, L. Shu, and J. Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *IET Information Security*, vol. 7, no. 2, pp. 97-105, 2013.

[32] T. Sherasiya, H. Upadhyay, and H. B. Patel, "A survey: intrusion detection system for Internet of Things," *International Journal of Computer Science and Engineering*, vol. 5, no. 2, pp. 91-98, 2016.

[33] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Proceedings of 2014 IEEE International Conference on Industrial Engineering and Engineering Management*, Bandar Sunway, Malaysia, 2014, pp. 1244-1248.

[34] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: an IoT perspective," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 22, 2019.

[35] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of PUF-based hardware security solutions for the internet of things," in *Proceedings of 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Abu Dhabi, United Arab Emirates, 2016, pp. 1-4.

[36] P. Sethi and S. R. Sarangi, "Internet of Things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, article no. 9324035, 2017.

[37] D. M. Mendez, I. Papapanagiotou, and B. Yang, "Internet of Things: survey on security and privacy," 2017 [Online]. Available: https://arxiv.org/abs/1707.01879.

[38] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.

[39] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Proceedings of 2008 The 28th International Conference on Distributed Computing Systems*, Beijing, China, 2008, pp. 3-10.

[40] R. P. Kurbah and B. Sharma, "Survey on issues in wireless sensor networks: attacks and countermeasures," *International Journal of Computer Science and Information Security*, vol. 14, no. 4, pp. 262-269, 2016.

[41] S. Fosso Wamba, A. Anand, and L. Carter, "A literature review of RFID-enabled healthcare applications and issues," *International Journal of Information Management*, vol. 33, no. 5, pp. 875-891, 2013.

[42] M. S. Van Devender, W. B. Glisson, M. Campbell, and M. A. Finan, "Identifying opportunities to compromise medical environments," in *Proceedings of Twenty-second Americas Conference on Information Systems*, San Diego, CA, 2016, pp. 1-9.

[43] J. Deogirikar and A. Vidhate, "Security attacks in IoT: a survey," in *Proceedings of 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017, pp. 32-37.

[44] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): taxonomy of security attacks," in *Proceedings of 2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, 2016, pp. 321-326.

[45] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269-284, 2016.

[46] A. Patel, S. Jain, and S. K. Shandilya, "Data of semantic web as unit of knowledge," *Journal of Web Engineering*, vol. 17, no. 8, pp. 647-674, 2018.

[47] D. Jankowski and M. Amanowicz, "Intrusion detection in Software Defined Networks with self-organized maps," *Journal of Telecommunications and Information Technology*, vol. 4, pp. 3-9, 2015.

[48] D. Jankowski and M. Amanowicz, "On efficiency of selected machine learning algorithms for intrusion detection in Software Defined Networks," *International Journal of Electronics and Telecommunications*, vol. 62, no. 3, pp. 247-252, 2016.

[49] S. Rathore, P. K. Sharma, V. Loia, Y. S. Jeong, and J. H. Park, "Social network security: issues, challenges, threats, and solutions," *Information Sciences*, vol. 421, pp. 43-69, 2017.

[50] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): a review," *Journal of Computer Networks and Communications*, vol. 2019, article no. 9629381, 2019.

[51] S. Hameed, U. M. Jamali, and A. Samad, "Integrity protection of NDEF message with flexible and enhanced NFC signature records," in *Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 368-375.

[52] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: a big picture," *Future Generation Computer Systems*, vol. 49, pp. 58-67, 2015.

[53] Q. Gou, L. Yan, Y. Liu, and Y. Li, "Construction and strategies in IoT security system," in *Proceedings of 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, 2013, pp. 1129-1132.

[54] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721-743, 2020.

[55] I. R. Chen, J. Guo, D. C. Wang, J. J. P. Tsai, H. Al-Hamadi, and I. You, "Trust-based service management for mobile cloud IoT systems," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 246-263, 2019.

[56] Z. Zhang, J. Jing, X. Wang, K. K. R. Choo, and B. B. Gupta, "A crowdsourcing method for online social networks security assessment based on human-centric computing," *Human-centric Computing and Information Sciences*, vol. 10, Article no. 23, 2020.

[57] L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment," *Human-centric Computing and Information Sciences*, vol. 10, Article no, 15, 2020.

[58] A. Abubakar and B. Pranggono, "Machine learning based intrusion detection system for software defined networks," in *Proceedings of 2017 7th International Conference on Emerging Security Technologies (EST)*, Canterbury, UK, 2017, pp. 138-143.

[59] S. K. Singh, Y. S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustainable Cities and Society*, vol. 60, article no. 102252, 2020.

[60] Y. S. Jeong and J. H. Park, "Security, privacy, and efficiency of sustainable computing for future smart cities," *Journal of Information Processing Systems*, vol. 16, no. 1, pp. 1-5, 2020.

[61] S. Kumar, T. Kumar, G. Singh, and M. S. Nehra, "Open flow switch with intrusion detection system," *International Journal of Scientific Research Engineering & Technology*, vol. 1, no. 7, pp. 1-4, 2012.

Jose Costa Sapalo Sicato **https://orcid.org/0000-0002-7834-2268**

He received Bachelor's degree in Telecommunication engineer from the International University of Management in 2015, Namibia and Diploma in PC engineer from the Institute of Information Technology from 2009 to 2011 in Namibia. Since 2018, he is a Master's degree Scholar at the Seoul National University of Science and Technology. His current research interests include SDN, artificial intelligence, big data, and the IoT.

Sushil Kumar Singh **https://orcid.org/0000-0003-2926-3931**

He received his M.Tech. degree in Computer Science and Engineering from Uttarakhand Technical University, Dehradun, India, in 2018. He also received an M.E. degree in Information Technology from Karnataka State University, Mysore, India, in 2011. Currently, he is pursuing his PhD degree under the supervision of Prof. Jong Hyuk Park at the UCS Lab, Seoul National University of Science and Technology, Seoul, Korea. He has more than 9-year experience of teaching in the field of computer science. His current research interests include blockchain, artificial intelligence, big data, and the Internet of Things. He is a reviewer of the *IEEE SYSTEMS* Journal, *FGCS*, *Computer Network*, *HCIS*, *JIPS* Journal, and others.

Shailendra Rathore **https://orcid.org/0000-0001-8053-2063**

He is a PhD student in the Department of Computer Science at Seoul National University of Science and Technology (SeoulTech.), Seoul, Korea. Currently, he is working in the Ubiquitous Computing Security (UCS) Lab under the supervision of Prof. Jong Hyuk Park. His broad research interest includes Information and Cyber Security, SNS, AI, IoT. Previous to joining Ph.D. at Seoul Tech, he received his M.E. in Information Security from Thapar University, Patiala, India.

James J. (Jong Hyuk) Park **https://orcid.org/0000-0003-1831-0309**

He received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December 2002 to July 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September 2007 to August 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences–MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of *Human-centric Computing and Information Sciences* (HCIS) by Springer, The *Journal of Information Processing Systems* (JIPS) by KIPS, and *Journal of Convergence* (JoC) by KIPS CSWRG. He is an Associate Editor / Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.