A Review on Honeypot-based Botnet Detection Models for Smart Factory

Lee Seungjin[1], Azween Abdullah[2], NZ Jhanjhi[3]
School of Computer Science and Engineering (*SCE*)
Taylor's University
Subang Jaya, Selangor, Malaysia

Abstract*—Since the Swiss Davos Forum in January 2017, the most searched keywords related to the Fourth Revolutionary Industry are AI technology, big data, and IoT. In particular, the manufacturing industry seeks to advance information and communication technology (ICT) to build a smart factory that integrates the management of production processes, safety, procurement, and logistics services. Such smart factories can effectively solve the problem of frequent occurrences of accidents and high fault rates. An increasing number of cases happening in smart factories due to botnet DDoS attacks have been reported in recent times. Hence, the Internet of Thing security is of paramount importance in this emerging field of network security improvement. In response to the cyberattacks, smart factory security needs to gain its defending ability against botnet. Various security solutions have been proposed as solutions. However, those emerging approaches to IoT security are yet to effectively deal with IoT malware, also known as Zero-day Attacks. Botnet detection using honeypot has been recently studied in a few researches and shows its potential to detect Botnet in some applications effectively. Detecting botnet by honeypot is a detection method in which a resource is intentionally created within a network as a trap to attract botnet attackers with the purpose of closely monitoring and obtaining their behaviors. By doing this, the tracked contents are recorded in a log file. It is then used for analysis by machine learning. As a result, responding actions are generated to act against the botnet attack. In this work, a review of literature looks insight into two main areas, i.e. 1) Botnet and its severity in cybersecurity, 2) Botnet attacks on a smart factory and the potential of the honeypot approach as an effective solution. Notably, a comparative analysis of the effectiveness of honeypot detection in various applications is accomplished and the application of honey in the smart factories is reviewed.

Keywords*—IoT; smart factory; honeypot; Botnets; detection; security; model

I. Introduction

Smart plant strategies are being pushed forward to innovate global manufacturing competitiveness. Germany is undergoing the Industry 4.0 process. It builds manufacturing into an automatic production system through the Internet of Things, Initiated in China 2025 in China, Terrain Manufacturing System in Japan and Seoul is pushing for Manufacturing Innovation 3.0 [1]. Smart factories in the era of the Fourth Industrial Revolution refer to consumer-oriented intelligent factories that incorporate digital new technologies and manufacturing technologies beyond the current level of factory automation (FA). It can produce a variety of products from one production line and is expected to change from mass customization to flexible production systems through modularization. It is possible to save energy by changing from a person-centered working environment to an ICT-oriented one, and it is expected that the productivity of the manufacturing industry will increase [2], Various possibilities for the transition to smart factories are recognized. It is predicted that it will be able to monitor and control manufacturing sites via virtual space, making it easier to manage factories. It will enhance competitiveness in quality and cost [3]. Smart factories are closely linked to data by application of the latest ICT technologies such as AI, Blockchain and hyper-automation, Augmentation as well as IoT as shown in Fig. 1.

Based on that, production processes are controlled on their own, making the industrial control system (ICS, Industrial Control System) more complex and advanced than the ordinary systems. However, due to the complexity of the system and the application of new technologies, the advancement in smart factories raises the risk of new security threats that have not occurred earlier. Specifically, the number of attacks on actual cyber vulnerabilities has increased sharply in recent years on physical equipment and software in power generation, energy, and manufacturing [5].

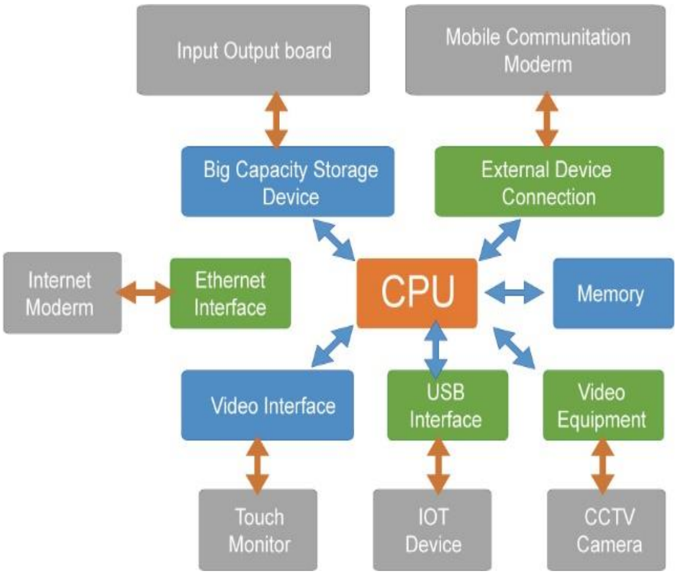

Fig. 1. Smart Factory Function Requirements[4].

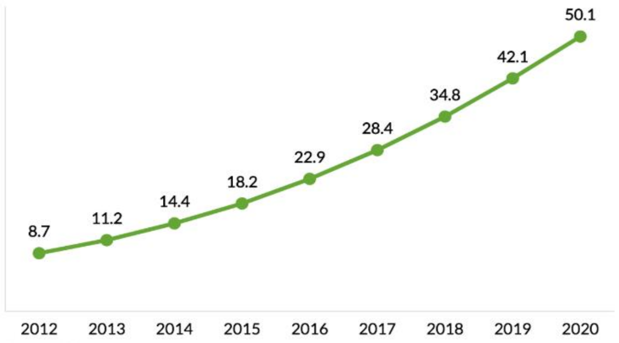

Fig. 2. Growth in the Internet of Things Devices [9].

In order for smart factories to operate and maintain their autonomy, they must analyze themselves and accurately carry out product design as well as quality process management and production management. It utilizes important information such as process know-how, requirements of analysis data, product design diagrams, business secrets and research and development results. The threat of leaking confidential information by exploiting the security vulnerability of wireless communications via remote control or monitoring of systems in a factory using wireless devices could cause severe damage and economic loss.

In the last five years, there is a tremendous increase in the use of IoT devices from 8 billion to 25 billion, noticeably in the application for smart factories [6]. However, one significant limitation of these IoT devices is its instability, as identified in 250 vulnerable features (shown in Fig. 2) [7]. In an analysis of 10 most popular IoT devices such as the open telnet ports, firmware of outdated Linux and the transmission of sensitive data without being encrypted [8]

Due to the instability of the IoT devices on the infrastructure of the Internet, they become an ideal target of the IoT botnet with a surging number of attack cases. A good example is an attack that occurred in October 2016 when the Dyn DNS infrastructure involving 100,000 IoT devices (mainly on CCTV cameras). It was under the attack of a DDoS (distributed denial of service) caused by Mirai botnet. This DDos attack resulted in temporary unavailability in several commercial websites like Amazon, Netflix, Twitter, CNN and PayPal. Another example is the new Mirai source code released in 2017. It rendered increasing DDos attacks. Such Mirai-induced IoT botnets occurred more frequently in recent times and their consequences became more severe. Thus, the identification and mitigation of IoT botnets are urgently needed due to the development of new technologies [10].

With a great potential of machine learning (ML) emerging recently, it offers a new solution for anomaly detection of any malicious internet traffic. Indeed, internet traffic is distinct from other Internet-connected devices (smartphones and computer laptops) in a way that communication between IoT devices is allowed by small endpoints contained in a limited set. In contrast, internet-connect devices use a variety of web servers. Moreover, for the IoT devices, the patterns of network traffic are repetitive in the regularity of network pings with small packets for logging. Interestingly, there is a scarcity of research investigating in development of ML models featured in networks of IoT devices and attacks in IoT traffic using the machine learning approach.

Botnets are a collection of computers associated with the Internet that are compromised and are controlled distantly by intruders through malicious software, normally called bots. Malicious software is generally used by attackers [11]. Mirai botnet. It was recently unveiled as an open source, used the vulnerability of such an IoT device to launch a botnet attack on the DSN provider, DYN. The reason for the significance of a botnet attack is that it was not a computer but an IoT device such as a webcam. Besides, similar incidents are expected to occur due to the open code as well as attacks that have already been carried out. Mirai botnet starts with an attacker approaching a random IP address. An attacker uses a pre-specified ID and password to gain root privileges on the device. An attacker has an ID and a cryptographic list of several IoT devices that are specified when a product is sold, thereby gaining the device's ROOT authority from the contents of the list. This is a vulnerability that occurs because users do not change passwords on their IoT devices even after they purchase the products [10].

If root privileges are obtained in this way, the shell script executes an infection behavior in the device. The infection code is downloaded and executed from the attacker's loader server to infect the device completely. When the surveillance is complete, a standby message is sent to the attacker's C&C server in Fig. 3 [12]. The same routine that infects other IoT devices and increases the bot exponentially. The attacker then sets a target of the attack and commands the bots to execute the DDOS attack as the target of an attack on the attacker server. To prevent the infection of the BOT of a DDOS attack, the code of the attacker, who is connected to find, defend and detect attacks of the same pattern was proposed to be analyzed [13].

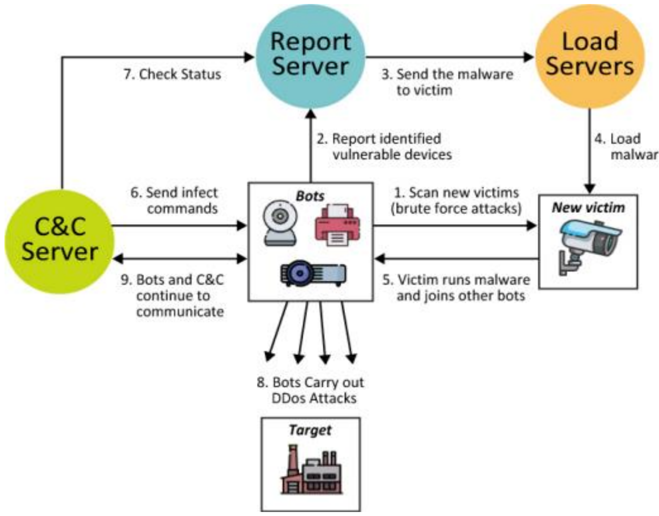
Report Server
Load Servers
7. Check Status
3. Send the malware to victim
2. Report identified vulnerable devices
4. Load malware
C&C Server
6. Send infect commands
Bots
1. Scan new victims (brute force attacks)
New victim
9. Bots and C&C continue to communicate
5. Victim runs malware and joins other bots
8. Bots Carry out DDos Attacks
Target

Fig. 3. Mirai Botnet Operations [12].

A. Review Aim

The review aims to compare various methods of detecting botnet attacks and to evaluate the potential of using honeypot as a solution to botnet attacks in the smart factory situation.

II. Related Work

The work mainly focuses on two sections. The first section presents the threat of cyber-attacks to the IoT based system and narrows the case of the smart factory with the utilization of IoT equipment. The second section addresses the latest security solutions to the botnet attack, especially honeypot detection for a smart factory. A comparative analysis is made among related studies with respect to the advantages and disadvantages of the honeypot and other similar methods. Finally, future work is suggested for developing a botnet detection model using the Honeypot approach.

A. Smart Factory Security

In the Industry 4.0, smart factories raise interest in manufacturing companies and academic researchers [14]. Although smart factories are already constructed and operated in the industry, implementation standards are yet to be established for smart factories [15]. The manufacturing system could be rated in scale based on different perspectives, such as function [16]. A smart factory is conceptualized as adaptive and flexible manufacturing consisting of three aspects, i.e., interconnection, collaboration and execution [17]. Furthermore, systems in the smart factory's architecture for IoT are segregated into four layers arranged hierarchical starting at physical resource layer, networking layer, application layer and interface layer, as shown in Fig. 4 [18] [19]. With the aim of transforming a modern factory into a smart factory, key technologies related to all layers require in-depth research.

The key element of a smart manufacturing system, such as smart factories is intelligence. It is based on network technology and manufacturing data. Additionally, system maintenance and requirements of manufacturing should be incorporated into the implementation of smart factories. Due to such complexity in the design and operation of the smart factories, many technical problems arise and need to be solved [20].

Although the industrial radio sensor network (IWSN) has advantages for industrial manufacturing networks, the Internet of Things (IoT) can be used to apply for the network layer with support of new protocols and new data formats at higher flexibility and scalability. At the data application layer, the cloud platform should be able to perform semantic analysis of various data. Therefore, modeling smart plants should consider the employment of ontology to provide self-organization, self-learning and self-adaptation capabilities. In addition, data analysis and data mining are useful to provide a scientific basis for decision-making and design optimization, respectively. All layers of smart factories are developed and analyzed by focusing on core technology [21].

At the sensing or physical resource layer, the acquisition of real-time information is obtained by physical equipment and transmission of heterogeneous information at high-speed through communication devices. As a result, rapid reconfiguration and adaptability have to be ensured at the workplace by increasing the intelligence of these basic devices/equipment to meet the requirements for the Internet of Things [22]. In the entire operating cycle of smart factories, including the physical resources, the efficiency of smart manufacturing to produce customized products creates new demand for adjusting manufacturing equipment, production lines and data acquisition. Due to the limitation in flexibility and configurability, current manufacturing equipment in the workplace is highly specific and relatively narrow in scope, making it vulnerable to adapt to changes in the manufacturing environment.

Some manufacturing equipment such as robots, mechanical arms, machining centers can be modulated in the manufacturing unit to improve a dynamic scheduling. This leads to a reconfiguration of the controller and extension of the manufacturing equipment function. The assembly capability of the workshop can be improved to be more adaptive and self-configurable at the robotic islands for each modular manufacturing units. Because of this, the capability of flexible manufacturing can be enhanced at the integrated management level [20]. A variety of algorithm was proposed [23]. This is for the reconstruction of grid-based, modular self-reconfiguring robots that dramatically simplify the complexity of robot configurations through a repetitive approach.

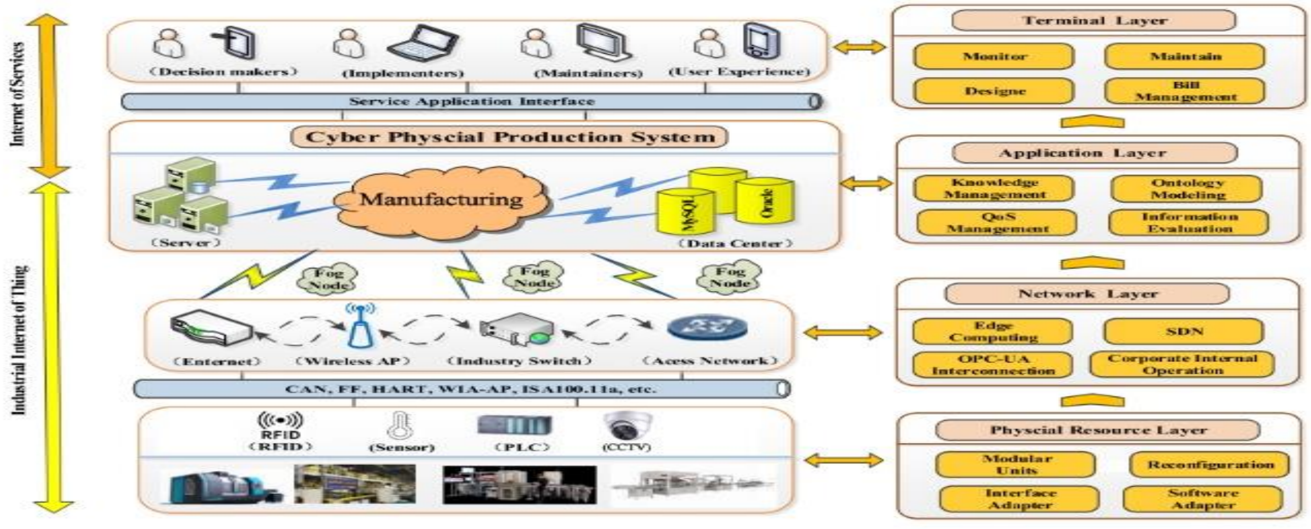

Fig. 4. Function Requirements of Smart Factories [18].

cyber-physical integration of cognitive robots in manufacturing was proposed [24]. Specifically, a humanoid robot is used to integrate with the smart manufacturing plant in coordination with the execution system. These robots can cognitively adjust their own manufacturing behaviors to recognize information uncertainty, changes in schedule management and independently dealing with complex problems of manufacturing. There is a relationship between the level of intelligence of smart factories and the modular maturing units. Therefore, increasing the intelligence of the modular manufacturing units such as robotic units is very important to allow them to work together to accomplish common tasks by mutual recognition and co-working mechanisms. The heterogeneity of interactions should also be considered. It is important to create an optimal or lane combination method because the functions of other modular manufacturing devices can be duplicated for a particular product. Each manufacturing unit not only meets the manufacturing requirements of the product, but it can also systematically improve the smart factory efficiency on its own. However, a deadlock can occur in smart manufacturing as some different products enter the production system in a disordered manner [25]. Currently, a solution to a deadlock in a flexible manufacturing system increasingly becomes a research interest [25].

Smart factories operate in an IoT platform. It collects and processes information from various RFID devices [26]. Fig. 5 shows the system structure of the study that manages various data by integrating middleware and sensors (RFID readers) into a single framework based on RFID security network systems. RFID is a technology that collects information from tags through signals that detect and transmit radio frequencies from tags installed on devices. The application of RFID technology is considered to be the key to establishing an environment for smart factories with ubiquitous security networks. Because of the many advantages in the real-time product, equipment transportation and automatic information collection, various areas such as plant facility management and worker safety management are being applied [27]. Besides that, RFID technology is also used in building security networks of the smart factories by gathering tags and removing duplicated or unnecessary tag information. RFID middleware is needed to provide information only in application programs and to manage security under the framework [27].

The RFID system is constructed. The RFID system consists of a reader, a questionnaire, a tag and a transponder. Readers need to recognize tags in the fast-paced reading range. The reader has a radio communication module and an interface to communicate with the antenna, power supply, math and memory and host systems. The reader is relatively less restrictive in terms of power, computing power and memory size. It can be divided into fixed and mobile types depending on its mobility. The reader sends the identified tag information to the host computer system. It consists of database and application software to processes the tag information [29].

Tags being attached to objects are in the form of microchips with unique allocation IDs that contain information about each object. The tag has relatively big limits on the power, operating functions, adding memory and antenna size required to operate a circuit. Tags can be classified into different types depending on the nature of the internal memory or the presence of batteries. Classification of RFID tags is made according to the characteristics of the internal memory or the availability of batteries [30]

RFID tags, which are widely used in smart factories in IoT platforms, are equipped with a variety of memories, i.e. to read-only or to read/write memory types. The classification of RFID tags is based on battery installation. First, passive tags have no power source for their own functions. Instead, they utilize the power generated by the electromagnetic signals of the readers with similar functions. Secondly, semi-passive tags equipped with their own internal battery are able to be identified at a longer distance. Thirdly, active tags are more advanced than the semi-passive tags. Due to their longer wavelength and their own supply of power, their capacity covers are not only for channel detection but also for collision detection. In comparison between the three RFID tags, the active tag is the most expensive, followed by the semi-active whereas the more economical one is the passive tag [31].

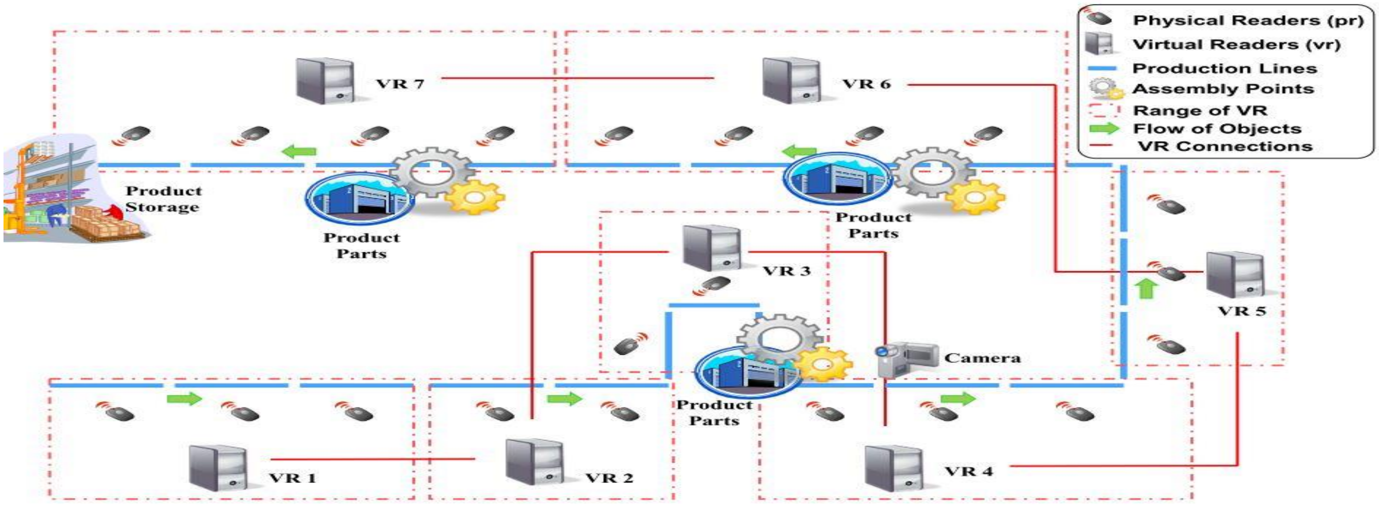

Fig. 5. RFID System Deployment in Smart Factories [28].

Data written on the RFID tags are collected by the process sensors, known as RFID tag readers. These data are then combined to become real-time information for smart factories to analyze in the IoT platform. Such analyzed information is crucial for communication like warning notifications for the management [28].

B. Botnet Detection

Serious damages caused by botnet attack occurs in online banks, e-commerce Internet systems and industries as a whole. Such damages become increasingly threatening to users as well as the service providers. Therefore detection is imperative.

One of the severe cybercrimes is botnets, which are termed software robots or boats that operate automatically and systematically. A four-stage bot is typically created and maintained. Zombie computer groups are controlled remotely by attackers who call them botmasters [32].

Stage 1 - Initial infection: The computer can be infected in several different ways. For example, 1) being actively exploited. There are some vulnerabilities in the host, such as DCE-RPC. The malware then runs on the host and exploits the vulnerability, 2) The malware is automatically downloaded while viewing the web page, 3) The malware is downloaded and executed automatically by opening an e-mail attachment, 4) USB autorun.

Stage 2 - Injection: In this stage, the infected host downloads and runs the bot code and then becomes a real bot. Downloading is available via FTP, HTTP and P2P (e.g., Trojan horses).

Stage 3 - Malicious activity: The bot communicates with the controller to get instructions for performing the activity like spam, DDoS and scanning. Currently, there are more sophisticated methods called fast flush service networks. Command communication can avoid single points of failure using IRC-based, HTTP-based, DNS-based, or P2P protocols[33].

Stage 4 - Maintenance and upgrade: Botnets are always classified according to control structures and commands. The bot will continue to upgrade its binary number. At this stage, for example, the Internet Relay Chat (IRC)-based bonnet is an IRC protocol user[34]

Network devices that have a low level of information security and mass distribution of personal computers, as well as IoT devices, are the attractive targets for cybercriminals. The most serious attacks in recent years have been made by a botnet consisting of unsecured IoT devices. Among the botnets, Mirai botnet, as the largest botnet in history, has affected a vast number of IoT devices [35]. The working principle of the Mirai is that performing an IPv4 address space scan to identify vulnerable devices with open port TCP / 23 and TCP / 23233 [36] used by the network service TELNET [37] and then conduct a robbery attack on these ports.

In the work of Nguyen et al., (2020), the mechanism of spreading Mirai botnet was identified and its effects on IoT devices investigated. A combination of more than 60 basic user credentials is employed in Mirai to access the shell of any devices which are open to the public. Once, a smart device becomes a part of the botnet, other connected devices which are subjected to vulnerability as it will scan for other IPv4 address spaces. It would be subsequently identified and damaged. Despite becoming a botnet, receiving the order of the energy to perform malice, the botnet infected devices are still able to carry out the default activities set by the manufacturer. Such attacks caused by Mirai botnet has laid a foundation for the rising of botnet targeting IoT devices such as botnet list and botnet amnesia. For example, the attack that happened to Telnet and SSH services caused by most botnets resulted from gaining unauthorized access to IoT devices. Another example is the unauthentic access to nearly 400,000 IoT devices via two services reported in the Cybersecurity Survey on IoT [38]. Therefore, due to the availability of numerous network devices that are vulnerable to protection, botnets remain one of the main concerns of cyberspace. To become a useful part of the botnet, vulnerable network devices go through the step sequence.

The first step of the lifecycle compromises with vulnerable devices that are considered potential boats. In the second step, the malicious code that is required to communicate with the botmaster is downloaded and installed. The third step is to connect to the Command and Control (C&C) server and receive instructions from the botmaster. The next step is malicious activity, which assumes malicious behavior in accordance with the instructions of the botmaster of the infected host. The final step consists of upgrades and maintenance. This step is essential for botmasters to effectively monitor infected hosts as long as possible and modify their behavior as follows: installing malware updates to prevent the loss of large-scale malicious activity by botnets, breaking the representative chain at any stage.

Other detection methods are for after botnet penetration. In particular, post-intrusion measures are much less effective in terms of detection rates. Contrary to previous research, honeypot protects IoT equipment inside the smart factory by installing the trap in advance, not after the botnet intrusion. The following studies compare the pros and cons.

Signature-based detection is a method of analyzing, scaling and detecting botnets based on their knowledge. A typical one is Snort. The signature-based detection method has the advantage of high detection and low false detection for botnets and malware, as previously found. However, if a new botnet attacks, it is not able to detect it because it does not have a signature. For example, in Lishi, a bot is judged by the IRC name of the bot. The IRC name of the boat was thought to be much different from the nickname of the end-user. However, making IRC nicknames similar to end-users is difficult to detect and impossible to detect without an IRC-based botnet [39].

Anomalies-based detection is a way to suspect and detect strange things that behave differently than normal users in the network traffic, such as intensive traffic or abnormal port use. Yeung's study presented a method for detecting botnets by analyzing the data flow data of the transport layer. The data suspected from the bot is extracted separately from the data flow and scores are calculated and determined by the bot if the score exceeds the threshold. This method is detectable, even if botnet communication is encrypted and has a low error rate. It is also highly scalable and can help to measure the size of a botnet. Again, only IRC-based botnets can be detected [40].

Bots communicate through command and control, bots and botmasters exchange messages to regularly perform certain tasks. Botnet relies heavily on C&C servers and provides low-latency communication [41]. The botsniffer, HTTP-based botnets can also be detected, and abnormal detection technologies can be applied to stop all bots. In addition, servers as channels are detected in similar types of behavior i.e., flexible in the substation of C&C server addresses. It also provides the information needed to detect hybrid botnet structures[42].

Mirai botnet detection using binary code is a classic method developed by Lee Jun-soo. First, the binary code of the malicious code is analyzed and the structure of the binary file is determined before it is used [43]. For example, the binary code is described as a portable file structure that runs in a Windows environment. PE format should be implemented based on the nature of the detection, i.e., compatibility in various operating systems (OS) to facilitate detection. So, it was named the “Easy Movement” format. This is because this format is a file format for executable files used in Windows, such as Dynamic-Link Library (DLL), Object Code (object code) and FON-type font files. Similar to PE, there are executable files and connection formats (ELF) and Mac OS X formats, which are x86-based UNIX and UNIX systems[44].

Honeypot is a system that is installed with a purpose to detect abnormal access and it also serves to track down attackers and gather information. To deceive an attacker, a trap is created, as if the attacker had infiltrated into a normal system. And then a bot is caught and analyzed. Based on the analysis results, software disguised as a bot is created and traffic exchanged with the software is analyzed to find a botmaster or botnet. One advantage is that botnets can be detected at a high detection rate without existing knowledge [45].

Kippo: Medium Interaction SSH Honeypot can add or delete files through a fake file system and save files separately on the host system when downloading them. It also configures simple command execution and setup files. It can record Burt Force attacks and malicious user behavior [46].

Cowry: Similar to Kippo’s Honeypot, Telnet service, SFTP and SCP are added to allow the collection of uploaded files via Telnet and SSH attack houses, SFTP, and SCP [47].

Dionaea: uses libemu to detect shellcodes with Python honeypot. It supports IPv6 and TLS to collect malicious codes by providing vulnerabilities to malicious users[48].

Telnet-IoT-Honipat: Honeypot for collecting Telnet attacks is written in Python and mainly collects malicious botnet codes. Then the collected malicious code to Virus Total is uploaded [49].

IoTPOT: jointly developed by German and Japanese universities. It consists of Honeypot and Sandboxes against Telnet attacks. It provides Telnet service for various IoT devices and consists of two parts. The front end provides a low level of interaction and the back end provides a high level of interaction through an environment called the IoTBox. The IoTBoX integrates eight CPU architectures, including Mips and ARM, to provide a variety of virtual environments commonly used in the systems. However, the use is limited until it is released, not for open-source [50]

C. *Potential of Botnet Attack to Smart Factories and the Honeypot Approach*

The network environment in the smart factory will require both the new honeycomb system and the IDS method to be deployed if the honeypot detection system is applied. It also designs scalable honeypot clients that perform and interact efficiently. The purpose of their study will be to increase capture capacity and establish in-depth analysis. The autonomous version of the honeypot implementation was addressed by [51].

There is a high possibility that some major attacks will target smart manufacturers, especially those smart factories using IoT technologies. Typical IoT nodes can be directly attacked by individuals within the radio range, such as relatively low-power processors and wireless networking functions. This undermines the security model in which borders and devices (e.g., firewalls and intrusion detection systems) are defined. Instead, each device needs to be self-secured, at least in part and this is a task that becomes more difficult due to the reduced processing power of typical IoT nodes. Normally, manufacturers may not be aware of large-scale attacks that do not adequately secure individual devices.

Botnet Mirai [35], the biggest cause of distributed denial-of-service attacks, is the best example and hypothesis of the failure of the smart manufacturing defense. Operation of the Miribot Net allows Mirai to identify vulnerable IoT devices that can be accessed using the Internet.

Once these devices are identified, an attack is carried out using a simple pre-attack (composed of factory default user names and passwords belonging to users such as administrators) [5]. The boat sees the identified IP address of the vulnerable device (1), reposts it to the server (2) and then deploys the vulnerable device to the load server (3). The load server loads the malware associated with the operating system (4). When the device executes malicious code, bot (5) appears and receives new commands from the command and control server (C&C server) (6). Mirai also has the ability to eradicate other malware processes by closing all processes using SSH, Telnet and HTTP ports, searching for and removing other botnet processes that may be running on the device. The C&C server communicates with the report server to keep an eye on the infected devices (7). The boat carries out distributed denial-of-service attacks on targets (8), continues to scan and infect new victims and receives further instructions from C&C Server (9) [12].

It will take advantage of the lack of security in IoT devices and carries out a successful approach that can cause production downtime and negatively affect the company’s reputation due to equipment failure or attacks on other systems.

The operation of smart factories on the IoT platform reveals some features. It became vulnerable to the Botnet attack.

Web interface insecure: Loss or damage to data can be caused by unsafe web interfaces [52].

Lack of accountability or denial of access can lead to a complete device takeover. (security impact) [53].

Lack of transport encryption: Depending on the data exposed, user accounts or devices lose data or become completely corrupted (e.g., sending unencrypted credentials and data) [52].

Privacy concerns: Data collection of the smart factories, along with a lack of data protection, can lead to a compromise of a user's personal data.

The threat of botnet attacks on smart factories can possibly be encountered by applying honeypot as a detection method. This is because the honeypot approach presents the following special features: Able to capture attack into log files. And log analysis allows for details about exploitation and attack patterns to be found. Able to capture anything that interacts with them, including tools or tactics which have not seen before (0-Days).

Only deal with incoming malicious traffic. So, the collected information is smaller and has a higher value. Fewer false positives compared to other security solutions since only attack traffic is detected (no legitimate traffic). Require minimal resources with no additional budget for the companies. Simple to understand, to configure and to install. Do not require known attack signatures (unlike IDS). Able to detect an IPv6-based attack the same way it does with an IPv4 attack. Besides the good features, limitations of the honeypot detection method are also presented: it suffers from fingerprinting: it is easy for an experienced hacker to differentiate between a fake system and a real one. The risk of being hijacked by the honeypot system (if not adequately designed) may be used to attack other systems. Limited visions: a honeypot can only capture data involving directly interacting hacking activity.

Industrial manufacturers need to maximize production and plant management efficiency. It is important to understand and resolve issues that occur in the manufacturing process. Finding security-related issues is critical in running the operating system smoothly. In addition, concerning the management of smart factories involving the use of various IoT equipment, the recent threat of botnet has become a problem because it has caused considerable damage to production. Since botnet attacks are becoming increasingly more serious, it is an urgent matter for producers to detect botnet. Problems with data transfer between botnets, sensors, CCTVs, PLC equipment, and main database servers may be affected by data leakage in the smart factory network which resulted in data updates being exploited by unauthorized users who may cause unexpected impact on smart factory operations. Indeed, real-time detection is of paramount importance, especially in smart manufacturing environments [11]. Various methods of detecting botnet are compared, as shown in Table I. Honeypot and honeynet can respond to attacks in real-time and attract attackers to deceptive assets rather than real assets. For binary, anomaly and C&C detection methods, reaction to real-time is slower than honeypot and honeynet method [43], [57], [58]. Although binary detection is simple in structure, the detection processing is too slow for smart manufacturing environments that seek real-time detection. In terms of cost-effectiveness, honeypot has an advantage in being capable of responding to attack in real-time at relatively low cost for construction and management. It is suitable for smart manufacturing environment [55], [56] However, processing botnet information by the honeypot is slow for analysis. It results in a decrease in accuracy and processing speed [59], [60]. Notably, an attempt of using machine learning techniques to combine with honeypot has not studied so far.

TABLE I. COMPARISON OF HONEYPOT VS. OTHER DETECTION METHOD

Division	Honeypot	Honeynet	Binary detection	Anomaly detection	C&C detection
Configuration form	One host	General host Security solution Honeypot Network	BINARY	Heuristic Rules[54]	SERVER
Advantages	High Efficiency of Collective Data Efficient Packet Data Processing Install, apply, operate, and manage [55]	Application flexibility Excellent data collection and warning Applicable to various systems and applications[56]	Suitable computer application Only 1 & 0 are being used, implementation becomes easy[43]	Systems have the capability to detect zero-day attacks as well [57]	It has the advantage of being able to detect and expand HTTP-based botnets.[58][41]
Disadvantages	Intrusion into the network Information analysis slow [59]	Difficult to set up and build [60]	Long-term processing [61]	Not simple structure high false-positive [62]	In the case of botnets with large delays, the detection rate drops, and the false detection rate increases.[63][42]
Research Gap	Botnet is highly efficient in collecting data and easy to build and manage detection However, information analysis is slow.	Data collection and alerting against botnet attacks are quick. It takes a lot of time to build a system for the first time.	The structure of the system is very simple, and the computer is highly recognizable. However, the process is too slow. So not suitable for smart factory environment	It is good for detecting attacks that attack vulnerabilities such as zero-day, but the program structure is complex, and the probability of failure is high.	There are many IoT devices used for the smart factory. If there is a high probability of a delay in IoT communication devices such as RFID, the detection rate and error rate will automatically increase. Not suitable for the smart factory environment.

TABLE II. HONEYPOT STAGE OF INTERACTION

Interaction stage	Pros	Cons	Honeypot types
Low	Ability to log huge amounts of attack data. No simulation needed for the actual OS used for interaction	Time-consuming . The highest probability of risk. Complex [70]	Honeynet [71]
Medium	Offer better. Simulated services. More difficult for attackers to identify [72]	Increasing subject to the security vulnerability Longer time for implementation and expertise required [73]	Kippo [74]
High	Easy to install and price effective. Low risk. Require little to no expertise [75]	Require to have a complete set of features Give limited information about the specific attacks [76].	Honeyd [77]

Honeypot is a program designed for cybersecurity to defend against virus attacks. Attackers are attracted by the exploits contained in the honey software to extract data from the network of an organization with the intention of causing malice. Frank Cohen was the designer of the first honeypot known as The Deception Toolkit. It was used to effectively against the automated attacks on a system. With a variety of vulnerabilities as a form of deception, attackers are lured to the system. This deception toolkit has an important feature to create alert for the administrator against the deceptions, given that information used to hack into the system was often under a particular service like sending an e-mail [64]. The invention of honeypot created a breakthrough in the field of security networks and computers. Due to this, honeypots have been widely used in the year of 2000s. Meanwhile, some computer programs. It can self-replicate were spread rapidly within the Internet network, causing an outbreak of worms. The spread of such computer worms poses a danger to network traffic and thus, increases the latency of the whole network. The idea of capturing these worms for analysis was not considered. Instead, the optimal solution to collect these worms was by trapping them into a honeypot [65].

A variety of honeypot solutions has been used within the organization or applied to specific industries and services. It was found that honeypots are categorized into two main dimensions: level of interaction with attackers and service provision, as shown in Table II. Analysis requires a variety of data to be collected, requiring a higher level of interaction, with reference to the research conducted by Ronald and Keshnee [66].

Some applications of honeypots in distinct research fields were studied. A good example of this is the design of a system called “Sweetbait”, using the honeypot approach for capturing fast worms with the purpose of automated analysis and signature generation. Continuous updates of signatures were sent to both network and host-based IDS/IPS all over the parts of the Internet [67].

Machine learning as an alternative solution to the conventional detection methods using in smart factories currently. So far, smart manufacturing has been using rule-based intrusion detection methods that use signal DB or SNORT to analyze security data. The detection method is mainly based on anomaly-based detection. It determines normal and abnormal conditions compared with normal network conditions.

This makes it difficult to respond quickly to unknown attacks or attacks on manufacturing IoT using a botnet. There is a hassle to manually set the rule for attack patterns. And it often results in poor efficiency of security personnel input. In addition, the rule-based methods, based on expert knowledge, have difficulties in flexibly responding to changes in the external attacks and maintain consistency in high detection performance. This is because such rule-based detection makes it impossible to detect intrusions outside of pre-designed rules and it can vary the quality of the rules depending on the experts and system environment. Therefore, research related to the development of the detection model using machine learning has recently been attempted to overcome the shortcomings of the rule-based detection methodology. Indeed, machine learning (ML) is a procedure that teaches computers or devices to perform automatic processes. Network machine learning will learn from the network environment for a period of time. In addition, ML is based on mathematical modeling. Thus, it is better than signature-based and rule-based detection methods, so it will be able to cope with the continuously advanced and sophisticated attacks [68][69].

D. Critical Literature Review

Taxonomies of the botnet detection and smart factories IoT security are illustrated in Fig. 6 and 7. Table IV gives a summary of the selected papers used in these reviewed papers. These studies were conducted with the effort to detect botnet, the honeypot approach to detect botnets and narrowly focused on botnet detection using honeypot for smart factories. They are then grouped in Fig. 8, 9 and 10 accordingly.

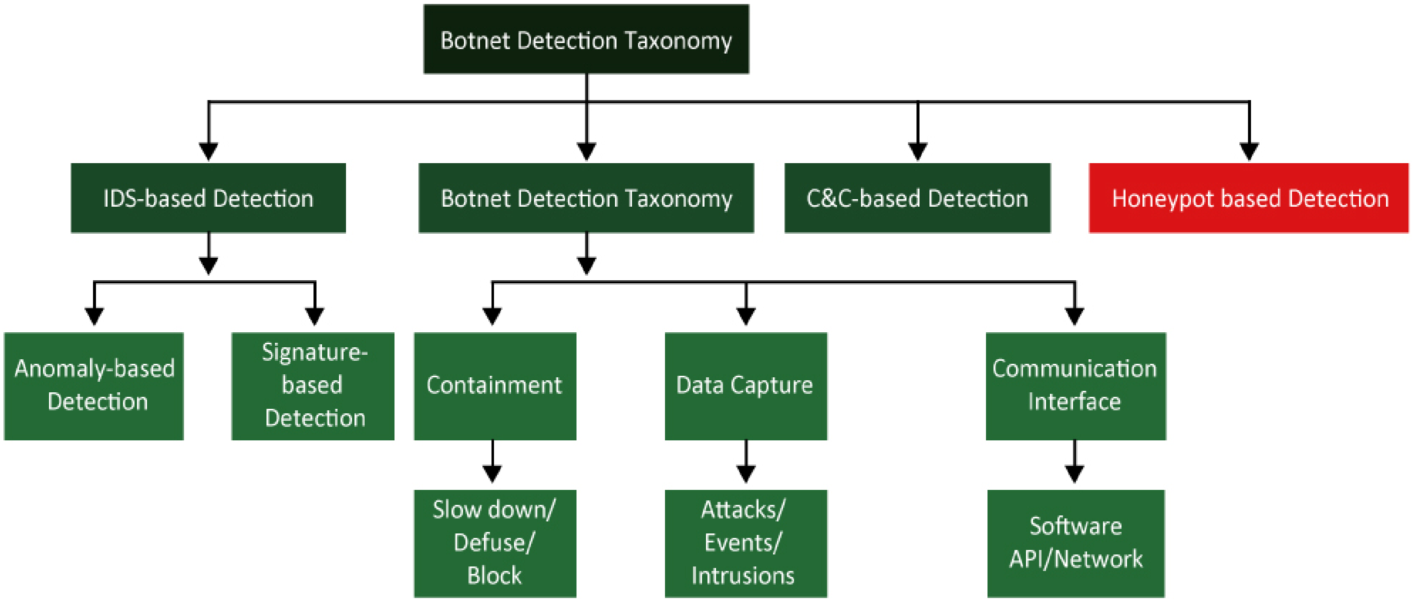

Fig. 6. Botnet Detection Taxonomy.

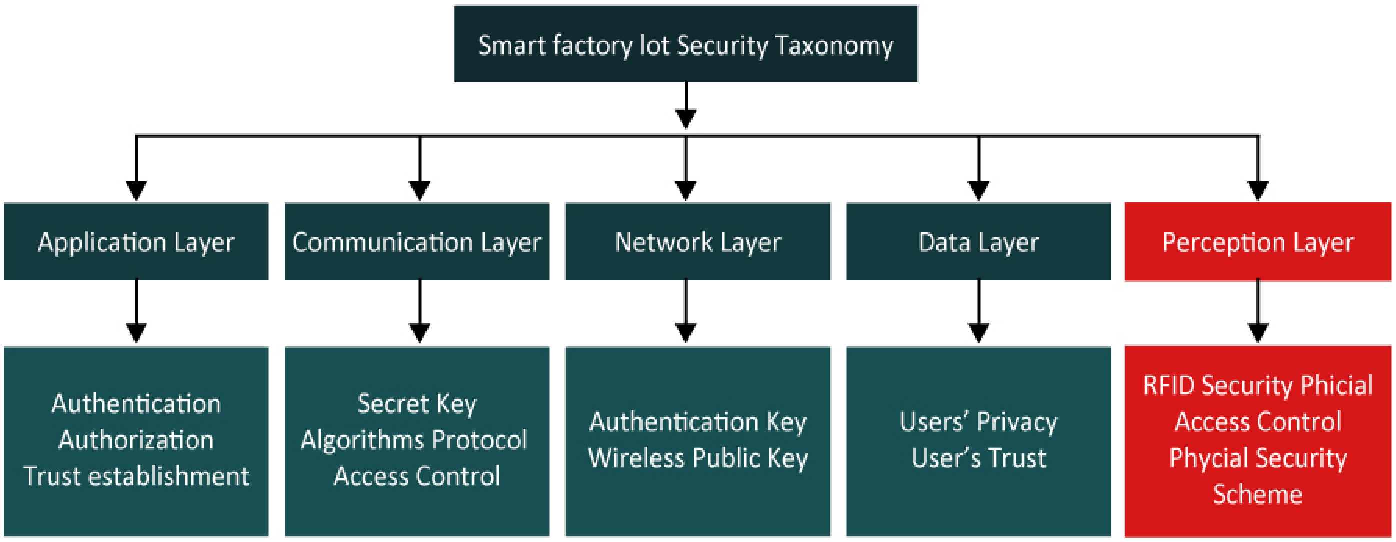
Smart factory Iot Security Taxonomy
Application Layer
Communication Layer
Network Layer
Data Layer
Perception Layer
Authentication Authorization Trust establishment
Secret Key Algorithms Protocol Access Control
Authentication Key Wireless Public Key
Users' Privacy User's Trust
RFID Security Phicial Access Control Phycial Security Scheme

Fig. 7. Smart Factory IoT Security Taxonomy.

This section provides a review of the literature related to work conducted by the researcher in smart factories detection and machine learning areas. The task scheduling algorithm is detailed in the two taxonomies to clearly understand and classify the basic approaches currently in use. Recently, there has been a significant increase in Botnet threats. In particular, it can be seen that botnet's attack on IoT platform has increased dramatically. Table III summarizes some important studies in using the Honeypot approach for detecting botnet in smart factories. A study in IoT botnet detection suggested that it is easy to monitor, if the IoT devices are infected through web services [79]. Some restrictions have pointed out that monitoring algorithms for IoT devices are simple to implement and it is scalable enough for smart factories using IoT equipment [79]. The capacity for the IoT devices has clear limits. This approach was first designed with a hypothesis that botnet contacts IoT devices were used to invent a detection model based on the binary. The botnet detection uses a machine learning approach that shows high accuracy of 99.94%. The combination of flow-based with graph-based detection and machine warning has a high accuracy of detecting a botnet attack as an advantage. The disadvantage of this approach is that it is harder to detect quickly in the randomized number of packets. Thus, the appropriation of applying this approach for smart manufacturing needs more research in real-time and it is time-consuming [80].

TABLE IV. A COMPARATIVE SUMMARY OF STUDIES IN BOTNET DETECTION FOR SMART FACTORIES USING THE HONEYPOT APPROACH

Ref.	Approaches	Strengths	Weaknesses	Research gap
[78]	Smart factory detection using machine learning	Cost reduction	Low detection rate, high complexity and uncertainty	Intrusion detection systems deployed in this study are implemented by deep neural networks, requiring intrusion detection systems through convolutional neural network, recurrent neural network, deep brief network and deep q-networks applied to various systems in this study.
[79]	Botnet , IoT botnet	Web service is available for easy monitoring of IoT device health and is useful for smart factories with many IoT devices.	Limited capacity.	Develop a strategy to simplify and optimize the binaries that implement this security technology to broaden the application of the results in this study.
[80]	Botnet detection using Machine learning	It shows the effect of bookmarks. Hybrid analysis of flow-based and graph-based traffic behavior achieves 99.94% detection accuracy, surpassing individual detectors	Randomly specify the number of bytes per packet and the number of packets per flow so that they are not detected.so flow-based detectors are not easy to apply quickly.	Improved detection results show new botnet detection through effective graph-based features and botmark effects.
[80]	Detection using IoT Honey pot	The speed of information gathering is rapid. Because it implements only part of the system, it consumes fewer resources.	Unnecessary data piles up	To support high protocols, the company plans to expand the IoT and expand sandboxes with features that can further activate the architecture and environment commonly used in IoT devices.
[68]	Detection using Honey pot Machine learning	It has developed a honeypot-based solution for botnet detection using a machine-learning detection framework. The use of honeypot ensures logging of newly released malware functions.	The function varies greatly depending on the difference in the system performance.	The honeypot approach should be expanded. Cloud servers should also be employed to handle IoT devices with minimal resources.

For smart factories, botnet detection using honeypot integrated with IoT (IoT honeypot) was studied [81]. There is a stochastic basis compared to the machine learning approach with superstitious running. Although the IoT honeypot has stopped scalability by simply applying it to sandboxes IoT, it aims to apply for common expansion in more situations and environments [14.] In the detection system using honey pot machine botnet, the learning logging for detection and tracking are so accurate. The system, in accordance with the system different but most standard equipment, is suitable for performance smart factories. Hence, it is likely to be adopted in the future. The cloud server approach uses the proposal [68]. As for IDS used by the smart factory, although the machine learning approach can reduce costs, significant imperfections such as low detection rates, highly complex and unsustainable systems were observed [78]. Three studies in IDS, IoT botnet and honeypot machine learning showed some application results for smart factories. Such solutions are possible to trace through logging at low cost and are most cost-saving for the IoT devices. Thus, botnet detection for smart factories using machine learning based on honey pot detection needs more in-depth research.

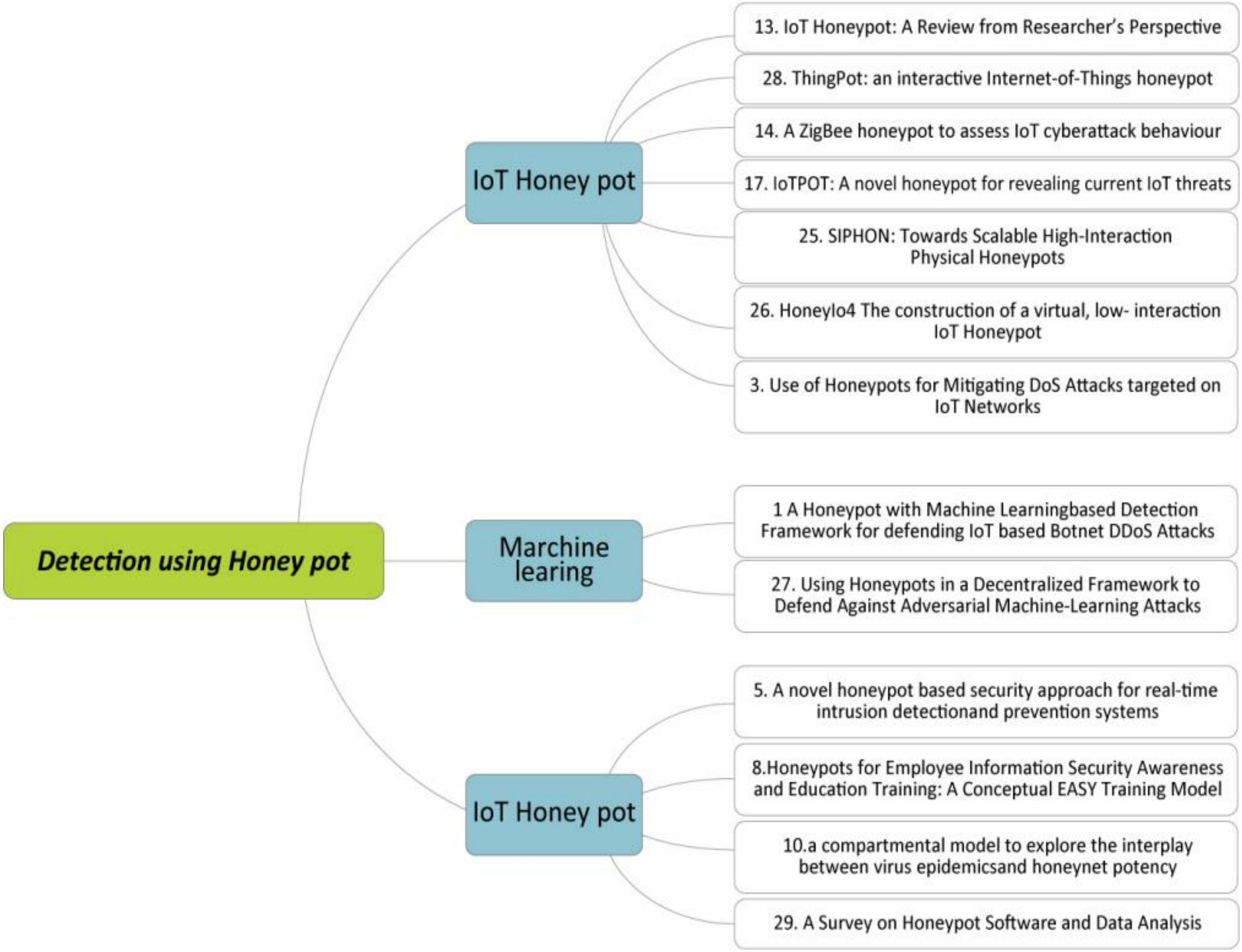
Detection using Honey pot
IoT Honey pot
13. IoT Honeypot: A Review from Researcher's Perspective
28. ThingPot: an interactive Internet-of-Things honeypot
14. A ZigBee honeypot to assess IoT cyberattack behaviour
17. IoTPOT: A novel honeypot for revealing current IoT threats
25. SIPHON: Towards Scalable High-Interaction Physical Honeypots
26. HoneyIo4 The construction of a virtual, low- interaction IoT Honeypot
3. Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks
Marchine learing
1 A Honeypot with Machine Learningbased Detection Framework for defending IoT based Botnet DDoS Attacks
27. Using Honeypots in a Decentralized Framework to Defend Against Adversarial Machine-Learning Attacks
IoT Honey pot
5. A novel honeypot based security approach for real-time intrusion detectionand prevention systems
8.Honeypots for Employee Information Security Awareness and Education Training: A Conceptual EASY Training Model
10.a compartmental model to explore the interplay between virus epidemicsand honeynet potency
29. A Survey on Honeypot Software and Data Analysis

Fig. 8. Grouping of Honey Pot based Botnet Detection Model for Smart Factory (A).

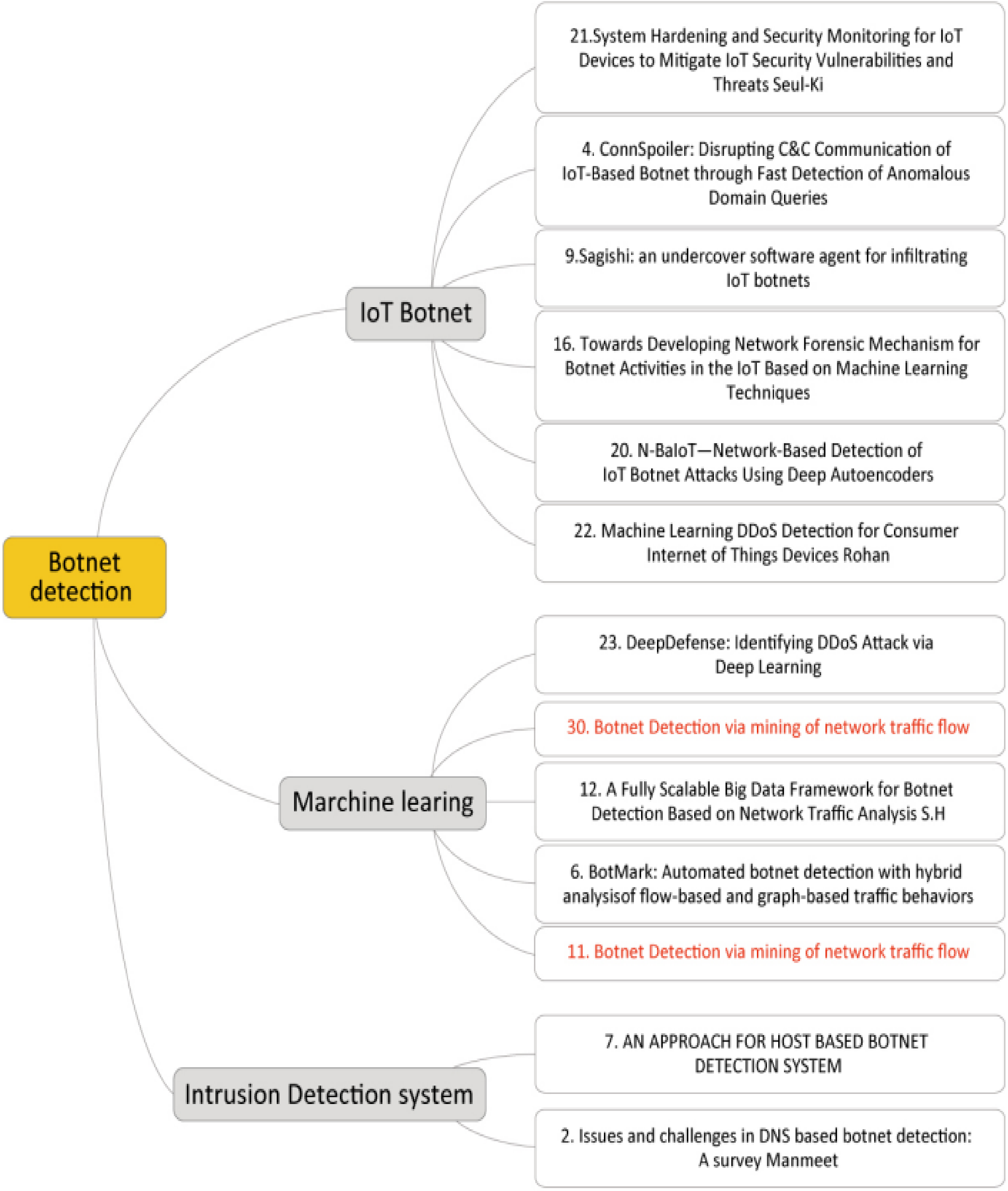
Botnet detection
IoT Botnet
21.System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats Seul-Ki
4. ConnSpoiler: Disrupting C&C Communication of IoT-Based Botnet through Fast Detection of Anomalous Domain Queries
9.Sagishi: an undercover software agent for infiltrating IoT botnets
16. Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques
20. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders
22. Machine Learning DDoS Detection for Consumer Internet of Things Devices Rohan
Marchine learing
23. DeepDefense: Identifying DDoS Attack via Deep Learning
30. Botnet Detection via mining of network traffic flow
12. A Fully Scalable Big Data Framework for Botnet Detection Based on Network Traffic Analysis S.H
6. BotMark: Automated botnet detection with hybrid analysisof flow-based and graph-based traffic behaviors
11. Botnet Detection via mining of network traffic flow
Intrusion Detection system
7. AN APPROACH FOR HOST BASED BOTNET DETECTION SYSTEM
2. Issues and challenges in DNS based botnet detection: A survey Manmeet

Fig. 9. Grouping of Honey Pot based Botnet Detection Model for Smart Factory (B).

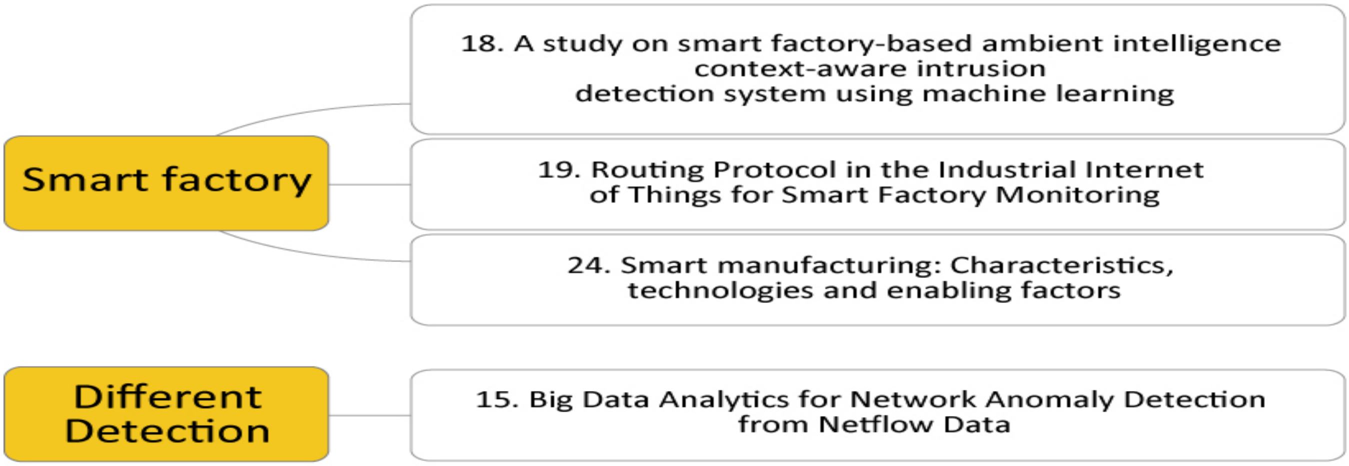
Smart factory
18. A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning
19. Routing Protocol in the Industrial Internet of Things for Smart Factory Monitoring
24. Smart manufacturing: Characteristics, technologies and enabling factors
Different Detection
15. Big Data Analytics for Network Anomaly Detection from Netflow Data

Fig. 10. Grouping of Honey Pot based Botnet Detection Model for Smart Factory (C).

TABLE V. SUMMARY OF LITERATURE REVIEWED

No	Contribution	Research gap
[68]	. It has developed a honeypot-based DDoS detection solution that utilizes a real-time machine learning detection framework. Using beehives can ensure logging of newly released malware functions that can be utilized as ML-based detection.	IoT honeypot structure is heterogeneous because IoT device types are different. But the original Honeypot structure is similar. So there is a big difference between traditional honey and IoT honeypot
[82]	Propose an in-depth category for DNS techniques within a category.	While various papers talk about DNS-based botnet detection, each detection technique does not provide efficient classification and does not think about parameters.
[83]	Implemented in real-time environments with a variety of microcontrollers that interface with central servers. The idea of deploying a honeypot to handle DoS attacks can also be extended by deploying a honeypot system that can handle DDoS attacks using botnets.	Suggest a Honeypot Model to Mitigate DoS Attacks Started with IoT Devices
[84]	This paper provides a lightweight sensing system. NXDomain's ConSpoiler Works in Nuclear IoT-based botnets in response mode, NXDomain's compiler works the weeks. Also, on a DNS train collected from two other large ISP networks, Conspoiler can have this peculiarity that computers have been developed by the city.	Information gathered from ISP networks requires an identifiable assessment of devices infected with botnets.
[85]	The system developed is a type of honeypot-based IDPS that allows real-time animation of server network traffic. Zero-day attacks can be detected more effectively than other IDS. And you can save resources by reducing the amount of data on IDS.	A good hybrid honey pot is reminiscent of high interaction and low interaction. Perform Honeypot. To effectively analyze data in real-time, The developed Honeypot server application works by combining with IDS.
[80]	A variety of experiments outstrip flow-based or graph-based detection by achieving 99.94% accuracy.	A combination of flow-based network traffic behavior and graph-based and network traffic behavior for botnet detection suggests an automatic model of botmark. Network anomalies detect and detect botnets through flow-based traffic analysis using optical communication patterns in traditional methods. However, simple flow-based traffic analysis and graph-based analysis increasingly increase the failure rate due to the evolution and precision of botnet attacks.
[86]	The system host interface is used as an aberrant detection technique by analyzing the traffic of genetic algorithm variation. The experimental results analyze each algorithm and show that it is relevant. Future work provides additional detection techniques as an extension of system functions. Anomaly signature-based techniques such as the addition of data integrity analysis are integrated to enable rapid delivery.	The host-based chip-in-detection system approach is based on the modification of the algorithm It can be used in the event of an attack. Based on the approach of anomaly detection. The cause of the current system's malicious code is the use of bots. This approach analyses the cause of botnet attacks.
[74]	By placing Honey pot in a company or institution in the future, employees are aware of the importance of security awareness and increase the risk of detection by increasing the security culture within the organization.	Analyze the honeypot data to analyze how employee information security awareness and systems can be utilized by reviewing cybercriminals (including vendors and malicious insiders).
[87]	In this work, the concept of active honeypots was introduced to	Mapping and classifying boats that form part of the existing IoT botnet

	mimic real bots so that information can be leaked, usually only to infect machines. It also described how active honeypots are integrated into the proposed software architecture that allows users to receive malware samples and extract botnet functions for the purpose of penetrating botnets.	and how it spreads through the Internet are difficult. Forensic had previously sought to solve the problem by installing, reporting and securing remote IoT devices that had been changed to boats. The activity was based on honey pot, which can only “detect” the Internet to guide and classify the IoT bot according to its behaviour.
[71]	Here are some ideas for improving the design of honeynet and for the constitution of the spread of the virus. Because the honeynet has a low power index, it is easy to obtain virus samples and it is easy to provide a number of numerical examples for theoretical analysis.	Within a systematic framework, honeynet’s potency was not evaluated theoretically.
[88]	The existing detection system shows limits in preventing botnet attacks on IoT. Because botnet keeps evolving, but the study shows that ML technology has advanced in detecting specific threats to IoT networks.	One method of detection is botnet processing power, amount of energy consumption, IoT environment requirements, etc. Often it does not meet the potential to address security threats. So the IoT network and Ddos attacks botnet often cause major security problems.
[89]	Extensible botnet detection methods can be integrated by providing computing infrastructure for building big data frameworks using crowd service providers in large networks. In addition, skilled human resources include the cost of ownership because they build a framework	The scalability problems of botnet detection systems arise from a variety of problems, such as bottlenecks in the detection process, storage, data collection and analysis.
[67]	The design of IoT honeypots can be expanded to provide intelligent responses based on interaction in the combination of login/passwords, distribution of attacks, types of devices being attacked and IP addresses by country of distribution. It can be used as an additional review of IoT honeypots for IoT devices.	Implementing a strong security mechanism leaves little room for security implementation of IoT devices and limited hardware functions, making it very difficult to implement.
[81]	Zigby is one of the wireless technologies used for IoT. Large global malware uses SSH as an entry point to continue pre- and violent attacks. Therefore, deploying this Honeypot in SSH to collect large data sets to identify awareness and interest in the ZigBee network makes it easy to collect and recognize automated attack types.	There is a lot of inconvenience by limiting attack statistics to the physical scope of zigbee communications to collect cyber attackers’ paddles.
[40]	The accuracy of high anomaly detection should provide high-quality service and communication, even as the complexity of the attack and analysis processes increases. Anomaly attacks and singularities are naturally rare. Propose innovative algorithms achieved in future studies with more data and anomalies.	Big Data Anomalies Detection Security is key to continuing and long-term cyber-attacks. With constant changes in the distribution of network data, detection becomes more difficult
[90]	In DT, ANN, NB and AN machines, the machine learning technique proved to be superior to other techniques in false alarm rate and accuracy, showing excellent ability in identifying and investigating botnet without errors.	To used ML techniques to investigate botnet activity and apply detection to bonnet attacks, but there were many problems and high false alarm rates to make perfect detection. So I found that there are many problems in training and verification research of the detection model of ML technique.
[91]	Five malign program families were identified, all of which are actively used in DDoS attacks.	The botnet has done a lot of damage to devices powered by Microsoft and Sony’s IoT through spam e-mails and we learned that the main target point of the attack came from IoT devices. IoTPop analyses the samples of malware captured by honeypots and analyses them on Telnet-based This research proposes this method because it will be easy to track and analyze attacks.
[78]	Machine learning-based intrusion detection systems have reduced the frequency of incorrect replacement of existing devices, resulting in significant savings. It showed 33% to 1.33% process performance and 29% to 1.29% abnormalities but showed an effective scoring architecture.	In a smart manufacturing environment, real-time detection is important enough to have a significant impact. But there is a limit to real-time detection. The efficiency of IoT development and application should be increased within smart manufacturing.
[92]	This paper aimed at proposing and analysing the efficient framework of industrial IoT and providing the latest approach to industrial applications. This paper also dealt with the adoption of Laura.	Industrial IoT requires more thorough security to prevent data leakage, transmission errors and data injection due to communication between hundreds of devices. Access should also be naturally controlled by IoT devices. Real-time industrial IoT device security needs to be monitored.
[93]	While the IoT device, part of the botnet, was launched in a damaged state, it demonstrated the ability to detect the exact and immediate manner of attack that we proposed.	A new network-based abnormality detection method called IoT N-BaIoT, which detects abnormal network traffic by taking snapshots of network operations using deep automatic encoders from damaged IoT devices, is needed. This is because the number of IoT-based botnet attacks should be rapidly increasing and the threat of botnet attacks should be mitigated by detecting IoT-based attacks that last for hours and milliseconds.
[94]	The proposed technique is expected to be useful in managing	The weak aspects of IoT device security through real-time security

	numerous IoT devices such as the smart factory. The IoT market is rapidly changing and IoT devices are widely adopted in various fields. It suggested a system and operation method. It can easily apply security functions to IoT devices. This study further validated the usefulness of the proposed technique by developing a prototype.	monitoring In order to minimize the threat of attack, there is a threat of secondary attacks or malware attacks on damaged IoT devices. So I propose to build various security functions and strengthen the system.
[7]	The network traffic pattern of IoT devices classifies Ddos detection general and Ddos attack traffic, thus using a limited set of functions that are important for real-time intermediate box layout. So the study of machine learning at the packet level shows that it depends on the hypothesis.	To remain limited due to memory constraints in IoT devices, caching adds to the delay time and complexity. Therefore, the optimal algorithm should store flow information only for a short period.
[95]	Reducing the error rate from 7.517% to 2.103%, the in-depth learning approach was automatically extracted from the high level of characteristics and then patterned from the sequence of network traffic, making it easier to track network attacks. It has shown enough that the new model is superior to the existing one.	Traditional detection solutions have failed to defend against fatal threats and have shown limitations in monitoring network traffic based on statistical variances against rapidly growing DDoS attacks. However, if performance identification based on machine learning is improved, there is also a potential for the development of statistical characteristics.
[4]	Smart manufacturing ontology feature that can be used to provide a platform for active technology and factors identified, discussions and clusters. Overall, situational awareness, modularity, bilateral, inter-operability and configuration of five characteristics are considered.	Intelligent manufacturing, many items that appear to be indistinct redundancy to smart factories, one of the most advanced manufacturing, need to be established as a foundation for manufacturing ontology.
[96]	Potential weaknesses in IoT devices and Internet attacks have always been threats to IoT equipment. SIPHON can expose IoT devices to the Internet to enable clear monitoring of test beds and enhance honeypot's reality. The limitations of simple security test mechanisms can be overcome.	An inefficient way for an attacker to move benefits before solving the vulnerability problem of finding vulnerabilities in IoT devices. In traditional IT security, we understood accounts that were critical to the dynamic threat environment without hacking and potentially conducted honeypot attempts to establish unauthorized connections. There were attacks in realistic ways, such as log-in shellfish.
[97]	It detects Honeypot with IoT devices and provides detailed information to attackers. HoneyIo4 can run on both CLI and GUI and for both experienced and inexperienced users. Although its initial performance is limited, it succeeded in detecting IoT OS. Honey can be improved by adding more features to this basic core.	Honeypot usually deceives the system in a limited way. They also have less risk to the network if the honeypot is damaged, but the information collected for attackers or attackers is also very limited. Preventive, detection and response mechanisms should be provided to facilitate maintenance and protection on the organization's network.
[98]	A decentralized defense framework that prevents opponents from degrading the learning model, suggesting a network of high-interaction honeypots (HIHP). To achieve a goal by preventing an attacker from learning the label correctly and by approximating the structure of a black box system. Attracting attackers, using adobe honey to generate calculations that are not feasible for the enemy, for the Decoy model and for the enemy.	Limited access to input and output labels of data can be used to confuse input learning. However, the market is increasingly in demand for machine learning services. Naturally, there is a possibility of exposure to a variety of complaints by increasing threats.
[[99]	The IoT platform and device attackers are caught. In particular, five types of attacks have been discovered.	IoT device signals clearly sent to IoT for the exploitation of security vulnerability by those who want it. So it may be possible to secure IoT, but it is important to identify an attack strategy.
[100]	Honey pot that analyses the data methodology, the ethical and legal issues are discussed.	The survey provides a broad overview of honeybees. This includes not only honeypot software but also methodologies for analyzing honeypot data.
[101]	Apply deep learning optimization to handle the high false cost of the algorithm, integrating high-level new detection model. So by classifying random filters, effectively achieve botnet defense.	Many researchers have many botnet detection models in the past, but most of them have not found botnets these days with both high probability and good memory and time efficiency.

Table IV elaborated literature review critically to the botnet issues with smart factories, and other related domains. This issue equally impedes to the smart homes as well [102]. In addition, studies elaborated that the phishing works and supports for botnet attacks [103]. Further, these botnet attacks help to the attacker by providing them ground, where they can launch different attacks and make possible intrusion of the network [104], and later these attacks could help the criminals [105-106] for their different activities.

III. Conclusion

Throughout this review of literature, the field of IoT-based smart factory using honeypot approach to detect botnet is a potential area for the research to explore. Conventionally, smart factories have been using three methods i.e. signature-based, rule-based and anomaly-based for detection.

However, these conventional methods were recognized to have a limitation in the responding time which is desired to be quicker in detection. It took a long time to detect the botnet, exposing the vulnerability of smart factory. Honeypot is an approach that has been examined for its effectiveness to trap botnet in some studies. The honeypot approach can overcome the limitation of the conventional methods in terms of quick detection, while the botnet is easy to spread in the IoT based environment.

So far, there is a scarcity of studies in applying the honeypot approach for botnet detection designed for smart factories. However, this paper suggests the possibility. If honeypot botnet detection is applied in Smart factory IoT environment, it can improve the productivity of Smart factory and fasten the production time.

IV. Future Work

Future research should look into developing honeypot models and algorithms that can be applied in smart factory IoT environment. And if the failure rate and detection time can be reduced through the metadata score, the model performance will be improved dramatically.

Acknowledgment

I would like to thank my supervisors, Associate Prof. Dr Azween Abdullah & Dr. Noor Zaman Jhanjhi, for their patient guidance, encouragement and continuous support provided throughout my postgraduate studies. I have been extremely fortunate to have supervisors, who cared so much about my work, and professional growth.

References

[1] L. Barreto, A. Amaral, and T. Pereira, “Industry 4.0 implications in logistics: an overview,” Procedia Manuf., vol. 13, pp. 1245–1252, 2017.

[2] B. Huang, W. Wang, S. Ren, R. Y. Zhong, and J. Jiang, “A proactive task dispatching method based on future bottleneck prediction for the smart factory,” Int. J. Comput. Integr. Manuf., vol. 32, no. 3, pp. 278–293, 2019.

[3] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, “Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges,” Mech. Syst. Signal Process., vol. 135, p. 106382, 2020.

[4] S. Mittal, M. A. Khan, D. Romero, and T. Wuest, “Smart manufacturing: Characteristics, technologies and enabling factors,” Proc. Inst. Mech. Eng. Part B J. Eng. Manuf., vol. 233, no. 5, pp. 1342–1361, 2019.

[5] R. A. Rojas and E. Rauch, “From a literature review to a conceptual framework of enablers for smart manufacturing control,” Int. J. Adv. Manuf. Technol., vol. 104, no. 1–4, pp. 517–533, 2019.

[6] M. S. Smith, “Protecting Privacy in an IoT-Connected World.,” Inf. Manag. J., vol. 49, no. 6, pp. 36–39, 2015.

[7] R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer internet of things devices,” Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018, no. Ml, pp. 29–35, 2018.

[8] A. D. Manyika James, Chui Michael, Bisson Peter, Woetzel Jonathan, Dobbs Richard, Bughin Jacques, “Unlocking the potential of the Internet of Things | McKinsey &amp; Company,” McKinsey, pp. 1–4, 2015.

[9] E. (TOPICAL C. Casalinuovo, “Thematic Investment Opportunity – Internet of Things,” no. March, pp. 3–6, 2019.

[10] M. Ozcelik, N. Chalabianloo, and G. Gur, “Software-Defined Edge Defense Against IoT-Based DDoS,” IEEE CIT 2017 - 17th IEEE Int. Conf. Comput. Inf. Technol., pp. 308–313, 2017.

[11] M. A. Rajab, “My Botnet is Bigger than Yours (Maybe, Better than Yours) : why size estimates remain challenging,” HotBots’07 Proc. first Conf. First Work. Hot Top. Underst. Botnets, no. USENIX Association Berkeley, CA, USA ©2007, pp. 5–5, 2007.

[12] N. Tuptuk and S. Hailes, “Security of smart manufacturing systems,” J. Manuf. Syst., vol. 47, no. November 2017, pp. 93–106, 2018.

[13] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas, “DDoS in the IoT: Mirai and Other Botnets,” Computer (Long. Beach. Calif)., p. 79, 2017.

[14] J. Wan et al., “Software-Defined Industrial Internet of Things in the Context of Industry 4 . 0,” vol. 16, no. 20, pp. 7373–7380, 2016.

[15] N. E. Vaskenly and M. Dhanya, “Smart factories: An Indian scenario,” Int. J. Pure Appl. Math., vol. 118, no. Special Issue 9, pp. 505–509, 2018.

[16] F. Galati and B. Bigliardi, “Computers in Industry Industry 4 . 0 : Emerging themes and future research avenues using a text mining approach,” Comput. Ind., vol. 109, pp. 100–113, 2019.

[17] Z. Zhang, Y. Zhang, J. Lu, X. Xu, F. Gao, and G. Xiao, “CMfgIA : a cloud manufacturing application mode for industry alliance,” 2018.

[18] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, “Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges,” IEEE Access, vol. 6, no. c, pp. 6505–6519, 2017.

[19] X. Li, D. Li, J. Wan, C. Liu, and M. Imran, “Adaptive Transmission Optimization in SDN-Based Industrial Internet of Things With Edge Computing,” vol. 5, no. 3, pp. 1351–1360, 2018.

[20] M. Ghobakhloo, “The future of manufacturing industry: a strategic roadmap toward Industry 4.0,” J. Manuf. Technol. Manag., vol. 29, no. 6, pp. 910–936, 2018.

[21] M. Salhaoui, A. Guerrero-González, M. Arioua, F. J. Ortiz, A. El Oualkadi, and C. L. Torregrosa, “Smart industrial iot monitoring and control system based on UAV and cloud computing applied to a concrete plant,” Sensors (Switzerland), vol. 19, no. 15, 2019.

[22] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, “Review on cyber-physical systems,” IEEE/CAA J. Autom. Sin., vol. 4, no. 1, pp. 27–40, 2017.

[23] J. Bourgeois et al., “Programmable matter as a cyber-physical conjugation,” 2016 IEEE Int. Conf. Syst. Man, Cybern. SMC 2016 - Conf. Proc., pp. 2942–2947, 2017.

[24] A. Valente, S. Baraldo, and E. Carpanzano, “Smooth trajectory generation for industrial robots performing high precision assembly processes,” CIRP Ann. - Manuf. Technol., vol. 66, no. 1, pp. 17–20, 2017.

[25] Nguyen, “Study on realtime control system in IoT based smart factory Interference awareness, architectural elements, and its application,” pp. 1–4, 2017.

[26] J. Feng, F. Li, C. Xu, and R. Y. Zhong, “Data-Driven Analysis for RFID-Enabled Smart Factory : A Case Study,” IEEE Trans. Syst. Man, Cybern. Syst., vol. PP, pp. 1–8, 2018.

[27] S. Lu, C. Xu, R. Y. Zhong, and L. Wang, “A RFID-enabled positioning system in automated guided vehicle for smart factories,” J. Manuf. Syst., vol. 44, pp. 179–190, 2017.

[28] B. Hameed, F. Rashid, F. Dürr, and K. Rothermel, “Self-calibration of RFID reader probabilities in a smart real-time factory,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7319 LNCS, pp. 253–270, 2012.

[29] L. Shen, Q. Zhang, J. Pang, H. Xu, and P. Li, “PRDL: Relative Localization Method of RFID Tags via Phase and RSSI Based on Deep Learning,” IEEE Access, vol. 7, pp. 20249–20261, 2019.

[30] K. H. Wang, C. M. Chen, W. Fang, and T. Y. Wu, “On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags,” J. Supercomput., vol. 74, no. 1, pp. 65–70, 2018.

[31] S. U. Rehman, R. Liu, H. Zhang, G. Liang, Y. Fu, and A. Qayoom, “Localization of moving objects based on RFID tag array and laser ranging information,” Electron., vol. 8, no. 8, 2019.

[32] J. M. Ceron, K. Steding-Jessen, C. Hoepers, L. Z. Granville, and C. B. Margi, “Improving iot botnet investigation using an adaptive network layer,” Sensors (Switzerland), vol. 19, no. 3, pp. 1–16, 2019.

[33] S. Maeda, A. Kanai, S. Tanimoto, T. Hatashima, and K. Ohkubo, “A Botnet Detection Method on SDN using Deep Learning,” 2019 IEEE Int. Conf. Consum. Electron. ICCE 2019, pp. 1–6, 2019.

[34] S. Baruah, “Botnet Detection : Analysis of Various Techniques Sangita Baruah a,” Int. J. Comput. Intell. IoT Proc., vol. 2, no. 2, pp. 461–467, 2019.

[35] C. V. F. Jr, “Mirai Bot Scanner Summation Prototype,” 2019.

[36] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, “An In-Depth Analysis of the Mirai Botnet,” Proc. - 2017 Int. Conf. Softw. Secur. Assur. ICSSA 2017, pp. 6–12, 2018.

[37] F. F. Giordani, “Consiglio nazionale delle ricerche,” How long does it Tak. before a new Internet node is contacted very first time?, vol. 3, no. 6, p. 413, 2018.

[38] H. Nguyen, Q. Ngo, D. Nguyen, and V. Le, “PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms Huy-Trung,” ICT Express, 2020.

[39] A. Mathematics, “DETECTION AND ERADICATION OF BOTNETS IN ONLINE BANKING,” vol. 116, no. 10, pp. 73–77, 2017.

[40] C. H. Yeung, “Big Data Analytics for Network Anomaly Detection from Netflow Data Duygu,” Int. J. Androl., 2017.

[41] R. S. and A. Thakral, A Review of Various Mechanisms for Botnets Detection. Springer, Singapore, 2018.

[42] S. Mulik and A. Patil, “Botnet Detection using Traffic Analysis and Defenses,” vol. 6, no. 2, pp. 108–115, 2019.

[43] A. Aziz, “A soft-decision fusion approach for multiple-sensor distributed binary detection systems,” IEEE Trans. Aerosp. Electron. Syst., vol. 47, no. 3, pp. 2208–2216, 2011.

[44] F. Gerstmayer, J. Hausladen, M. Kramer, and M. Horauer, “Binary protection framework for embedded systems,” 2017 12th IEEE Int. Symp. Ind. Embed. Syst. SIES 2017 - Proc., 2017.

[45] J. Zhen and Z. Liu, “New honeypot system and its application in security of employment network,” Proc. - 2012 IEEE Symp. Robot. Appl. ISRA 2012, pp. 627–629, 2012.

[46] A. Pauna, I. Bica, F. Pop, and A. Castiglione, “On the rewards of self-adaptive IoT honeypots,” Ann. des Telecommun. Telecommun., vol. 74, no. 7–8, pp. 501–515, 2019.

[47] R. K. S. authorBazila B. Hota, Attack Detection and Forensics Using Honeypot in IoT Environment Rajesh, vol. 2, no. Dec. Springer International Publishing, 2018.

[48] A. Amjad, A. Griffiths, and M. Patwary, “QoI-Aware Unified Framework for Node Classification and Self-Reconfiguration Within Heterogeneous Visual Sensor Networks,” IEEE Access, vol. 4, pp. 9027–9042, 2016.

[49] M. Wang, “Understanding Security Flaws of IoT Protocols through Honeypot Technologies,” J. Opt. Soc. Am., 2017.

[50] D. Ramirez, J. I. Uribe, L. Francaviglia, P. Romero-Gomez, A. Fontcuberta i Morral, and F. Jaramillo, “IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices,” J. Mater. Chem. C, vol. 6, no. 23, pp. 6216–6221, 2017.

[51] E. Pricop, J. Fattahi, N. Dutta, and M. Ibrahim, Recent Developments on Industrial Control Systems Resilience. 2020.

[52] H. Sharma and K. Govindan, Advances in Computing and Intelligent Systems. 2019.

[53] A. Umamaheswari and B. Kalaavathi, “Honeypot TB-IDS: trace back model based intrusion detection system using knowledge based honeypot construction model,” Cluster Comput., vol. 4, pp. 1–8, 2018.

[54] H. Hadeli, R. Schierholz, M. Braendle, and C. Tuduce, “Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration,” ETFA 2009 - 2009 IEEE Conf. Emerg. Technol. Fact. Autom., pp. 1–8, 2009.

[55] N. C. Rowe, “Honeypot Deception Tactics,” Auton. Cyber Decept., pp. 35–45, 2019.

[56] A. Noaman, A. Abdel-Hamid, and K. Eskaf, “A novel honeynet architecture using software agents,” 2019 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2019, pp. 1–6, 2019.

[57] P. Duessel, C. Gehl, U. Flegel, S. Dietrich, and M. Meier, “Detecting zero-day attacks using context-aware anomaly detection at the application-layer,” Int. J. Inf. Secur., vol. 16, no. 5, pp. 475–490, 2017.

[58] G. Fedynyshyn, M. C. Chuah, and G. Tan, “Detection and classification of different botnet C&C channels,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6906 LNCS, pp. 228–242, 2011.

[59] S. Morishita et al., “Detect me if you... Oh wait. An internet-wide view of self-revealing honeypots,” 2019 IFIP/IEEE Symp. Integr. Netw. Serv. Manag. IM 2019, no. 1, pp. 134–143, 2019.

[60] C. Dalamagkas et al., “A Survey on honeypots, honeynets and their applications on smart grid,” Proc. 2019 IEEE Conf. Netw. Softwarization Unleashing Power Netw. Softwarization, NetSoft 2019, pp. 93–100, 2019.

[61] D. Gur, H. E. Rockette, and A. I. Bandos, “‘Binary’ and ‘non-binary’ detection tasks: are current performance measures optimal?,” Acad. Radiol., vol. 14, no. 7, pp. 871–876, 2007.

[62] L. Fernandez Maimo, A. L. Perales Gomez, F. J. Garcia Clemente, M. Gil Perez, and G. Martinez Perez, “A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks,” IEEE Access, vol. 6, no. c, pp. 7700–7712, 2018.

[63] C. Han and Y. Zhang, “CODDULM: An approach for detecting C&C domains of DGA on passive DNS traffic,” Proc. 2017 6th Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2017, vol. 2018-Janua, pp. 385–388, 2018.

[64] H. Šemić and S. Mrdovic, “IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks,” 2017 25th Telecommun. Forum, TELFOR 2017 - Proc., vol. 2017-Janua, pp. 1–4, 2018.

[65] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, “Botnet attack detection at the IoT edge based on sparse representation,” Glob. IoT Summit, GIoTS 2019 - Proc., pp. 1–6, 2019.

[66] R. M. Campbell, “A Survey of Honeypot Research : Trends and Opportunities,” pp. 208–212, 2015.

[67] M. F. Razali, G. Muruti, M. N. Razali, N. Jamil, and F. Z. Mansor, “IoT honeypot: A review from researcher’s perspective,” 2018 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2018, pp. 93–98, 2019.

[68] R. Vishwakarma, “A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks,” 2019 3rd Int. Conf. Trends Electron. Informatics, no. Icoei, pp. 1019–1024, 2019.

[69] K. P. Murphy, “Machine Learning - A Probabilistic Perspective - Table-of-Contents,” MIT Press, 2012.

[70] Z. Wang et al., “Honeynet construction based on intrusion detection,” ACM Int. Conf. Proceeding Ser., 2019.

[71] J. Ren and Y. Xu, “A compartmental model to explore the interplay between virus epidemics and honeynet potency,” Appl. Math. Model., vol. 59, pp. 86–99, 2018.

[72] A. Belqruch and A. Maach, “SCADA security using SSH honeypot,” ACM Int. Conf. Proceeding Ser., vol. Part F1481, 2019.

[73] A. Vetterl, R. Clayton, and I. Walden, “Counting outdated honeypots: Legal and useful,” Proc. - 2019 IEEE Symp. Secur. Priv. Work. SPW 2019, no. 2001, pp. 224–229, 2019.

[74] L. Christopher, K. K. R. Choo, and A. Dehghantanha, Honeypots for Employee Information Security Awareness and Education Training: A Conceptual EASY Training Model. Elsevier Inc., 2016.

[75] E. P. Joshi and P. S. Barth, “Honeypots and Honeynets: Level of Interaction and Issues in Privacy,” vol. 21, no. 16, pp. 881–885, 2019.

[76] S. Sekhar, D. K. Vijayakumar, B. Ketan, P. Swagatam, and D. Editors, Advances in Intelligent Systems and Computing 517 Artificial Intelligence and Evolutionary Computations in Engineering Systems, vol. 517. 2016.

[77] R. Breuk, “A visual analytic approach for analyzing SSH honeypots,” 2012.

[78] S. T. Park, G. Li, and J. C. Hong, “A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning,” Journal of Ambient Intelligence and Humanized Computing, vol. 0, no. 0, Springer Berlin Heidelberg, p. 0, 2018.

[79] S. K. Choi, C. H. Yang, and J. Kwak, “System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats,” KSII Trans. Internet Inf. Syst., vol. 12, no. 2, pp. 906–918, 2018.

[80] W. Wang, Y. Shang, Y. He, Y. Li, and J. Liu, “BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors,” Inf. Sci. (Ny)., vol. 511, pp. 284–296, 2020.

[81] S. Dowling, M. Schukat, and H. Melvin, “A ZigBee honeypot to assess IoT cyberattack behaviour,” 2017 28th Irish Signals Syst. Conf. ISSC 2017, pp. 0–5, 2017.

[82] M. Singh, M. Singh, and S. Kaur, “Issues and challenges in DNS based botnet detection: A survey,” Comput. Secur., vol. 86, pp. 28–52, 2019.

[83] M. Anirudh, S. Arul Thileeban, and D. J. Nallathambi, “Use of honeypots for mitigating DoS attacks targeted on IoT networks,” Int.

Conf. Comput. Commun. Signal Process. Spec. Focus IoT, ICCCSP 2017, pp. 8–11, 2017.

[84] L. Yin, X. Luo, C. Zhu, L. Wang, Z. Xu, and H. Lu, “ConnSpoiler : Disrupting C & C Communication of IoT-Based Botnet through Fast Detection of Anomalous Domain Queries,” IEEE Trans. Ind. Informatics, vol. PP, no. c, p. 1, 2019.

[85] Baykara, M., & Das, R., "A novel honeypot based security approach for real-time intrusion detection and prevention systems", Journal of Information Security and Applications, 41, 103–116, 2018. https://doi.org/10.1016/j.jisa.2018.06.004.

[86] Y. ALEKSIEVA, H. VALCHANOV, and V. ALEKSIEVA, “An approach for host based botnet detection system,” 2019 16th Conf. Electr. Mach. Drives Power Syst., no. June, pp. 1–4, 2019.

[87] A. Oliveri and F. Lauria, “Sagishi: an undercover software agent for infiltrating IoT botnets,” Netw. Secur., vol. 2019, no. 1, pp. 9–14, 2019.

[88] R. Alhajri, R. Zagrouba, and F. Al-Haidari, “Survey for Anomaly Detection of IoT Botnets Using Machine Learning Auto-Encoders,” Int. J. Appl. Eng. Res., vol. 14, no. 10, pp. 2417–2421, 2019.

[89] S. H. Mousavi, M. Khansari, and R. Rahmani, “A fully scalable big data framework for Botnet detection based on network traffic analysis,” Inf. Sci. (Ny)., 2019.

[90] N. Koroniotis, N. Moustafa, and E. Sitnikova, Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques, vol. 235. Springer International Publishing, 2018.

[91] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoTPOT: A novel honeypot for revealing current IoT threats,” J. Inf. Process., vol. 24, no. 3, pp. 522–533, 2016.

[92] M. Boer, M. Friedrich, M. Krämer, P. Noack, J. N. Weiss, and A. Zimmermann, Routing Protocol in the Industrial Internet of Things for Smart Factory Monitoring Abdellah. Springer Singapore, 2019.

[93] Y. Meidan et al., “N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders,” IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, 2018.

[94] S. K. Choi, C. H. Yang, and J. Kwak, “System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats,” KSII Trans. Internet Inf. Syst., vol. 12, no. 2, pp. 906–918, 2018.

[95] X. Yuan, C. Li, and X. Li, “DeepDefense: Identifying DDoS Attack via Deep Learning,” 2017 IEEE Int. Conf. Smart Comput. SMARTCOMP 2017, pp. 1–8, 2017.

[96] J. Guarnizo et al., “SIPHON: Towards scalable high-interaction physical honeypots,” CPSS 2017 - Proc. 3rd ACM Work. Cyber-Physical Syst. Secur. co-located with ASIA CCS 2017, pp. 57–68, 2017.

[97] A. Guerra Manzanares, “HoneyIo4 The construction of a virtual, low-interaction IoT Honeypot Treball Final de Grau,” 2017.

[98] P. Mesa and A. Rodr, B SIEM-IoT : A Blockchain-Based and Distributed SIEM. 2019.

[99] M. Wang, J. Santillan, and F. Kuipers, “ThingPot: an interactive Internet-of-Things honeypot,” 2018.

[100] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, “A Survey on Honeypot Software and Data Analysis,” 2016.

[101] L. Mathur, M. Raheja, and P. Ahlawat, “Botnet Detection via mining of network traffic flow,” Procedia Comput. Sci., vol. 132, pp. 1668–1677, 2018.

[102] Z.A. Almusaylim and N. Zaman, “A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks”, 25 (6), 3193-3204.

[103] Alyssa Anne Ubing, Syukrina Kamilia Binti Jasmi, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam, “Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning” International Journal of Advanced Computer Science and Applications(IJACSA), 10(1), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100133

[104] S.H. Kok, A. Abdullah, NZ. Jhanjhi and M. Supramaniam, “A Review of Intrusion Detection System using Machine Learning Approach”, International Journal of Engineering Research and Technology 12 (1), 8-15.

[105] M. Lim, A. Abdullah, N. Jhanjhi, M. Khurram Khan and M. Supramaniam, "Link Prediction in Time-Evolving Criminal Network With Deep Reinforcement Learning Technique," in IEEE Access, vol. 7, pp. 184797-184807, 2019. doi: 10.1109/ACCESS.2019.2958873

[106] Lim, M.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M. Hidden Link Prediction in Criminal Networks Using the Deep Reinforcement Learning Technique. Computers 2019, 8, 8.

AUTHORS’ PROFILE

Mr. Lee Seungjin is currently pursuing his Master’s Degree in Taylor’s University. Previously, he was employed as part of a cold-air manufacturing team under Samsung Electronics in South Korea

Dr. Azween Abdullah is a professional development alumni of Stanford University and MIT and his work experiences include thirty years as an academic in institutions of higher learning and as the Director of Research and Academic Affairs at two institutions of higher learning, Vice-President for educational consultancy services, 15 years in commercial companies as a Software Engineer, Systems Analyst and as a computer software developer and IT/MIS consultancy and training.

Dr. Noor Zaman has awarded as top reviewer 1% globally by WoS/ISI (Publons) recently for the year 2019. He has edited/authored more than 13 research books with international reputed publishers, earned several research grants, and a great number of indexed research articles on his credit. He has supervised several postgraduate students, including master’s and PhD. Dr Noor Zaman Jhanjhi is an Associate Editor of IEEE ACCESS, moderator of IEEE TechRxiv, Keynote speaker for several IEEE international conferences globally, External examiner/evaluator for PhD and masters for several universities, Guest editor of several reputed journals, member of the editorial board of several research journals, and active TPC member of reputed conferences around the globe.