Chapter 1

Secure Fog-Cloud of Things

Architectures, Opportunities and Challenges

Adam A. Alli
Uganda Technical College Bushenyi, Uganda

Kalinaki Kassim and Nambobi Mutwalibi
Islamic University in Uganda, Uganda

Habiba Hamid
University of Malaya, Malaysia

Lwembawo Ibrahim
Islamic University of Technology Dhaka, Bangladesh

CONTENTS

1.1 INTRODUCTION

The paradigm of Internet of Things (IoT) has emerged due to recent advances in computer hardware, software, embedded computing technologies, communication together with reduced costs and a drastic improvement in the performance of interacting devices. IoT has become a formal means of connecting people, things and information systems to the Internet through cyber-physical devices. This has resulted in a new breed of systems that allow real-world solutions to be implemented across countless Internet infrastructure and services such as cities, health and agriculture [1].

The challenges associated with the swarm of IoT devices encourage Fog computing, and its related edge computing models (MEC, cloudlets, Dew and Mist) to intelligently distribute processes and data along the physical boundaries of a network (radio access networks, routers and switches), resulting in a complex distributed cloud system over the Internet that is seen to improve the performance and Quality of Services (QoS) among IoT systems [2].

Performance is improved through approving the application of mobility support, latency minimization, location awareness and ensuring the security of processes, infrastructure and data [3]. With the considerable increase in the number of applications that attract the use of fog-cloud of things infrastructure, platforms and services, security and privacy concerns have prevailed over the IoT infrastructure starting from the end device to the core networks. Studies in [4] note that the success of applications of IoT systems depends on the ecosystem characteristics with emphasis to security. It is apparent that efficient security mechanisms that fit the behavior of IoT devices must be thought of. Secondly, it has become important to think of mechanisms that mimic intelligent behavior [3] such as self-healing besides considerable use of computing power.

Fog-cloud of things involves a Fog computing paradigm that allows computing, networking and storage that could not otherwise happen at the IoT device level. With fogging, the cloud is extended closer to the user where data is generated. A node is characterized as a Fog node if it has ability to connect to the Internet, is rich in resources and has the ability to outsource its resources to clients. Fog devices may include embedded servers, wireless routers, switches, edge routers and access points. Resources constrained devices are often installed at the IoT points which may include controllers, sensors and actuators that utilize the fog facility for latency-sensitive, mobile and response-sensitive applications. Thus, Fog computing benefits organizations by allowing conservation of network resources, reducing expenses of using powerful computing only when needed, providing better analysis of local data, repositioning processing closer to the edge of a network, hence increasing ownership and privacy. Lastly, it provides a range of security options on data and computing devices.

Security concerns in IoT–Fog systems are aggravated by the nature of outsourced computing from either lower or upper levels of the network infrastructure. The placement of devices on the network infrastructure may aggravate confidentiality, authenticity, integrity, trust and data protection [5, 6]. For example, in smart homes users connect to each IoT device using wireless connectivity most of which may use Bluetooth or Wi-Fi. Through listening to the network, a Bluetooth id or Wi-Fi password may be obtained. This may give full access to a home network through which security breaches such as controlling devices and locating other devices of the same kind across the whole network to expand attack areas can be achieved. Using such access holding facilities at ransom can become very easy. Other forms of attack on the home facility may include the use of leaky video cameras or social media attacks. Each of the above kinds of attack requires users to fix their device identification numbers, personal identification numbers, passwords and proof of security of the devices. Another important consideration is to separate home/enterprise networks from public networks by the use of secured Edge device.

Authors in [7] explain the complications that arise when data is stored or computation is transferred to be performed in the fog. Among them is the loss of control over either data or computation. Fog nodes are resource constrained and therefore may choose to initiate a deletion, modification or a destruction without leaving a trace to reserve its resources. In [8], authors illustrate security concerns that arise when a Fog node reclaims its computational resources by discarding data. Authors in [9] and [10] ascertain the effect of big data generated at the lower level in the IoT–Fog–Cloud hierarchy as a security concern. The difficulty of classifying big data as an attack or not increases the complexity of handling complex data at the fog [3]. These concerns make security in fog-cloud of things [2] is a crucial area of study. This chapter discusses some of the important aspects of security in the fog-cloud of things domain.

In this work, we address security issues in the fog-cloud of things environment by providing fog-cloud of things security architecture, key features of attack in fog-cloud environment and new methods of detecting the growing grounds of cyberattack in the IoT–Fog–Cloud arrangement. Further we offer material on application and challenges in secure fog-cloud of things systems. Our contributions in this regard are as follows:

- The authors provide a comprehensive discussion about the secure fog-cloud of things architecture.
- Secondly, we describe the characteristics of attacks and perform cybercrime classifications.
- Thirdly, we provide an appropriate machine learning (ML) kit for secure fog-cloud of things architecture that may enable detection of new strains of attacks in fog framework.
- Lastly, we provide guidance to the readers about fog-cloud of things by presenting applications and future research direction into security aspects in Fog computing.

1.1.1 Chapter Road Map

In this chapter, we address security aspects in the building block of fog-cloud of things infrastructure. In Section 1.1, we present an introduction to secure fog of things. In Section 1.2, we discuss the secure fog-cloud of things environment and architecture, whereas in Section 1.3, threats vulnerabilities and exploits in fog-cloud of things ecosystem are discussed. In Section 1.4, ML kits that are necessary to enable the architecture to adapt to new arising threats are presented. Key applications that attract the use of secure fog-cloud of things are presented in Section 1.5. In Section 1.6, we present opportunities and challenges in improving security in the fog-cloud of things ecosystems. In Section 1.7, we present future trends, and conclusion is drawn in Section 1.8.

1.2 SECURE FOG-CLOUD OF THINGS

The next generation of smart infrastructure that links the information and communication technologies(ICT), the industry and sustainable development will be achieved by leveraging advances in information services that optimize operational cost, preserve energy consumption and allow service provision even in times of crisis will be powered mainly by IoT [9, 10]. The IoT networks are characterized by a wide range of users, heterogeneity, production of a massive amount of data, and some applications that require high-speed networks. The above features of IoT have encouraged the use of cloud computing, Fog computing, and other related extended cloud paradigms. The fog-cloud of things extends the services of the cloud in a distributed fashion, encouraging efficiency and robustness in latency-sensitive applications that can be deployed with ease [11, 12].

The distributed nature of fog-cloud of things architectures is organized in hierarchical nature, with the lower layers hosting IoT devices, the middle layers hosting the Fog devices and the upper layers hosting the cloud. These applications hosted at each layer are susceptible to security threats and attacks which may result from the distributed design flaws, misconfigurations and implementation bugs, and sometimes less attention paid to security requirement of IoT devices by both the users and designers of IoT systems. New forms of attacks have been discovered to include on and off attacks [13], Distributed Denial of Service (DDoS) [14], flooding attacks [15], side-channel attacks and malware injection. These attacks have potential to disrupt fog services, compromise a user's security and privacy using any publicly accessible information or create a rogue Fog node to compromise the fog-cloud of things infrastructure [16]–[17]. In totality, the means of autonomously provisioning application resources to respond to changes in load on a given platform without any central enterprise infrastructure causes numerous challenges. These challenges include sandboxing for security, secure distributed load balancing, resource management and hardware-based defense against malware and ransoms. In a bid to mitigate security concerns in the fog-cloud of things frameworks that are viewed to mitigate several challenges have been discussed in [4, 18]–[19]. The general arrangements of the frameworks are constructed on securing the IoT devices, services and applications at the tiered planes of the fog-cloud infrastructure.

1.2.1 Environment

Recently, there has been a continuous transformation of ICT systems toward multi-domain architectures. These architectures create ecosystems that encourage the use of different forms of cloud services internally on the edge devices and externally via the Internet on cloud services. The progressive use of IoT, the edge, the fog and the cloud extends the boundaries between private ICT zones and public domains. The extension of these boundaries allows employees to work off premises while accessing the ICT resources of the enterprise. The off-premise employment model forces enterprise cyber-security to adopt security mechanisms that assume safe isolation of enterprise ICT assets. This is done by creating a virtual private network (VPN). VPN is used as a mechanism to segment enterprises network resources and denying remote access by unauthorized. Such security models is unproductive.

Some of the common security breaches that have rendered such a mechanism ineffective include externalization and offloading, demand for hosting sensitive and complex data on third parties' infrastructures, multiplicity and heterogeneity of abundant data collected by sensors and delivered in floods to the clouds for service. Secondly, most IoT devices have limited processing capabilities, which makes them more exposed to compromise than other IT assets in enterprise networks [2]. Thirdly, most organizations encourage their employees to use personal and mobile devices (smartphones, tablets and removable media) in the enterprise ICT assets. These devices brought in the enterprises can be compromised at different stages. Fourthly, inflexible defense toward DDoS and busty data traffic is a situation that is tricky to resolve, often the ICT administration may choose to 'turn open' allowing traffic to pass without inspection in a struggle to maintain availability until the problem is resolved, or 'to fail closed' blocking all traffic in application of a lockdown until the problem is fixed. All the choices may not leave business undisrupted.

Fog-cloud of things ecosystem in Figure 1.1 encompasses a myriad of IT resources (IoT devices, the edge, network, Fog devices, the cloud, services and applications) spanning several geographical locations to catch up with increased demand for flexibility in enterprise models. The models enable fog-cloud of things resources to be distributed across multiple networks – sometimes across publicly available networks. This makes fog systems candidate to attacks at the cyberspace level, computing resources level or even at the physical level. Resources like processors, storage devices, networks can physically be compromised because of ease to reach. Therefore, securing individual resources in such heterogeneous distributed systems created by fog-cloud of things requires new forms of pervasive security techniques that can ably deal with network threats, correlate events in both time and space dimensions, provide timely operational information to feed novel disruptive approaches capable of estimating the risk in real-time and carry out focused and effective defensive and mitigation actions [4].

Observing the ecosystem in Figure 1.1, security ought to be maintained at the IoT devices level, at the edge level, at the multi-tier fog level and multi-tier cloud level. IoT security takes care of security issues at the IoT devices level, whereas the edge security takes care of security

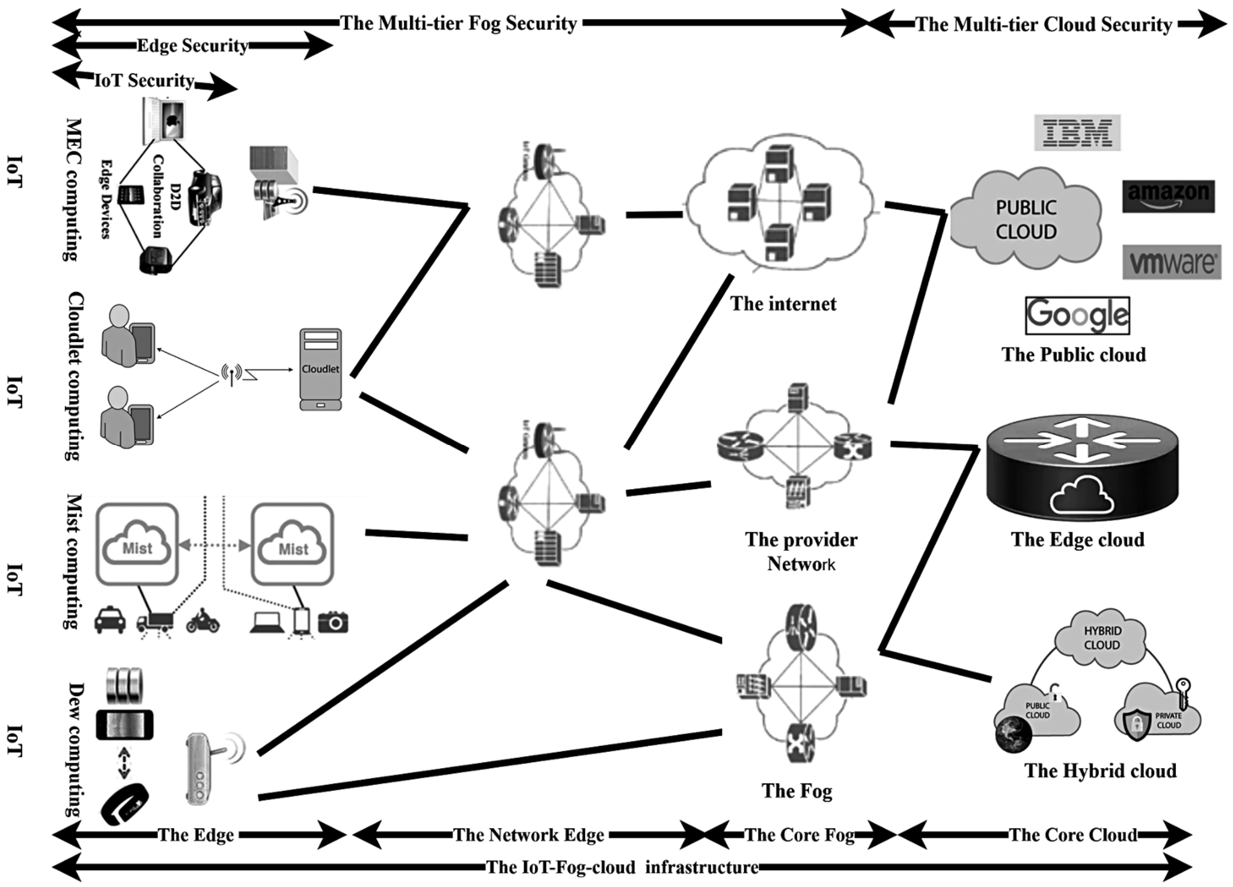

Figure 1.1 Fog-cloud of things ecosystem.

issues at the edge of the network. Beyond the edge issues of security at the multi-tier fog level are taken care of by the Fog security and lastly issues of security at the cloud level are taken care of by the cloud security.

1.2.2 Architecture

Figure 1.2 is a graphical representation of the secure fog of things architecture. This architecture is motivated to protect individual devices, data and processes in the IoT ecosystem. This is achieved through the implementation of end-to-end solutions that achieve protection through intelligent policy management, enforcement and continuous monitoring through aggregation. In addition, correlation of data is used to encourage the use of insights to enable automated functions of security in the IoT ecosystem. Automation of security function requires that the end-to-end solutions provide the following: i) Access control to users and devices based on security policy – these policies include issues of authentication, authorization, determination of security requirements, identification and inventorization of non-authenticated devices such as printers, scanners, etc.; ii) opportunities for context-aware policies that define security based on the full context of the situation – context-awareness may be defined in terms of sender/recipient information, size of information sent and received, reliability and the complexity of data. Context-awareness aligns closely with the business logic of the company; therefore, the context-aware solution is easy to implement and administer. With context-aware secure solutions, organizations can craft autonomous security policies that allow them to have effective security plan that gives them huge operational efficiency and control; iii) flexible deployment which includes options such as secure fog services and

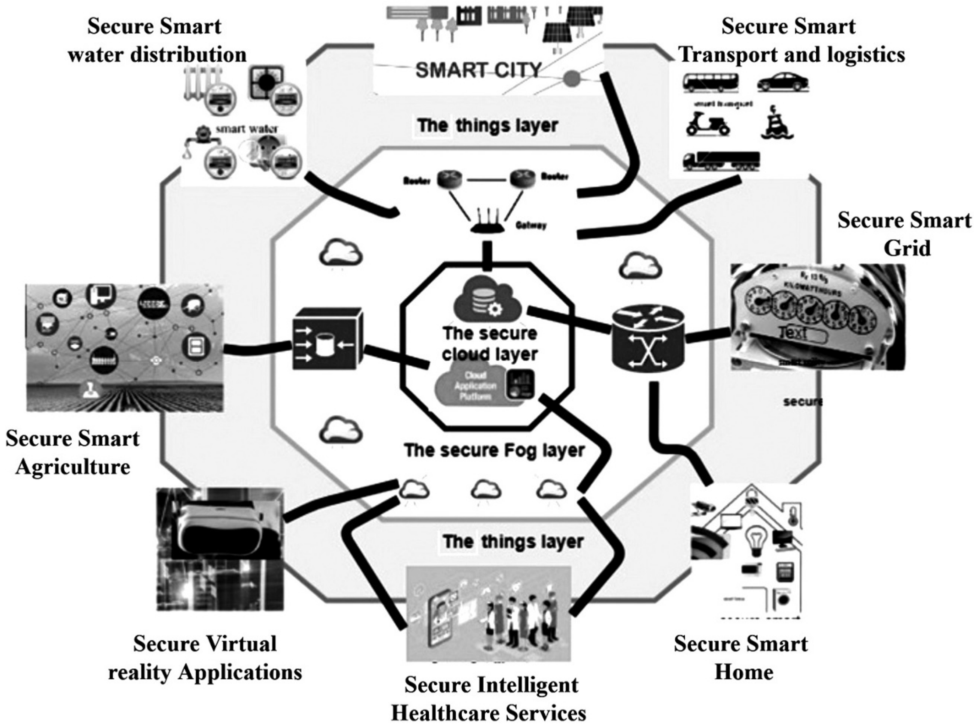

Figure 1.2 The secure fog-cloud of things architecture.

integrated security services across all the level of the network infrastructure to bring protection at the edge of the network; iv) support to reasonable insights into the network activities, transactions and threats. This allows enhanced protection and fast detection of anomalies.

The framework considered in the secure fog of things architecture is a layered architecture consisting of three layers. The framework is aimed at protecting things, processes and data in the fog-cloud of things ecosystems. The lower layers protect things (sensors and actuators), the second layer protects the network, the fog systems, data, processes and services, whereas the upper layer protects the cloud layer. Below we describe the functions of each layer.

i. **The secure things layer**

The things layer protects all types of cyber-physical objects that can connect to the Internet. These objects have embedded technologies that allow them to interact with the environment, collect a vast amount of data, send the data for processing over the network and then receive results of computation for further decision-making. The embedded technologies consist of sensors and actuators.

At this level, attacks mainly occur on IoT hardware (sensors, actuators and controllers) and produced data. One way by which hardware can be compromised is by placing an attack that increases the activities on the processors, memory, etc. forcing an overload, which in turn leads to poor resource utilization. On a poor resource utilization, the system performance is compromised leading to processor slow down and overuse of battery at IoT devices. These activities reduce the efficiency of the system as a whole. The second way of attacking devices at the IoT layers is forcing unauthorized access. This results in the misuse of data, jamming the device, privacy concerns, etc. To mitigate issues of security at the IoT layer, authentication mechanism, intrusion detection systems (IDS), lightweight encryption and anti-jamming mechanisms are applied.

At the things layer attacks are viewed in terms of being local or foreign. Local attacks originate from inside the network, whereas the foreign attacks originate from public networks. Inside attacks are launched from devices to physical objects, controllers and gateways. Some instances involve controllers' devices (e.g. gateways, switches, access points and routers) and users' devices. These attacks are triggered by rogue controllers, which pretend to be genuine on the network to serve as authentication point. Inside attacks affect controllers, IP and non-IP devices. The foreign attacks are launched from outside the network through gateways and routers. The foreign attacker formulates their attack in such a way that they disrupt services, applications and corrupt data used by the IoT devices. These attacks include denial of services, on and off attacks and botnets.

ii. **The secure fog layers**

The secure fog layer is responsible for protecting network resources, fog resources, applications and services. This layer protects not only attacks that are targeted toward gateways, routers, firewalls, etc. but also protocol services and application served at the fog. It prevents foreign attacks that are meant to disrupt the IoT services.

The secure fog layer host intelligent mechanisms that address network access concerns, information leakages and service attacks. Authentication, encryption, authorization and confidentiality are important considerations of the fog layer. Machine Learning(ML) plays a critical role in this layer as a means of advancing solutions that detect data disruption and distortion, intrusion and session breaches. The use of ML at this layer allows the network to adapt to changing dynamics to predict the behavior of applications and services. Further, the network can adjust to new forms of attack without compromising the robustness of the system. ML is used to advance recovery in form of self-healing.

iii. **The secure cloud layer**

The secure cloud is the upper layer of the architecture that provides a set of technologies, policies, software and applications that protect the cloud infrastructure as well as related data. The cloud security protects sensitive data, compliments data privacy, users' authentication and access control mechanisms to grant access and maintain security activities.

At this layer, security solutions are maintained on either public cloud, private cloud or hybrid cloud. Secure public cloud solutions offer both accessibility and security to data. Data in the public cloud is most often unstructured and attention is not given to customization. Security solutions at this level are cheap and affordable. On the other hand, the private cloud provides expensive security solutions but gives users security policies that allow them to manage their data. Secure hybrid cloud solutions are those that possess characteristics of both private and public cloud. In this setting, private secure policies apply to sensitive and complex data whereas, non-sensitive data are guided by public policy. The secure hybrid environment offers users with an alternative that strikes a balance between affordability and customization.

At the cloud, layer data is secured using advanced firewalls, intelligent intrusion detection systems, event logging, encryption and biometric physical security. Firewalls inspect data packets, verify the integrity of the packets and monitor behavior of the source and destination of the packets. Firewalls through inspection, verification and monitoring process can grant autonomous access and detect security breaches. Intelligent intrusion systems can detect intruders based on event log analysis. Proper analysis of event logs provides narratives that enable detection, prediction and prevention of new threats, attempted intrusion and other security breaches. This layer also provides advanced encryption and tight physical security normally based on biometric authentication systems.

1.3 THREATS, VULNERABILITIES AND EXPLOITS IN FOG-CLOUD OF THINGS ECOSYSTEMS

Threats, vulnerabilities and exploits in the IoT systems have continued to increase due to continuous desire to interconnect all things to the Internet. The increase in security threats in IT systems is motivated by the increase in value of information on the Internet, monitory resources on the Internet such as bank accounts that translate in monitory gains, complexity of the systems that attract satisfaction when compromised, alerts about security concerns reported by the users about the company information assets and lastly, increased interest in hacking as a profession.

In Figure 1.3, we group fog-cloud attacks in two basic categories: i) service disruption and ii) privacy breaches as discussed below.

Service disruption cybercrimes are intended to interrupt services provided by IoT systems, applications and processes. These attacks include but are not limited to

a. Ransomware: These are becoming the most public way of attacks accomplished through encryption of data. When successful hackers take control of services and processes provided by the IoT ecosystem using ransomware, they pursue for ransom from the service provider or the users [20]. Ransomware are of two kinds: i) those that encrypt valuable files on a computer and ii) those that lock the victim out of their device. Two interesting examples in these regards are WannaCry that appeared in 2017 and Ryuk that first

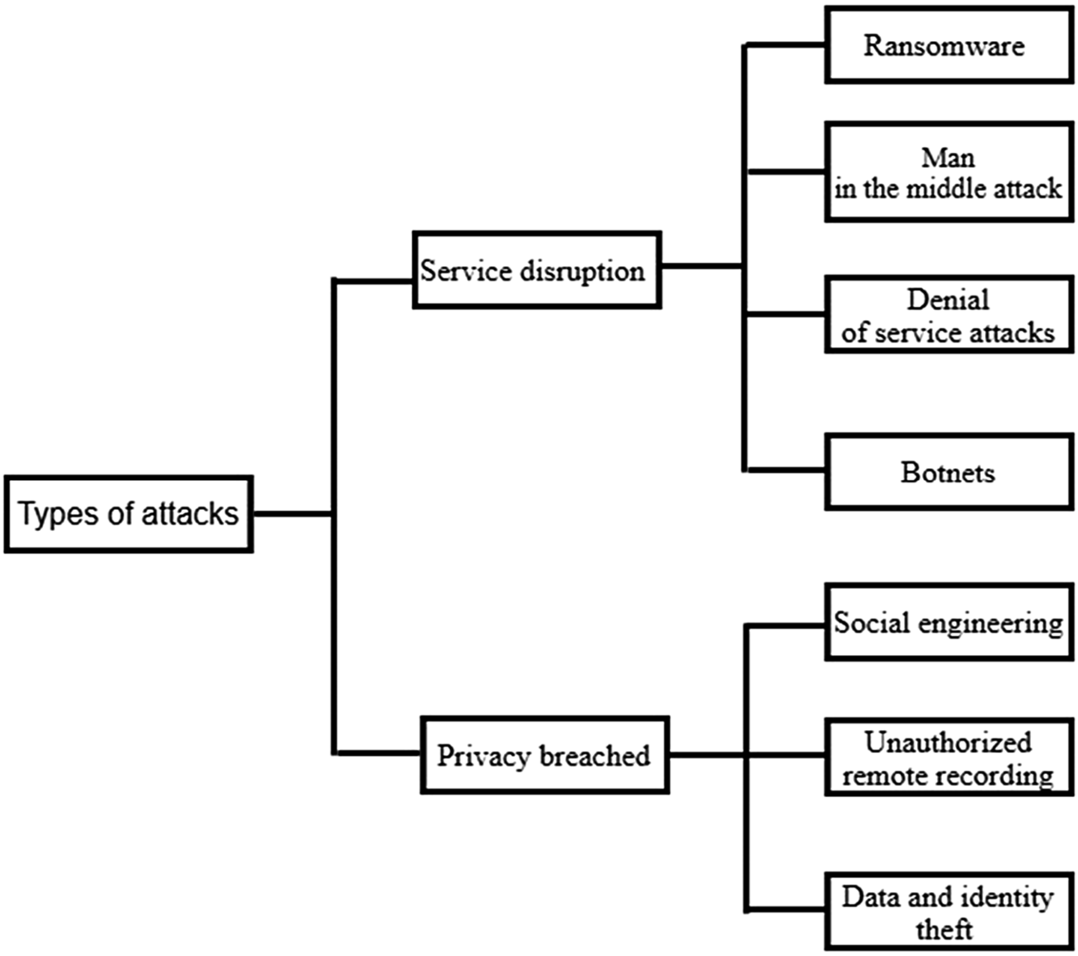

Figure 1.3 Classification of fog-cloud attacks.

appeared in 2018. WannaCry affected over 200,000 devices over the globe. Mainly its target was windows systems and locked its users out. A ransom was requested in bitcoin to gain access to your files or devices, whereas, Ryuk disabled windows restore, encrypted files and network drives. It affected many organizations in the USA. Ryuk is observed to be one of the most expensive ransomware attacks in history. Other examples include locky, jigsaw trodesh, cryptolocker and recently wastelocker.

b. Man-in-the-Middle attack: This is when a hacker positions himself in the middle of the individual communication system with an objective of intercepting and gaining access. On gaining access they can create harm to a fine working system [21]. Examples of Man-in-the-Middle attacks are IP, DNS, HTTPS spoofing and email hijacking.
c. Denial of service attacks (DoS): These are motivated to upset services by deliberately overloading the system. Overloading systems sets efficiency and reliability of systems to question. By downplaying the system reliability, users feel uncomfortable and frustrated about the system. In the critical system DoS can cause serious accidents. For example, delays in response in autonomous vehicle system can cause the autonomous vehicle to lose course. Normally DoS does not result in theft of data or identity [22, 23].
d. Botnets: With this kind of attack, a hacker creates a network in association with many systems to take control of the target system. The aim of botnets is normally to compromise confidentiality of a stable system, obtain data and access that would enable them to launch attacks on systems that use IoT devices and services [23]. Botnets can be very effective in launching a successful attack on a vulnerable IoT system. Examples of botnets include Mirai which targeted smart devices that run on ARC processors to launch DDoS attacks. Other Botnets are 3ve, Methbot, mariposa and Grum.

On the other hand, privacy breach attacks are motivated to withdraw freedom from users to use services, application and data provided by IoT systems. These types of attacks include the following:

a. Social engineering: Social engineering attacks involve manipulating users so that they can give up information that can grant hackers access to the system without question by posing as legitimate users. An example of social engineering could be a received mail fooling the user to change his password through a provided link. When the user chooses to update his email through the false link, his information is captured and used to have access and compromise the system [24]. Another related example is to compel users to click a link sent to the emails so that an automatic malware or spyware that continues collecting information about the system can be used to sidetrack the network on which the system is connected. Social engineering tricks can range from simply posing as a helper on call to sophisticated tricks that attackers attract user curiosity to share very important information about them and the systems they use on a daily basis. Social engineering can be avoided if the users verify the persons from whom they seek help in regard to their information, changing login information occasionally, setting security instruments such as anti-spamware and filters, and keeping information about their transaction as private as possible [25].
b. Unauthorized remote recording: This involves either audio, text or video surveillance of users so as to temper with their privacy. This is common with gadgets that are installed in places of work or homes such as surveillance cameras, TV and nanny dolls. Hackers find means through which they can take control of these gadgets and record activities around the environment and can use it to misrepresent person's character of interest. As a result of leaked information, the person of interest is forced to give up his career or buy out to save his integrity. This kind of attack can be avoided by ensuring that one installs security and surveillance equipment from legitimate providers and a

well-stipulated user contract is signed. Secondly, the user should have the knowledge on how privacy can be breached. In addition, all the default security setting should be changed before use. To avoid physical tempering, the surveillance equipment must be installed in secure hard to reach places around the users' location.

c. Data and identity theft happens when hackers steal user's personal information that may include bank accounts, social security details, billing details, passwords or email details. With the rise in the use of smart devices, gaining access to information about a user is becoming easier. They use this information to impersonate a genuine user resulting in loss of credibility or property through using the stolen information to gain access to user's digital life. Along with this information, hackers may gain access to sensitive information about users' family, belongings and health. This information can be used to harm the user in numerous ways, which may include reputation obliteration, covering security crimes, public humiliation and financial loss. Data and identity theft can be avoided by proper management of user accounts starting with device access accounts by creating strong passwords that cannot easily be cracked. A strong password is that which is long enough to remember, consists of a combination of text, numbers and special symbols. Finally, users should avoid unlimited social media exposure, opening suspicious emails and also learn about site privacy and security policies [25].

In Table 1.1 below, we present types of attacks and their attack vectors. These vectors may be engineered in many ways to allow the hacker hurt the organizational ICT resources with ease.

Table 1.1 Showing types of attacks and their attack vectors.

Articles	*Attack Type*	*Attack Vector*
[5, 8, 9]	Ransomware	• Remote desktop protocol (RDP) • Email phishing • Software vulnerabilities
[5, 13, 15]	Man-in-the-Middle	• Rouge Fog nodes • Vulnerabilities in web browsers • SQL injection • Trojan Horses, worms • Public networks
[5, 13, 26]	DDoS	• **DNS Amplification** • **UDP flood** • IP fragmentation • SNMP Reflection • SYN flood
[5, 20, 27]	Botnet	• **DNS Amplification** • **UDP flood** • IP fragmentation • SNMP Reflection • SYN flood
[24, 28]	Social engineering	• **Rouge websites** • **Fake emails** • posing as a helper on call
[5, 8]	Unauthorized remote recording	• surveillance cameras • **Television** • **Nanny dolls** • **Personal assistant devices**
[28, 29]	Data and identity theft	• Social media • Emails • Rogue websites

1.4 KEY MACHINE LEARNING KITS FOR SECURE FOG-CLOUD OF THINGS ARCHITECTURE

Fog computing is a source of big data. Observing the emerging trends in Fog computing technology and applications of ML has been explored in many places such as improving efficient resource management, modeling traffic in fog-cloud environment, improving security, etc. The importance of ML kits is threefold: i) improving security techniques in terms of security models, handling security in systems in order to manage large volumes and varied data, flexibility in handling attacks and issues of cryptography; ii) developing security architectures that are able to autonomously detect and handle future security vulnerabilities with little human intervention; iii) improving issues of reliability, trust and privacy in the fog-cloud of things at all levels.

ML approaches provide useful mechanisms that have been used for data analytics to engineering pattern, extract useful features and predict values from massive amounts of data [30, 31]. ML approaches at the fog allow development of autonomous security systems at the fog of things that are distributed, can manage and update security credentials at a local level, scan for security vulnerabilities such as malware and distribute timely software patches on large scale [3]. In this section, we highlight some important aspects of ML kits for authentication, access control, etc.

a. ML-based authentication.

   Hackers have recently developed a mechanism that bypasses the utmost complicated authentication mechanisms. These authentication mechanisms may include password-enabled authentication [32], two-factor authentications [25], biometric authentication or by the use of extensible authentication protocols. The superlative way to keep unwanted users' authentication is to combine ML with n-factor authentication where n defines many or multiple factors. This would enable security systems to learn and prevent attacks based on behavior.

   The ML-based authentication at the fog level enables identification of high-risk users at the local level and gives them different treatment other than those given to trustworthy users. For example, resident users (those logging in from the inside) are treated differently from the off-premise users. This is accomplished through authentication-related data of the users over time to establish baseline normal behavior putting numerous factors to check. These factors may include time-based login activities, location and IP address used to log in, successful and failed log in frequencies, analysis of the login done on premises and off premises, frequencies of application-level authentication, analysis of risky authentication, etc. Generally, machine authentication is capable of keeping authentication procedures local and private, keeping track of users and guarantee authentication at both the IoT level and cloud.

b. ML-based access control

   Hackers dedicate most of their time crafting complicated mechanisms to realize an attack on ICT infrastructure of organizations no matter how intricate the security is. Most of the time security breaches in a network system are traced back to the inadequate access control mechanism especially during this period of the IoT that has brought up new working habits and policies. Such habits may include but are not limited to working anywhere at any time, bring your own device, etc. Due to requirements of working off-premise companies most often relax or completely neglect access policies creating security loopholes.

   ML access control could help bridge access control gaps by enabling systems to autonomously learn how to adjust privileges to include write or read access, isolating access according to roles, duties and functions let alone enabling the system to group users devices according to behavior then applying policies such as no sharing among groups, locking down some groups based on IP or working time. On the other hand, auditing and monitoring of accounts is important such that devices can take care of sensitive information for i) local processing, ii) prompt users to renew their passcode locally or iii) update policies on accessing information regularly. Secure fog of things ensures well-structured access control mechanisms for both local and cloud infrastructure.

c. ML botnet detection

Botnet detection involves spotting attacks caused by controlled network environment. The botnet systems are used to create DDoS attacks, floods and sometimes used to spread the virus. Attackers often recruit an army of computers and IoT systems to allow them to fulfill their mission. These recruited systems are known as bots. The bots are usually unaware that they are used as attack agents. The way botnets work is by the use of botnet master to initiate, manage, coordinate and recruit attack systems as many as possible for destructive mission. The botnets then send instructions to the bots to launch an attack. With the increase in computing capacities of ICT devices mobilizing smart devices, computers and IoT into a botnet can launch a pretty powerful and disruptive attack.

The primary purpose of ML techniques for botnet detection is to identify, learn, and collapse the botnet server including all its assets. The kits used for botnet detection collect information and find out what technology is used in the botnets, analyze the risk and intensity of attack and identify botnet server for disabling action. Furthermore, the kits are equipped with the ability to observe network traffic, responses, loads and link status. This information is used in different ways to monitor sleepers, sniffers and trojans. These kits can be used to accomplish both passive and active monitoring of the IoT ecosystem for the intrusion. We note that the botnet detection systems can be loosely characterized as intrusion detection systems [26] and HoneyNets [27].

d. ML-based Malware detection and classification

Overtime the number of malwares, their complexity and dynamicity in signatures have increased rendering the traditional methods ineffective in detecting and classifying malware files [33]. Their intricacy increases more in the era of big data whose velocity, size and variability plays important role in identifying the underlying signatures of attacking malware.

ML toolkits at the fog are useful mechanisms to obtain statistics and reports about the malware activities, explore them, select features important for their identification, train and retrain on datasets using different kinds of suitable ML algorithms [33, 34], and then deploy the machine at the Secure fog of things to monitor traffic. The toolkit deployed here would help identify and classify malware on both entry and exit of IoT network.

Secondly, these toolkits are getting considerable attention among the anomaly detection scholars to address the weaknesses of knowledge base detection techniques [34]. This is due to the fact that anomaly detection can effectively help in catching fraud while discovering strange activity in large and complex big data sets, thus proving to be useful in areas such as banking security, natural sciences, medicine and marketing, which are prone to malicious activities [14]. Moreover, anomaly detection can be a key for solving intrusions [35], while detecting anomalies. Worries of abnormal behavior indicate a presence of intended induced attacks, defects and faults.

ML algorithms installed at the fog have the ability to learn from data and make predictions based on that data. ML for anomaly detection includes techniques that provide a promising alternative for detection and classification of anomalies based on an initially large set of features. Generally, secure fog of things frameworks will allow businesses to be provided with a simple yet effective approach for detecting and classifying anomalies.

e. Offloading

Critical infrastructures that are powered by IoT such as health facilities, industries, utilities and cities may be compromised thus lowering the Quality of Service (QoS) and experience. To maintain the QoS of these systems, offloading is encouraged [36]. The emergency of Fog computing combines IoT and ML to facilitate the moving of services near to the devices at the edge, offloading minimizes delay, improves performance and balances traffic load in the network. Besides load balancing, offloading can be done to save IoT devices that under attack. Secondly, offloading sensitive data can be localized on the fog or private cloud to preserve confidentiality and trustworthy computing. Further, offloading combined with technologies such as blockchain may yield excellent security mechanism [28]

1.5 APPLICATIONS

The core objective of enterprises is improving productivity using IoT systems, at the same time maintaining quality of service and experiences. Securing devices is critical for business environments, utility industry, factories and other infrastructures such as health facilities, cities, and environment that host services that are delay-sensitive. The following applications attract the use of secure fog-cloud of things:

Secure Intelligent healthcare services

Numerous wearable smart devices are being used by health workers to monitor the user's general health condition and keep the records of the patients [37]. During the use of these IoT devices to monitor the health status of the patients by harvesting data which is sensitive and private. Securing confidential information of the patients and processing them on local or the fog is the best use of extended cloud framework [29]. Thus, secure Fog computing can be employed to minimize issues related to detecting, predicting and preventing a breach of patients' devices and data to cause harm to their health or attacking their privacy by sending warning signals to the patients, doctors and caretakers. This increases issues of trust, reliability and prevention of data and information in the secure Fog-cloud infrastructure for smart health [38].

Intelligent traffic lights

Smart traffic regulator systems may assume some functionality of Fog devices to coordinate traffic signals as well as send a warning signal to an approaching vehicle [29]. Moreover, the intelligent traffic lights are also capable of identifying the flashing lights of an ambulance or a police car at crossroads using video cameras and immediately change traffic lights accordingly [38]. Similarly, the smart traffic systems may communicate locally with sensors to identify the occurrence of the person on foot and cyclists thereby evaluating the distance and speed of approaching vehicles thus preventing accidents while maintaining a stable flow of traffic [29]. Such a system requires robust intelligent security applied to it.

Intelligent Grid

In many of power generation and distribution systems, IoT have been deployed to be used in different ways starting from power generation, optimized distribution and consumption. The intelligent grid technology is made up of a two-way smart and intelligent flow of information between the consumer and supplier. The IoT fixed at consumers' premise gather data and forward it to the nearest Fog. At the Fog near real-time analytics is performed to discover issues related to electricity supply, consumption patterns, metering and pricing among other particulars. This next-generation application of IoT and related fog infrastructure requires to be safe, secure and trustworthy. Explicit security and privacy solutions at the fog-cloud of things should be able to maintain data confidentiality, handle big data and serve intelligent meters fixed at both the supplier and consumer households without being compromised.

Other applications related to secure Fog computing are industrial IoT, smart agriculture, Augmented reality, smart water metering among others. Each of these applications require robust, scalable, trustworthy security mechanisms that allow them to handle complex, sensitive and big data.

1.6 OPPORTUNITIES AND CHALLENGES IN IMPROVING SECURITY IN FOG-CLOUD OF THINGS

The use of smartphones and other cyber-physical devices has opened a Pandora's box in the areas of security, privacy and trust in the IoT ecosystems. Most of the concerns fall in three broad areas: a) the ever-increasing number of IoT-based attacks launched from heterogeneous platforms of smart devices (smartphones, cameras, printers, etc.). Hackers use these platforms to exploit enterprise ICT default systems, bringing the critical system in the organization down and affect many applications around enterprise daily operations. b) The second concern is the interoperability in IoT–Fog systems. The IoT–Fog architectures are fairly new and have not been dealt with before. Therefore, issues that involve handling heterogeneous protocols, operating procedures, communication resources and constrained resource utilization in a secure fog environment are still at large. c) In addition to the novelty of IoT–Fog, the upcoming of the new multi-tier IoT–-Fog–Cloud paradigms defined by multiple customers and tenants, exposed hardware, software and distributed infrastructure present new concerns in their way.

1.6.1 Opportunities

The secure fog of things provides security opportunities in mainly two ways:

i. Boosting security services: This is done by improving the security function of the Fog device through provision of service and support functions. The fog may be used to process, store and transmit sensitive data locally along the edge protecting the users' privacy. Secondly, the fog software backplane may be improved to supply IoT devices with the necessary security updates and patches to keep them secure. Updating billions of IoT devices is a challenging undertaking; therefore, management functions that include new policy-based access control models may be used to overcome the limitations of updating IoT security functions.

ii. Provision of SECurity as a Service (SECaaS): Secure fog may also offer SECaaS along with the ability to solve many other fog challenges such as Latency Constraints, Network Bandwidth Constraints, Resource-Constrained Devices, Uninterrupted Services with Intermittent Connectivity to the Cloud [3].

Generally, the secure fog of things provides opportunity for secure and trusted computing to be available to IoT devices. They are capable of making IoT systems more robust and trustworthy.

1.6.2 Challenges

Challenges associated with security in the next-generation IoT systems include the following:

i. Interoperability of security systems. Perhaps the most complex phenomena arising in computing today. Interoperability cuts along many dimensions specifically the diversity of devices (surveillance, wearables, smart appliance, etc.), interfaces (wireless, vehicular, powerline, etc.) and operating paradigms. Each of these may need a diverse security mechanism to communicate first among themselves and the longstanding network-based use of TCP/IP and its related security mechanisms.

ii. Unlike in the cloud or enterprise data centers setting where important ICT resources are protected by physical security mechanisms such as key and lock, physical security breach in Fog computing has not been completely resolved yet. Most IoT devices in the fog environment are formed within the reach of any unauthorized person. Therefore, anybody with the intention of attacking the systems can physically reach the sensors, actuators and the Fog devices. This gives opportunity to malicious person to physically manipulate the systems. An example of such attack is planting a trojan on a flash disk and dropping it in parking yard. If a person picks and plugs it in the organization system, then a Trojan horse is automatically transferred to a computer on the systems without the user's knowledge. Another example is tempering with fog by physically resetting them without the knowledge of the administrator with the intention of creating backchannels to access the system. It is easy to initiate a physical security breach in the Fog working environment which results in a complex attack. Due to probable physical reach to the fog, it is easy to compromise the system and make it available to attackers who will gain control. Therefore, ensuring physical security and privacy becomes a serious concern in the security of fog systems.

iii. Trust, security tracking and monitoring is another serious challenge. Trust plays a two-way role in a fog network. The first role is that the Fog nodes offer services to IoT devices. In this case the fog should be in position to corroborate whether the devices requesting services are genuine. Secondly, since IoT networks are expected to provide secure and reliable services to the end-users, it becomes a requirement for all devices that form part of the fog network to have a certain level of trust.

iv. The Fog networks are complex distributed systems. Complexity of fog systems increases vulnerabilities which in turn creates loop holes. This makes it easy for hackers to find a way of connecting to the network from many unauthorized points without notice. This provides grounds for attackers to deploy attack mechanisms such as DDoS, Jamming, Eavesdropping, Man-in-the-Middle attacks, Active impersonation, Message replay attacks, Data breach, Sniffing and Illegal resource consumption.

1.7 FUTURE TRENDS

Recently, there has been a renewed effort to boost security of complex IoT systems. The complexity arises from the need for mobility, diversity in applications and hardware, and the demand of distributed powerful computing closer to the user. This nature of computing encouraged by IoT devices and networks does not only provide rich ground for hackers but also simulate large transactions over the network which is an ingredient to poor quality of service (QoS). Adopting secure Fog computing is a means of improving quality of service at the same time stopping intruders from conducting their business. Fog computing eliminates vulnerabilities as a result of decentralized architecture. Secondly, they localize computing, which in turn reduces the target of cyberattack. It is hoped that advances in ML and blockchain in the fog will eliminate new threats and single point of failure created by centralized architectures. Hence the future will see a) secure and trusted service and b) SECaaS provided at the edge of the network.

a. Secure and trusted computing services
The beauty embedded in future of secure Fog computing is trustworthy computing. The ability to create an accurate defense system built upon pillars of different security domains such that when an anomaly is detected, a policy or behavior-based decision is taken. Using such in-depth strategy, a responsive security system that is always available is built. Additionally, such kind of a system shall exhibit survivability given that it can respond to new threats without difficulties. Secure Fog of things enables distributed data processing and storage near the data source, and affordable high-performance trusted computing anywhere any time. This shall enable adoption of new technologies (5G and beyond) with considerable ease.

b. SECurity as a Service
The secure fog of things is seen to be a great enabler of SECaaS on the edge of a network. The edge SECaaS shall provide protection to both the lower and the upper layer IoT systems. In addition, it shall facilitate secure transaction between the local networks and the cloud. This will be realized through fog-based intrusion detection systems and secure data repositories. Moreover, the secure fog shall provide coordinated and distributed defense in a way that the fog systems shall be integrated with dynamic centralized response to any form of attack, threat and vulnerabilities.

1.8 CONCLUSION

This chapter covered content related to secure fog architecture. We provided a discussion on fog-cloud infrastructure, ML kits that may enable autonomous detection of new strains of attack in Fog. We noted that ML is usable in many fog applications, and security is one of them. ML methods are capable of adapting to new threats, vulnerabilities and exploits. As part of Fog computing we have included fog-cloud of things and their applications. The challenging aspects of fog-cloud of things include interoperability of security issues, easy physical access that enables easy compromise, complexity in motoring attacks due to mobility of devices, vast amount of data generated, traffic bust along the infrastructure which may not necessarily mean an attack and scalability in network devices. Lastly, the future prospects of secure fog shall be based on trusted services and SECaaS. Therefore, readers may consider various ML kits in fog-cloud architecture to develop secure fog systems and address diverse challenges. In future we intend to study methodologies that may be used to enhance intelligent security at the Fog.

REFERENCES

1. H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," *IEEE Netw.*, vol. 32, no. 6, pp. 144–151, Nov. 2018.
2. A. A. Alli and M. M. Alam, "The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications," *Internet of Things*, vol. 9, p. 100177, Feb. 2020.
3. A. A. Alli and M. M. Alam, "SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications," *Internet of Things*, vol. 7, p. 100070, Sep. 2019.
4. M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
5. S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," *In International conference on wireless algorithms, systems, and applications* 2015 Aug 10, pp. 685–695.
6. M.-H. Maras, "Internet of things: Security and privacy implications," *Int. Data Priv. Law*, vol. 5, no. 2, pp. 99–104, May 2015.
7. M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram, and S. Raza, "Fog computing: An overview of big IoT data analytics," *Wirel. Commun. Mob. Comput.*, vol. 2018, Article ID 7157192, p. 22, 2018. doi:10.1155/2018/715719.
8. J. Yakubu, H. A. Christopher, H. Chiroma, M. Abdullahi, and others, "Security challenges in fog-computing environment: A systematic appraisal of current developments," *J. Reliab. Intell. Environ.*, vol. 5, no. 4, pp. 209–233, 2019.
9. E. K. Markakis et al., "Efficient next generation emergency communications over multi-access edge computing," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 92–97, 2017.
10. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
11. E. Ahmed and M. H. Rehmani, "Mobile edge computing: Opportunities, solutions, and challenges," *Futur. Gener. Comput. Syst.*, vol. 70, pp. 59–63, 2017.
12. O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "Edge computing enabling the internet of things," in *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, Milan, Italy, 2015.
13. C. V. L. Mendoza and J. H. Kleinschmidt, "Mitigating on-off attacks in the internet of things using a distributed trust management scheme," *Int. J. Distrib. Sens. Networks*, vol. 11, no. 11, p. 859731, Nov. 2015.
14. R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devisces," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, no. Ml, pp. 29–35, 2018.
15. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.
16. W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, pp. 1606–1616, 2018.
17. E. Alemneh, S.-M. Senouci, P. Brunet, and T. Tegegne, "A two-way trust management system for fog computing," *Futur. Gener. Comput. Syst.*, vol. 106, pp. 206–220, 2020.
18. N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," *J. Inf. Secur. Appl.*, vol. 52, 2020.
19. X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: A security framework for the Internet of Things," *Secur. Commun. Networks*, vol. 9, no. 16, pp. 3083–3094, Nov. 2016.
20. A. Namavar Jahromi et al., "An improved two-hidden-layer extreme learning machine for malware hunting," *Comput. Secur.*, vol. 89, 2020.
21. I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," *2014 Federated Conference on Computer Science and Information Systems*, Warsaw, Poland, 2014, pp. 1–8, doi: 10.15439/2014F503.
22. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", *Computer Networks*, vol. 44, no. 5, 2004, pp. 643–666, ISSN 1389-1286, doi:10.1016/j.comnet.2003.10.003. https://www.sciencedirect.com/science/article/pii/S1389128603004250

23. M. Alauthman, N. Aslam, M. Al-Kasassbeh, S. Khan, A. Al-Qerem, and K.-K. Raymond Choo, "An efficient reinforcement learning-based Botnet detection approach," *J. Netw. Comput. Appl.*, vol. 150, p. 102479, 2020.
24. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, Jun. 2015.
25. S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technol. Soc.*, vol. 32, no. 3, pp. 183–196, Aug. 2010.
26. W. Li, W. Meng, and M. H. Au, "Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments," *J. Netw. Comput. Appl.*, vol. 161, 2020.
27. Z. Li, A. Goyal, and Y. Chen, "Honeynet-based Botnet Scan Traffic Analysis," *Botnet Detection*, in Lee, W., Wang, C., & Dagon, D. Ed. Boston, MA: Springer US, 2008, pp. 25–44.
28. A. A. Alli, M. Fahadi, and C. Atebeni, "Blockchain and fog computing: Fog-blockchain concept, opportunities, and challenges," in *Blockchain in Data Analytics*, Mohiuddin Ahmed, Ed. Cambridge: Cambridge Scholars Publishing, 2020, p. 75.
29. G. Rahman and C. C. Wen, "Fog computing, applications, security and challenges, review," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 1615–1621, 2018.
30. S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," in *Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit on - eCrime '07*, Pittsburgh, PA, USA, 2007, pp. 60–69.
31. S. M. A. Karim and J. J. Prevost, "*A machine learning based approach to mobile cloud offloading*," *2017 Computing Conference*, no. July, pp. 675–680, 2017.
32. K. M. Renuka, S. Kumari, D. Zhao, and L. Li, "Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems," *IEEE Access*, vol. 7, pp. 51014–51027, 2019.
33. S. Joshi, H. Upadhyay, L. Lagos, N. S. Akkipeddi, and V. Guerra, "Machine learning approach for malware detection using random forest classifier on process list data structure," in *Proceedings of the 2nd International Conference on Information System and Data Mining - ICISDM '18*, Lakeland, FL, USA, 2018, pp. 98–102.
34. D. Raposo, A. Rodrigues, S. Sinche, J. S. Silva and F. Boavida, "Securing wirelessHART: monitoring, exploring and detecting new vulnerabilities," *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, 2018, pp. 1–9, doi: 10.1109/NCA.2018.8548060
35. R. U. Khan, X. Zhang, R. Kumar, A. Sharif, N. A. Golilarz, and M. Alazab, "An adaptive multi-layer botnet detection technique using machine learning classifiers," *Appl. Sci.*, vol. 9, no. 11, 2019.
36. P. Patil, A. Hakiri, and A. Gokhale, "Cyber foraging and offloading framework for internet of things cyber foraging and offloading framework for internet of things," no. September, 2016.
37. N. Tariq *et al.*, "The security of big data in fog-enabled IoT applications including blockchain: A survey," pp. 1–33, 2019.
38. J. Ni, S. Member, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 601–628, 2020.
39. A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, R. M. Parizi, and K.-K. R. Choo, "Fog data analytics: A taxonomy and process model," *J. Netw. Comput. Appl.*, vol. 128, pp. 90–104, 2019.
40. A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," *Computer (Long. Beach. Calif.)*, vol. 49, pp. 112–1162016.
41. P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: Architecture, key technologies, applications and open issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 27–42, 2017.
42. K. Sethi, R. Kumar, L. Sethi, P. Bera, and P. K. Patra, "*A novel machine learning based malware detection and classification framework*," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Oxford, UK, 2019, pp. 1–4.