CURRENT TRENDS IN COMPUTING
VOL.1 NO.1 PP.22-43 (2023)
ISSN: 2980-3152
Received: 04.03.2023
Accepted: 12.03.2023

FIREWALLS AND INTERNET OF THINGS SECURITY: A SURVEY

MOSTAFA RAEISI-VARZANEH [1], ADIB HABBAL[1], OMAR DAKKAK [1*]

[1] *Computer Engineering Department, Karabük Üniversitesi, Karabük, 78050, Türkiye*

Abstract. One way to define the Internet of Things is as a network of objects, data, and the internet. Things can be referred to as objects, whether an appliance, a car, a human, an animal, or a plant. Connected devices, manufacturers, and operators can exchange data over the Internet of Things to monitor and control their functions. According to analysts, thousands of things are predicted to be connected to the Internet of Things. Consequently, these devices generate a great deal of data. This enormous amount of data is described as Big Data. In addition to its volume and velocity, this data is diverse and varied. This data is at risk of being compromised. Firewalls are security devices that monitor, and control network traffic flow based on a set of predefined rules. More proactive firewalls are needed to block current and emerging threats such as botnets and targeted attacks. This paper provides a comprehensive overview of the information security issues and demonstrates how firewalls can mitigate these challenges in IoT applications.

1. INTRODUCTION

Agriculture, industry, and information technology are the first three waves of human history. A huge change has occurred in the quality of human life due to these waves. In the fourth wave of human history, we are entering the era of the cyber-age, in which everything is always connected to everyone [1]. Thanks to this huge development, all communication requirements will be fulfilled whenever they arise, with minimal human involvement and easily through the internet of things (IoT).

The IEEE describes the IoT as follows [2]: " It consists of a complex, self-configuring, adaptive network that connects devices via standard communication protocols to the internet. There are interconnected things which are programmable and uniquely identifiable with physical or virtual representations, sensing, and actuation capabilities. In addition to its identity and status, an object's representation includes its location and any information relevant to its private, social, or business life. Things Offer

E-mail address: omardakkak@karabuk.edu.tr [(*)].
Key words and phrases. Internet of Things, Security Threats, IoT Security, Firewalls.

services to consumers with or without human involvement by capturing data, communicating, and actuating sensors. Through intelligent interfaces, the service is accessible anywhere, anytime, and for any purpose involving security.".

As smart devices such as sensors and actuators become more connected, the internet of things (IoT) is forming. In addition to their use in smart cities, smart homes, and intelligent transportation systems, these devices can also be used in environmental and public health monitoring. The concept of IoT is depicted in Figure 1. Security and privacy issues are associated with this vast range of IoT applications. Unless an IoT ecosystem is trusted and interoperable, emerging IoT applications may not reach the level of demand they were designed for. Besides the challenges faced by the Internet, wireless, and cellular networks, the IoT also faces storage, privacy, authentication, and management security issues [3].

With IoT, things can be monitored and controlled remotely from anywhere globally [4]. Anyone or any machine can do the monitoring and control of IoT services. Mobile devices, for example, can be used by homeowners to monitor the status of their homes. Using this simple example, we can see how IoT can become a source of new privacy and security-related challenges for data sensed, collected, and exchanged by IoT devices [5]. Several attacks can be used to compromise IoT deployments due to these challenges, resulting in an insecure IoT environment. Many IoT devices on the market require secure configuration. Requests and responses from a device to its server can leak an IoT device's identity. IoT devices can also be subjected to DDoS attacks, as explained by Doshi et al. [6] illustrated how IoT devices can also be attacked with DDoS attacks. It is possible to configure IoT devices as wireless access points, transporters, and metadata collectors to determine what information can be gathered without cleartext access. The use of cryptography in network and internet security has been around for a long time. Private data and information can be obscured and protected using cryptography by preventing unauthorized individuals or groups from accessing it. Cryptography makes data exchange and secure communications possible in typical networks.

This paper proceeds as follows: Section 2 presents the IoT concept. Section **??** analyses the critical areas of IoT security. Section 4 reviews the hierarchical architecture and lists IoT security threats for each layer. The concept of cryptography and its applications in IoT is investigated in Section 5; Meanwhile, we compare and evaluate different cryptography techniques in Section 6. Finally, this survey is concluded in Section 7.

2. IoT SECURITY

With the advent of IoT, several security challenges and threats come with it, including risks to devices, platforms, operating systems, communications, and systems they connect to. In the digital age, For the IoT platform and devices to be secure, there will be a need for technology against physical tampering and information attacks, encrypt their transmissions, and respond to contemporary challenges. Therefore, IoT is increasingly recognized as a potential target for invasions. IoT elements must be protected to ensure that data, sensors, and interfaces stay confidential, secure, and authentic. It is imperative to maintain data security throughout the lifecycle of generated information. Table 1 summarizes IoT's fundamental security objectives [7] as follows:

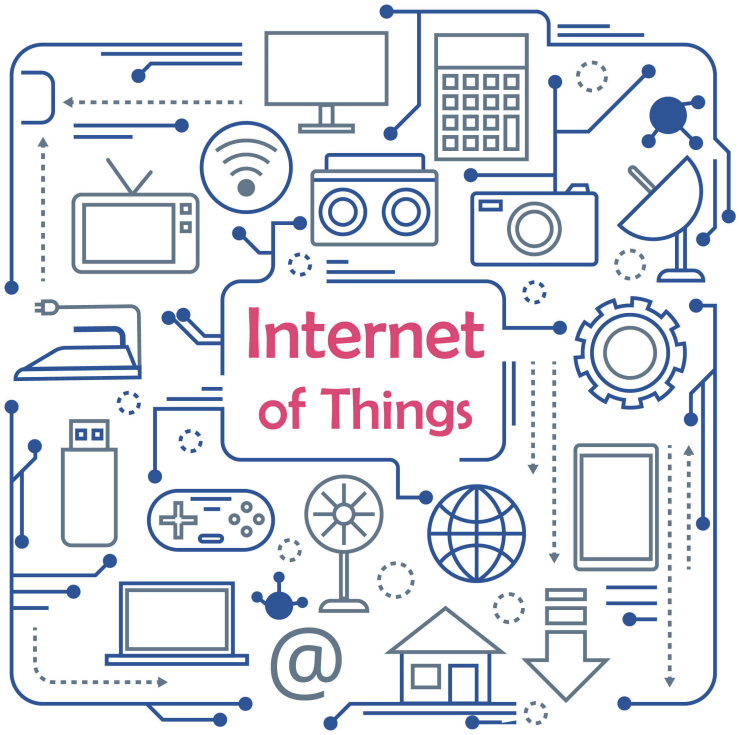

FIGURE 1. The concept of IoT.

- Confidentiality: Data security is crucial, and only authorized users should be able to access it. Sensors, for instance, must ensure that their collected data is not revealed to neighbours [8]. The management of data is another issue relating to confidentiality. IoT users need to know what data management mechanisms will be utilized, who will be responsible for the management, and what they can do to ensure that their data is secure and confidential [9].
- Integrity: In the Internet of Things, data is exchanged between a wide variety of devices, so it is crucial to guarantee the data accuracy, that it has come from a reputable source, and that there has been no interference during the transmission process, whether intentionally or unintentionally. It is possible to enforce the integrity feature of IoT communication by ensuring end-to-end security. Despite managing data traffic through firewalls and protocols, IoT nodes possess low computational power, making it difficult to guarantee security [10].

- The IoT requires that each object can authenticate and identify another. This process, however, may be challenging because of IoT's nature; there are many entities involved, and there are also times when objects have to interact for the first time (with objects they are unfamiliar with) [11]. Consequently, every interaction in the IoT requires a mechanism for authenticating entities.

TABLE 1. **IoT security objectives.**

Confidentiality	Intruders should not be able to intercept information transmitted between the nodes [12].
Integrity	Keep the information from being tempered [13].
Authentication	Information and systems should only be accessible to authorized users [14].

3. SECURITY CRITICAL APPLICATIONS FOR IOT

Security has been the key to almost all IoT applications' successful deployment. Almost all industries incorporate IoT into their operations as the applications increase rapidly. Operators need to provide a more rigorous level of security support for IoT applications, even though existing networking technologies support them. A variety of security-sensitive IoT applications are discussed in this section.

- Smart Cities: Creating smart cities is aimed at improving residents' life quality, by utilizing emerging technologies such as computation and communication [15]. For example, smart homes, traffic, and disaster management all fall under this umbrella. Governments around the globe are promoting smart cities through a variety of motivations [16]. Smart applications are designed to improve citizens' quality of life but threaten privacy. Citizens' card details and purchase behaviours are usually at risk when they use smart card services. There is a risk of users' location traces being leaked by smart mobile applications. Parental monitoring applications allow them to observe their children at all times. Children's safety can be at risk if such applications are hacked..
- Smart Environment: IoT applications in the smart environment include detecting forest fires, monitoring snow levels in high-altitude areas, monitoring pollution, preventing landslides, and detecting earthquakes [17]. Humans and animals in those areas are affected by all these IoT applications. National agencies will also use information gathered from these IoT applications. An IoT application can have serious consequences when it suffers a security breach or vulnerability [18]. These IoT applications are very susceptible to false positives and negatives. For example, the government and businesses may lose money if the application incorrectly detects earthquakes. Using an application that does not predict earthquakes can also result in property loss and lives. As a result, applications for smart environments must be precise, data non-tampering, and free of security breaches. .

- Smart Grids and Meters: Measuring, monitoring, and managing are all part of smart metering applications. One of the most common uses of smart meters is to measure and monitor electricity consumption through smart grids [19]. Moreover, it can be utilized to address the problem of electricity theft [20]. In addition to monitoring water levels, natural gas and petroleum levels in cisterns and tanks can also be controlled using smart meters. As part of the smart metering process, solar energy plants are also monitored to optimize their performance by rotating the solar panels to boost solar energy harvesting. The use of smart meters in IoT applications can be used for measuring water pressure in water transportation systems as well as measuring the weight of goods. Technically, analogue meters can only be physically tampered with, while cyber-attacks can occur on smart meters. As well as recording energy usage, it is possible to manage loads and costs with the help of smart meters in a smart home area network (HAN). Consumers or adversaries could intentionally interfere with these communication systems, resulting in monetary losses [1].
- Emergencies and security: Many IoT applications are used in the area of security and emergencies as well [21]. Among other things, it includes applications restricting access to restricted areas for authorized people. Detecting hazardous gas leaks around chemical factories or industrial areas is another application in this domain [22]. A cellular base station and nuclear reactors can also be monitored for radiation levels, and alerts can be generated [23]. Different buildings house sensitive goods or contain sensitive systems. Data and goods can be protected with security applications. The IoT can also prevent corrosion and breakdown in sensitive buildings by applying applications that detect liquids. There are also a variety of serious consequences that can result from security breaches in such applications. Criminals might attack these applications to gain access to restricted areas, for example. As well as immediate and long-term health risks, false radiation level alarms can be very dangerous. Radiation could result in serious fatal diseases in infants, for instance, if high levels are exposed to them [24].
- Smart Retail: Several retailers have recently launched smart services, improving customer service and efficiency [25]. As the goods move along the supply chain, the storage conditions of the products can be monitored using software applications. Also, IoT is used to enable warehouses to track goods in order to maximize restocking efficiency [26]. As part of developing intelligent shopping applications, customers' preferences, habits, and allergies to certain ingredients are taken into account. Online retailers can offer online shopping through augmented reality techniques. Various IoT applications have been deployed and used by retailers with security concerns. Morgan Chase, Apple, JP Home Depot and Sony are just some companies on the list [27]. Inventory of goods in the warehouse may be compromised by adversaries using IoT applications. To increase sales, they may need to provide users with accurate product information. Consider a scenario in which smart retail does not implement security features. Retailers and customers may lose money since attackers might steal customer information such as credit card details and contact information.

- Farming and agriculture: As part of smart agriculture, soil moisture is monitored, microclimate conditions are controlled, irrigation is selectively irrigated in dry regions, and humidity, temperature, and humidity are controlled [28]. Farmers can save monetary losses by utilizing such advanced features in agriculture. The production of seeds and vegetables could be prevented from contamination with fungi and other microorganisms if the right temperature and humidity grades were maintained. It is also possible to increase the yield and quality of vegetables and crops by controlling the weather [29]. Attaching sensors to farm animals makes monitoring their activities and health conditions possible, just as there are IoT applications for crop monitoring [30]. Animals may be stolen, and crops may be damaged if such applications are compromised.
- Home Automation: A popular and widely used application of IoT is home automation, which includes remote-controlling appliances to enhance energy consumption and protect from burglars [31]. Users are encouraged to monitor their energy and water consumption to save money and resources. Logic-based security algorithms have been proposed by Jose et al. [32] for enhancing home security. Various key locations in the home are monitored to detect intrusions by comparing the user's actions with their normal behaviour. However, the IoT devices in the home may be breached by attackers and used to harm their users. Using various home automation systems has rapidly increased the number of home burglaries. Furthermore, in the past, adversaries have used Internet traffic to judge the residents' behaviour and presence by analysing the types and flows of traffic in and out of the smart home.

4. INTERNET OF THINGS SECURITY THREATS

Four important layers make up an IoT ecosystem. The first layer includes acquiring data or information using actuators and sensors to perform various functions. An Internet-based communication network transmits the collected data in the second layer. To bridge the network and application layers, most IoT applications use a middleware layer as the third layer. Finally, the fourth layer consists of IoT-based end-to-end applications such as smart grids, transportation, and factories. The data is moved between these layers through various gateways. The gateways are subject to certain security risks. A few issues and security threats are associated with each layer of an IoT application. These four layers are illustrated in Figure 2.

This Subsection discusses these four layers, along with possible security threats. Figure 3 illustrates how these four layers can be attacked. Moreover, this section discusses how these layers are connected by gateways and the security issues that they raise.

4.1. **Issues Related to Security at Sensing Layer:**

Sensors and actuators are the primary components of the sensing layer. A sensor detects the physical phenomena around it [33, 34]. By contrast, actuators respond to the sensed data in the physical environment. In addition to ultrasonic and camera sensors, temperature and humidity sensors can also sense various data types. Various types of sensors can detect the physical environment, including mechanical, electrical, electronic, and chemical ones. Many types of sensing technologies are used in the Internet of

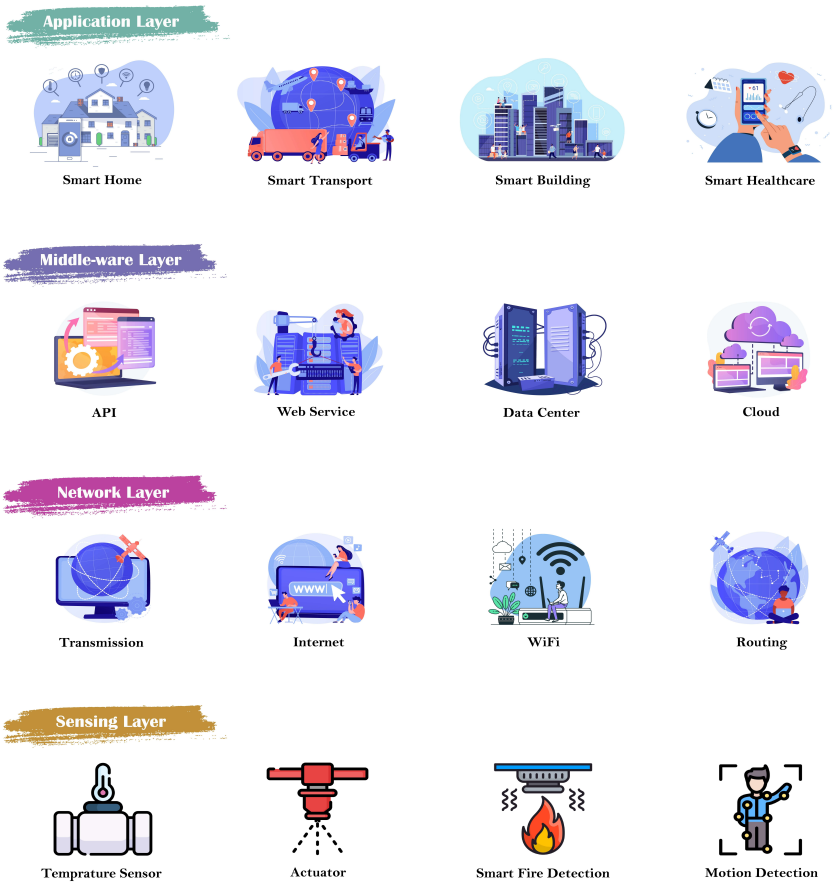

FIGURE 2. IoT multilayer architecture .

Things, including RFID, GPS, WSNs, and RSNs. A wide range of security threats can affect sensors, including:

- Node Capturing: Sensors and actuators are the low-power nodes that comprise IoT applications. An adversary can attack these nodes in several ways. Nodes in the IoT system may be captured or replaced with malicious nodes by attackers. An attacker might control a new node part of the IoT system, compromising its security [35].
- Injection of Malicious Code: By injecting malicious code into the node's memory, the attacker causes the network system to crash. It is common for IoT nodes to update their firmware or software over the air, allowing attackers to inject malicious code. An attacker may attempt to access an IoT system by using malicious code to manipulate the nodes to execute unintentional operations [36].

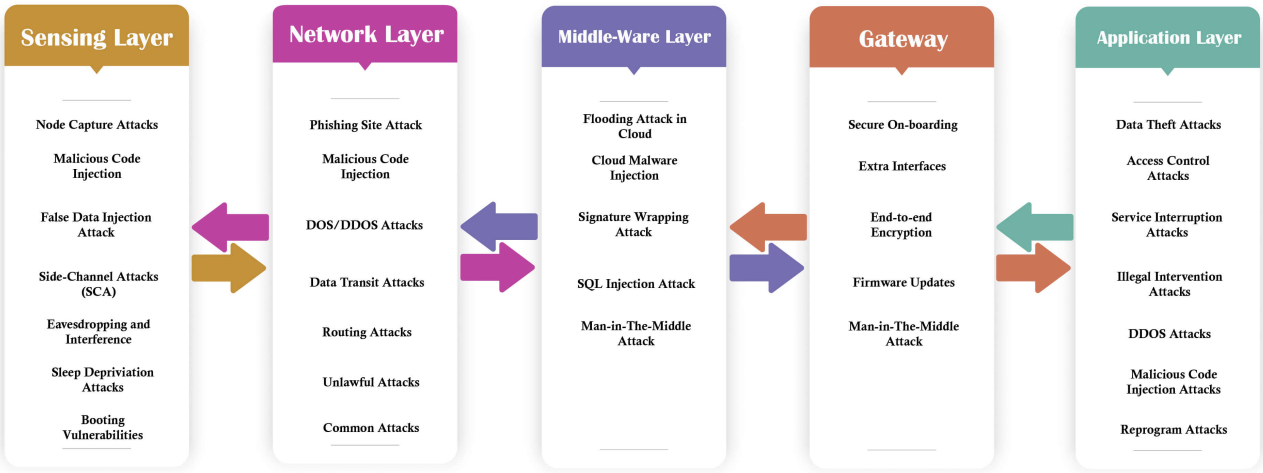

FIGURE 3. IoT multilayer architecture.

- Injection of false data: When the attacker captures the node, erroneous data may be injected into the application, leading to false results and malfunction [37]. Using this method, an attacker can also launch a DDoS attack.
- Attacks on side channels (SCA): It is also possible for sensitive data to be leaked through side-channel attacks as well as direct attacks on the nodes. Adversaries can obtain sensitive information from the microarchitecture of processors, electromagnetic emanation, and energy consumption [38]. Energy consumption is one form of side-channel attack. There are other types of attacks, such as laser-based and timing attacks. As cryptographic modules are implemented on modern chips, numerous countermeasures are taken to stop these side-channel attacks [39].
- Eavesdropping and Interference: Multi-node open environments are common in IoT applications [40]. Consequently, eavesdroppers can access these IoT applications. The data transmitted or authenticated through different transmission phases can be intercepted and captured by attackers.
- Sleep Deprivation Attacks: A low-powered IoT edge device can drain its battery in such attacks [41], resulting in a DoS from IoT nodes. In such an attack, malicious code can be used, or artificially inflated energy consumption can be employed.

- Booting Attacks: The inbuilt security processes on edge devices are not enabled during boot time, allowing various attacks to be carried out [42]. Attackers can be exploit restarting the node devices for penetration. Due to the low power of edge devices and the fact that they can sometimes sleep-wake, it is crucial to ensure the boot process security in them.

4.2. **Issues Related to Security at Network Layer:**

As sensing tier information is transmitted to the computing units through the network layer, it is a key component of the computation layer. At the network layer, there are several key security problems:

- Phishing Site Attack: Attackers often use phishing to target multiple IoT devices with little effort. A few devices are expected to be affected by the attack. While visiting a web page, users may encounter phishing websites. The entire IoT environment the user uses becomes vulnerable If the password or account of the user is disarranged. Phishing site attacks are highly prevalent in the IoT network layer [43].
- Access Attack: A network access attack occurs when someone unauthorized or an attacker obtains a network, also known as an advanced persistent threat (APT). Long periods can pass without the attacker being detected on the network. An attack of this type is less likely to damage a network than to steal valuable data or information. A vulnerability to such attacks exists due to IoT devices' continuous collection and transfer of valuable data [44].
- DDoS/DoS Attack: It involves bombarding the target server with numerous undesirable requests, crippling it, and disrupting real users' use. Distributed denial of service is a distributed attack that uses multiple sources to flood the target server with traffic [45]. IoT applications are not immune to such attacks, but IoT networks are vulnerable to such attacks due to their heterogeneity and complexity. Attackers can launch DDoS attacks on target servers easily using IoT devices in IoT applications that are not firmly configured. In the Mirai botnet attack, the IoT devices that were weakly configured continuously propagated requests, resulting in the blocking of various servers [46].
- Data Transit: It is common for IoT applications to store and exchange large amounts of data. Understandably, hackers and other adversaries are always interested in data because of its value. Local or cloud-based data storage can pose a security risk. However, data in transit or on the move is even more susceptible to cyber-attacks [47]: sensors, actuators, and the cloud all exchange data in IoT applications. Data movements involve different connection technologies; data breaches can compromise IoT applications.
- Routing Attacks: Data routing paths may be redirected during data transit by manipulated nodes in IoT applications. Sinkhole attacks occur when adversaries advertise an artificially shortest routing path and attract nodes to route traffic toward it [48]. Another serious security threat is worm-hole attacks, which can be combined with sinkhole attacks to create a serious security threat. Out-of-band connections are used to transfer packets quickly between two nodes. A wormhole can be created between a compromised device and an internet-connected node, allowing attackers to circumvent primary protection protocols in IoT applications [49].

4.3. **Issues Related to Security at Middleware Layer:**

Middleware, a layer between the network and application layers, plays a critical role in the Internet of Things. Computing and storage functionalities can be provided by middleware [50]. To meet the application layer's demands, this layer provides APIs. A middleware layer includes a broker, a persistent data store, a queueing system, and machine learning systems. Despite the middleware layer's ability to provide an IoT application with reliability and robustness, it can also be vulnerable to several attacks. A middleware infection can allow these attacks to take over the entire IoT application. Security challenges are associated with databases and the cloud at the middleware layer. We discuss possible middleware attacks in the following manner:

- Man-in-the-Middle Attack: By eavesdropping or pretending to be a legitimate participant, attackers use man-in-the-middle attacks to intercept existing conversations or data transfers. The attacker will appear to be part of a normal information exchange with the victim but can quietly intercept and steal information by inserting themselves "middle" between the two parties [51]. The attacker controls all communications with the clients without the clients' knowledge as long as he/she controls the broker.
- SQL Injection: Similarly, middleware can be impacted by SQL Injection (SQLi). A program can contain a malicious SQL statement. [52, 53], allowing the attacker to obtain a user's private information and even change the database records [54]. SQLi has been listed among the top threats to web security by the Open Web Application Security Project (OWASP) 2018 [55].
- Signature Wrapping Attack: Web services rely on XML signatures in middleware [56]. Attackers exploit SOAP vulnerabilities (Simple Object Access Protocol) to engage in signature wrapping attacks. By doing so, they can modify eavesdropped messages or execute operations on the stolen data [57].
- Cloud Malware Injection: Attackers can manipulate the cloud to create malware, inject malicious code, and create virtual machines through cloud malware injection [58]. The attacker creates a malicious service module or a virtual machine instance by pretending to be a good service. An attacker can capture sensitive data by accessing the victim's requests and modifying the data if needed.
- Flooding Attack: Attacks of this nature are similar to DoS attacks and negatively impact the quality of service (QoS). As a result of the attacker's repeated requests, cloud resources are depleted [59]. A large amount of load is added to cloud servers by these attacks, which can significantly impact cloud systems.

4.4. **Issues Related to Security at Gateways:**

There are many different gateways connecting devices, people, things, and cloud services. Hardware and software solutions are also provided through gateways for IoT devices. Decryption and encryption of IoT data are handled by gateways, whose communication protocols are translated between different layers [60]. Many IoT platforms are deployed today, such as LoraWan, ZigBee, Z-Wave, and TCP/IP stacks, with various gateways interconnecting them. IoT gateway security challenges include:

- Secure On-boarding: Network protocols provide security mechanisms that can be used once devices have been set up. Typically, secure onboarding is the process involved in this process.

New devices that are being introduced to the network are authenticated during secure onboarding, and credentials for communicating securely with other network devices are provided [61]. It is possible to capture encryption keys via 'man in the middle' attacks and eavesdropping on gateways, especially during onboarding.

- Extra Interfaces: Installation of IoT devices should be conducted with a focus on minimizing the attack surface [62]. Embedding only the necessary protocols and interfaces in an IoT gateway is recommended. In order to prevent backdoor authentication or unauthorized access to information, some services and features must be prohibited for end users.
- End-to-End Encryption: For data confidentiality, it is essential to ensure end-to-end application layer security [63]. Only the unique recipient of the encrypted message must be able to decrypt it. It is important to note, however, that Zwave and Zigbee protocols do not support end-to-end encryption since gateways must decrypt and re-encrypt messages to translate information between the protocols. It is possible to compromise the data when decrypted at the gateway level.
- Firmware updates: It has become increasingly important to update the firmware of your device to defend against endless attacks [64]. In IoT devices, firmware updates cannot be downloaded and installed because of resource constraints. Firmware updates are generally applied through gateways. The validity of signatures and records of firmware versions is essential for the security of firmware updates.

4.5. **Issues Related to Security at Application Layer:**

Providing services to end users is the responsibility of the application layer. This layer includes a smart home, a smart meter, an intelligent city, and a smart grid. As a result of the specific security issues this layer has, such as data theft and privacy issues, it is more vulnerable than other layers. Different applications also pose specific security challenges in this layer. In addition, many IoT applications utilize a middleware layer or application support layer between the network and application layers. Business services are supported by the support layer, which helps allocate and compute resources intelligently. The application layer encounters the following security issues:

- Data Thefts: Data collected and stored by IoT applications are often sensitive and private. In IoT applications, there is a lot of data movement, and data in transit is even more vulnerable to attacks [65]. Users will avoid registering their private data in IoT applications vulnerable to data theft. Several techniques and protocols are used in IoT applications to protect data from unauthorized access. These include encryption, isolation, authentication, and privacy management [66].
- Access Control Attacks: Data or accounts are protected by access control mechanisms that only allow access to authorized users or processes. IoT applications become vulnerable when access control is compromised, which becomes a major concern in IoT applications [67].
- Service Interruption Attacks: The existing literature also refers to these attacks as DDoS attacks or illegal interruption attacks. Such attacks have been reported on IoT applications in various instances. In this attack, servers and networks are artificially overloaded, making it impossible for legitimate users to use IoT applications [68].

- Malicious Code Injection: An attacker usually attempts to access a system or network through the simplest possible method. As a result of insufficient code checks, an attacker would begin by attacking the system's vulnerability to malicious scripts and misdirections. The most common way attackers inject malicious scripts into trusted websites is through XSS (cross-site scripting). IoT systems can be paralyzed, and their accounts hijacked by XSS attacks [69].
- Sniffing Attacks: As long as sufficient security protocols are not implemented, attackers may be able to sniff IoT network traffic and access confidential user data. [70].
- Reprogram Attacks: Without a protected programming process, attackers can reprogramme the object remotely and hijack the IoT network [71].

5. FIREWALL

There may be traffic entering or exiting the network from unauthorized sources, so it should not be allowed. It is advisable to block traffic from reaching its destination if it is not for an authorized purpose [72]. The traffic on the network may not be within the boundaries of what is considered normal or acceptable, so it should be dropped before it compromises the network. Firewalls are responsible for all these protections. Just like the firewall in a vehicle's engine compartment protects the passengers from harm in case of an accident, a firewall is intended to prevent damage. For network communication access control, either hardware or software firewalls are deployed. As a result, firewalls prevent malicious exploits, incursions, data, messages, or events from entering the network [73]. A firewall is nothing more than a device that enforces access control policies.

A firewall allows a network to define access control requirements, ensuring that only traffic meeting those requirements can traverse or access the protected system. As illustrated in Figure 4, a firewall only permits traffic to access protected resources if it has been authorized to do so.

Is there a need for a firewall? Firewalls determine whether to forward network traffic based on defined rules as it passes through them [74]. When installing a firewall, it is important to screen outgoing traffic and traffic entering the network. In most cases, a firewall is installed at the point where the internal network and the Internet are connected. Firewalls can be placed between different parts of the network depending on the level of security required, but most firewalls process traffic between an internal network and the Internet. Thousands of computers may be connected to this internal network. Firewalls commonly include the following features:

(a) Incoming network traffic can be blocked based on its source or destination: A firewall's most common feature is blocking unwanted incoming traffic [75, 76].
(b) Filter outgoing traffic based on source or destination: Employees should be prevented from accessing inappropriate websites, for example.
(c) Content-based network traffic blocking: A more advanced firewall can filter out unacceptable content from network traffic [77]. The firewall can, for instance, prevent viruses from entering the network if it is integrated with a virus scanner. E-mail screening capabilities can also be incorporated into firewalls to prevent unwanted e-mail messages.

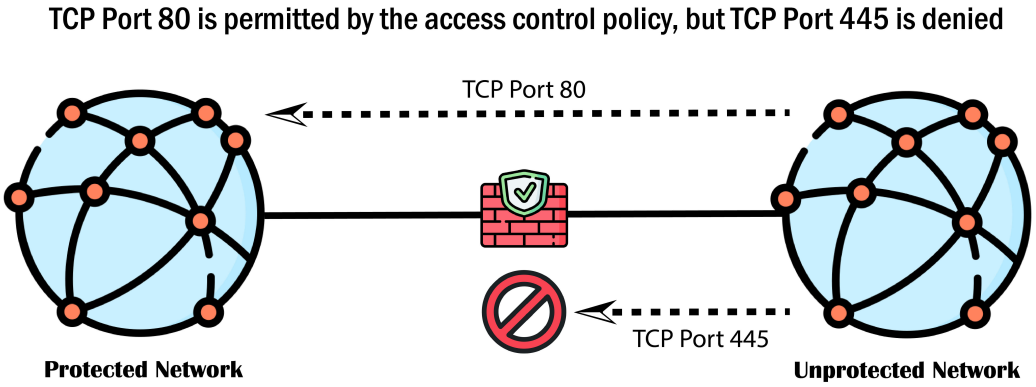

FIGURE 4. The firewall's operation.

(d) Make internal resources available: As well as preventing unwanted network traffic from passing through a firewall, many firewalls can also be configured to allow selective access to internal resources, such as public web servers, but to prevent other Internet users from accessing the internal network from the outside.
(e) Allow connections to the internal network: Connecting to a network is commonly accomplished through virtual private networks (VPNs). A VPN allows secure connections between a corporate network and the Internet [78]. Connecting to a corporate network can be accomplished through a VPN, for example, by telecommuters or traveling salespeople. It is also common for branch offices to be connected via VPNs. VPN connections can be easily established with some firewalls that include VPN functionality
(f) Activity reports on firewalls and network traffic: The network administrator should also know how the firewall handles network traffic to and from the Internet, who has attempted to break into the network, and who has accessed inappropriate materials online. It is common for firewalls to include some reporting mechanisms [79].

According to their size, firewalls are usually classified into one of the following categories:

- Departmental or small organization firewall: These firewalls protect all the computers in a small, single-location office [81]. To screen network traffic for a limited number of computers, firewalls in this category offer sufficient reporting and management capabilities.
- Enterprise firewall: Large organizations with diverse geographically dispersed users can benefit from enterprise firewalls [82]. User management tools allow the configuration of multiple firewalls simultaneously. Reporting capabilities include consolidated reports for multiple firewalls.

A brief overview of six popular firewalls is presented here. These firewalls are also discussed in terms of their advantages and disadvantages.

(1) An application-based firewall controls network access by allowing or denying certain applications [83]. Records can be kept of who attempted to get in and what was done by those who received access.
   - Advantages:
     (i) Internal and external hosts cannot communicate directly.
     (ii) User authentication is supported.
     (iii) Performs an analysis of the application commands within the data packet payload.
     (iv) Traffic and specific activities can be logged comprehensively.
   - Disadvantages:
     (i) The overhead introduced by this approach is higher than that of other approaches.
     (ii) Internal clients should be known.
     (iii) All connection types are not allowed.

(2) An easy-to-implement firewall is packet filtering. By comparing packet content with predefined specifications, routers can filter packets. Besides IP addresses, subnets, and TCP or UDP port numbers, combinations of these properties can also be used to access or deny access [84].
   - Advantages:
     (i) Among the firewall technologies, packet filtering is the easiest to configure.
     (ii) A wide variety of commercial and free routing products offer packet filtering capabilities.
     (iii) There is little or no performance overhead associated with adding a packet filter to a router.
     (iv) The packet filter can protect all applications since it operates at the network and transport layers.
     (v) All networks can be protected with one screening router.
   - Disadvantages:
     (i) Packet filters are susceptible to a wide variety of compromises. Would-be intruders can make incoming packets appear that they were sent from a trusted source by deceptively masking their origins.
     (ii) Router performance decreases as packet filtering complexity increases. Caching strategies commonly used for performance optimization can be incompatible with some filtering strategies.
     (iii) Normal packet filtering routers cannot easily enforce some policies.

(3) Packet filtering technology is enhanced by stateful inspection. Stateful inspection examines packet content and multipacket flow attributes [76].
   - Advantages:

(i) Throughput is high with low overhead. By comparing stateful inspection to packet filtering, stateful inspection offers enhanced security without degrading performance notably.
(ii) Additionally, it works at the transport layer and the network layer. Therefore, there are no special client configurations or client software requirements.
(iii) The hole in the Network Perimeter is only open for a short period. Dynamic packet filters are much more difficult to exploit than static packet filters due to the significantly reduced time it takes to open a hole in the perimeter. Due to the small amount of work performed outside of routing traffic, the overhead is relatively low. Consequently, dynamic packet filtering techniques are typically more efficient than application gateways on similar hardware platforms.
(iv) A wide variety of services can be provided (e.g., back-channel services (e.g., File Transport Protocol (FTP) must be handled as a special case). It can be set up so that packet filters allow IP traffic from any application to pass through a firewall since they are application independent.

- Disadvantages:
  (i) Provides direct IP connections between external clients and internal hosts. It is still possible for external systems to connect to internal machines under the firewall's control, even with dynamic packet filtering. An attacker can exploit any exploitable weakness in the host's software or configuration once the gateway has granted access to that host on the internal network. Those internal hosts may be accessed from other internal hosts only if their security allows it.
  (ii) Users must authenticate via an application gateway (if user authentication is supported, it must be handled by an application gateway).
  (iii) Packet filtering requires less administration than this type of firewall. (To determine access or denial actions, a connection table must track each packet flow. This information is compared to present policies, and the most appropriate action is taken.

(4) The proxy links the internal servers and servers on the Internet. Clients within the internal network use the proxy server to receive incoming data. As a client, the proxy sends data to databases on an external network for outgoing data [85].

- Advantages:
  (i) It provides the highest level of security and granularity since it operates at the application layer.
  (ii) Logging is one of the benefits of proxy services.
  (iii) It is possible to cache data using proxy services.
  (iv) Intelligent filtering is possible with proxy services.
  (v) Users can be authenticated through proxy systems.
  (vi) Proxy systems automatically protect weak or faulty IP implementations.
- Disadvantages:
  (i) There is much complexity involved in configuring this firewall.

(ii) Proxy servers act as relay agents, potentially causing performance bottlenecks.
(iii) Proxy software is widely available for older and easier services like FTP and telnet. However, it is more difficult to locate reliable software for newer or less commonly used services.
(iv) Depending on the proxy service, different servers may be required.
(v) Clients, applications, and procedures generally need to be modified when using proxy servers.

(5) When dealing with external networks, a network can use one set of network addresses internally and another set externally. In addition to concealing internal network layouts, network address translation forces connections to go through choke points. It will not be possible to connect to an untranslated address. The translation is done at the choke point [86].
- Advantages:
  (i) The firewall enforces its control over outbound connections by translating network addresses.
  (ii) Incoming traffic can be restricted with network address translation.
  (iii) By translating network addresses, internal network configurations can be hidden.
- Disadvantages:
  (i) By translating network addresses, internal network configurations can be hidden.
  (ii) Embedded IP addresses complicate network address translation.
  (iii) Some encryption and authentication systems are affected by network address translation.
  (iv) Logging is interfered with by dynamically allocated addresses.
  (v) It may not be easy to filter packets when ports are dynamically allocated.

(6) Virtual private networks (VPNs) employ encryption and integrity protection so that you can use public networks (such as the Internet) as if they were private networks (such as a small network you control) [87].
- Advantages:
  (i) Virtual private networks provide encryption.
  (ii) It is only possible to secure protocols over the Internet with virtual private networks.
- Disadvantages:
  (i) Setting up a private, high-speed connection is much more expensive than connecting two sites to a public high-speed network. Implementing a truly private network is often cost-inhibitive, even though it is more secure.
  (ii) There are dangers associated with virtual private networks.

6. IoT AND FIREWALLS

However, IoT devices can be just as valuable to attackers even though they are much more vulnerable than traditional computing devices. When applying traditional security measures to IoT environments, it is necessary to consider various factors. Due to the limited local resources on IoT devices, today's

intrusion detection software cannot be physically run on these devices. An IoT solution that works for all devices will not work due to the lack of consistency in low-level protocols, such as how devices receive updates. A final reason companies skip security precautions and testing procedures are market pressures to manufacture cheap devices and beat competitors to the market [88]. In a zombie attack, an IoT device may serve as a bot for an attacker once it has been compromised, allowing them to carry out further attacks on the local network. It has two main differences from traditional computing devices regarding IoT network security. Due to the wide deployment possibilities of IoT devices, network security solutions must support thousands of unique devices communicating inside and outside the network. Second, these devices generate unique traffic patterns on the network because they serve different purposes. Some of the challenges we present can be solved by existing IoT network security solutions; however, only a select few can handle both the scalability and heterogeneity of traffic generated by IoT devices.

IoT firewalls are a relatively new area, and so far, not many firewalls have been introduced, but the following are briefly discussed

- **F-Secure SENSE**: Users' home network is more secure with the SENSE. A network scan is conducted by connecting to the home router [89]. In addition to F-Secure's Secure Cloud, SENSE has access to its database of viruses and threats. The device sends an alert to the controlling device if it notices suspicious activity within the library or identifies a virus or threat. Mobile devices and computers can be installed with SENSE, the devices that receive alerts. Visit `www.f-secure.com` to learn more about SENSE.
- **Luma Wi-Fi router**: The manufacturer claims it monitors traffic for suspicious activity and malware-like behaviour and quarantines infected devices [90]. The router can be purchased from `www.lumahome.com`. There has not been much positive feedback for this device, which appears to be expensive compared to other devices.
- **Dojo**: An Ethernet cable connects Dojo-Labs' device to the router, which is extremely easy to use. Dojo acts as a gatekeeper for the home network. In addition to monitoring incoming and outgoing traffic, the device allows users to analyse and browse network traffic and profile network devices when configuring the device [91]. Apps are designed to send alerts when detecting abnormal behaviour or problems. Furthermore, a 'glowing-rock gadget' is included to help make the device visible throughout the house. It glows green, orange, or red based on the security level of the home network. Interested parties can purchase the device on the Dojo Labs website.
- **Cujo**: Besides having an easy-to-use interface, Cujo is equipped with antivirus, firewall, malware prevention technology, and deep packet inspection [92]. The crowdfunding campaign for Cujo funded the Cloud-connected device. It looks like a coffee mug, activates automatically on the router if plugged in, and does not require a different setup. A simple app is used to manage it. Monthly or annual subscriptions are available. Getting Cujo is as easy as visiting `www.getcujo.com`.

7. Conclusion

Home-network scenarios connect many internet-connected IoT devices (the things). Most of them are low-powered sensors with limited computing capabilities. They may therefore need more costly encryption protocols. Cloud services can be sniffed by adversaries, reconstructed, and potentially exposed to sensitive information. The cost of security must also be reduced for many companies. The things may come with default credentials which a naive user may keep the same. These factors lead to potential security risks, which are mitigated through security technologies, including firewalls. Most popular firewalls were not originally designed for devices with certain limitations, such as limited storage, low processing power, or a small battery. In the last decade, research on IoT firewalls has increased due to IoT devices having restrictions that might make some algorithms unviable. IoT firewalls have become a hot topic in the field of IoT security.

References

[1] J. Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, Towards the internet of things. Springer, 2020.

[2] B. Russell and D. Van Duren, Practical internet of things security. Packt Publishing Ltd, 2016.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721-82743, 2019.

[4] G. Mustafa, R. Ashraf, M. A. Mirza, and A. Jamil, "A review of data security and cryptographic techniques in IoT based devices," in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, 2018, pp. 1-9.

[5] J. M. Carracedo et al., "Cryptography for security in IoT," in 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, 2018: IEEE, pp. 23-30.

[6] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in 2018 IEEE Security and Privacy Workshops (SPW), 24-24 May 2018 2018, pp. 29-35, doi: 10.1109/SPW.2018.00013.

[7] H. Damghani, H. Hosseinian, and L. Damghani, "Cryptography review in IoT," in 2019 4th Conference on Technology In Electrical and Computer Engineering (ETECH2019), 2019.

[8] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, pp. 1-6, 2015.

[9] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Computer, vol. 44, no. 9, pp. 51-58, 2011, doi: 10.1109/MC.2011.291.

[10] T. N. Minh, "Confidentiality and integrity for IoT/mobile networks," Recent Trends in Communication Networks, p. 25, 2019.

[11] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013/07/05/ 2013, doi: https://doi.org/10.1016/j.comnet.2012.12.018.

[12] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," in 2012 International Conference on Computer Science and Electronics Engineering, 23-25 March 2012 2012, vol. 3, pp. 648-651, doi: 10.1109/ICCSEE.2012.373.

[13] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 17-31, 2015/09/01/ 2015, doi: https://doi.org/10.1016/j.adhoc.2015.01.006.

[14] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: a security framework for the Internet of Things," Security and Communication Networks, vol. 9, no. 16, pp. 3083-3094, 2016, doi: https://doi.org/10.1002/sec.1259.

[15] A. Gharaibeh et al., "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," IEEE Communications Surveys Tutorials, vol. 19, no. 4, pp. 2456-2501, 2017, doi: 10.1109/COMST.2017.2736886.

[16] D. Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," IEEE Communications Surveys Tutorials, vol. 20, no. 1, pp. 489-516, 2018, doi: 10.1109/COMST.2017.2748998.
[17] S. L. Ullo and G. R. Sinha, "Advances in smart environment monitoring systems using IoT and sensors," Sensors, vol. 20, no. 11, p. 3113, 2020.
[18] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A review of security standards and frameworks for IoT-based smart environments," IEEE Access, vol. 9, pp. 121975-121995, 2021.
[19] X. Xia, Y. Xiao, and W. Liang, "ABSI: An Adaptive Binary Splitting Algorithm for Malicious Meter Inspection in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 445-458, 2019, doi: 10.1109/TIFS.2018.2854703.
[20] S. I. Gerasopoulos, N. M. Manousakis, and C. S. Psomopoulos, "Smart metering in EU and the energy theft problem," Energy Efficiency, vol. 15, no. 1, p. 12, 2022/01/28 2022, doi: 10.1007/s12053-021-10011-y.
[21] D. G. Costa et al., "A Survey of Emergencies Management Systems in Smart Cities," IEEE Access, vol. 10, pp. 61843-61872, 2022, doi: 10.1109/ACCESS.2022.3180033.
[22] A. Rajbanshi, D. Das, V. Udutalapally, and R. Mahapatra, "dLeak: An IoT-Based Gas Leak Detection Framework for Smart Factory," SN Computer Science, vol. 3, no. 4, p. 273, 2022/05/05 2022, doi: 10.1007/s42979-022-01181-2.
[23] M. Saifullah, I. S. Bajwa, M. Ibrahim, and M. Asghar, "IoT-Enabled Intelligent System for the Radiation Monitoring and Warning Approach," Mobile Information Systems, vol. 2022, p. 2769958, 2022/12/20 2022, doi: 10.1155/2022/2769958.
[24] V. Tran-Quang and H. Dao-Viet, "An internet of radiation sensor system (IoRSS) to detect radioactive sources out of regulatory control," Scientific Reports, vol. 12, no. 1, p. 7195, 2022/05/03 2022, doi: 10.1038/s41598-022-11264-y.
[25] C.-Y. Lin, "Understanding consumer perceptions and attitudes toward smart retail services," Journal of Services Marketing, vol. 36, no. 8, pp. 1015-1030, 2022.
[26] M. G. Khan, N. U. Huda, and U. K. U. Zaman, "Smart warehouse management system: Architecture, real-time implementation and prototype design," Machines, vol. 10, no. 2, p. 150, 2022.
[27] N. N. Dlamini and K. Johnston, "The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review," in 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), 28-29 Nov. 2016 2016, pp. 430-436, doi: 10.1109/ICACCE.2016.8073787.
[28] B. B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of Internet of Things in smart agriculture: A survey," Future Generation Computer Systems, vol. 126, pp. 169-184, 2022/01/01/ 2022, doi: https://doi.org/10.1016/j.future.2021.08.006.
[29] V. K. Quy et al., "IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges," Applied Sciences, vol. 12, no. 7, p. 3396, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/7/3396.
[30] T. Vigneswari and N. Vijaya, "Smart livestock management using cloud IoT," Cloud IoT Syst. Smart Agric. Eng, vol. 1, pp. 55-74, 2022.
[31] N. Satheeskanth, S. D. Marasinghe, R. M. L. M. P. Rathnayaka, A. Kunaraj, and J. Joy Mathavan, "IoT-Based Integrated Smart Home Automation System," in Ubiquitous Intelligent Systems, Singapore, P. Karuppusamy, I. Perikos, and F. P. García Márquez, Eds., 2022// 2022: Springer Singapore, pp. 341-355.
[32] A. C. Jose and R. Malekian, "Improving Smart Home Security: Integrating Logical Sensing Into Smart Home," IEEE Sensors Journal, vol. 17, no. 13, pp. 4269-4286, 2017, doi: 10.1109/JSEN.2017.2705045.
[33] Bridgera. https://bridgera.com/sensors-and-actuators-in-iot/ (accessed).
[34] Smarthomeblog. https://smarthomeblog.net/smart-smoke-detector/ (accessed.
[35] K. S. K, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, "Security Enhancements to System on Chip Devices for IoT Perception Layer," in 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), 18-20 Dec. 2017 2017, pp. 151-156, doi: 10.1109/iNIS.2017.39.
[36] B. Yong, X. Liu, Q. Yu, L. Huang, and Q. Zhou, "Malicious Web traffic detection for Internet of Things environments," Computers Electrical Engineering, vol. 77, pp. 260-272, 2019/07/01/ 2019, doi: https://doi.org/10.1016/j.compeleceng.2019.06.008.

[37] J. Giraldo, M. E. Hariri, and M. Parvania, "Decentralized Moving Target Defense for Microgrid Protection Against False-Data Injection Attacks," IEEE Transactions on Smart Grid, vol. 13, no. 5, pp. 3700-3710, 2022, doi: 10.1109/TSG.2022.3176246.

[38] C. Liptak, S. Mal-Sarkar, and S. A. Kumar, "Power Analysis Side Channel Attacks and Countermeasures for the Internet of Things," in 2022 IEEE Physical Assurance and Inspection of Electronics (PAINE), 2022: IEEE, pp. 1-7.

[39] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," Sensors, vol. 22, no. 9, p. 3520, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/9/3520.

[40] C. H. Liao, H. H. Shuai, and L. C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," in 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 12-15 Jan. 2018 2018, pp. 1-2, doi: 10.1109/CCNC.2018.8319297.

[41] Y. Alotaibi and M. Ilyas, "Security risks in internet of things (IoT): a brief survey," in Proceedings of the 26th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2022), 2022, pp. 1-5.

[42] R. Wang and Y. Yan, "A Survey of Secure Boot Schemes for Embedded Devices," in 2022 24th International Conference on Advanced Communication Technology (ICACT), 13-16 Feb. 2022 2022, pp. 224-227, doi: 10.23919/ICACT53585.2022.9728840.

[43] APWG. https://apwg.org/trendsreports/ (accessed).

[44] C. Li and C. Chen, "A multi-stage control method application in the fight against phishing attacks," Proceeding of the 26th computer security academic communication across the country, p. 145, 2011.

[45] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: A systematic review," Soft Computing, pp. 1-37, 2022.

[46] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80-84, 2017.

[47] C. Silpa, G. Niranjana, and K. Ramani, "Securing Data from Active Attacks in IoT: An Extensive Study," in Proceedings of International Conference on Deep Learning, Computing and Intelligence: ICDCI 2021, 2022: Springer, pp. 51-64.

[48] A. Bilal, S. M. N. Hasany, and A. H. Pitafi, "Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices," IET Communications, vol. 16, no. 8, pp. 845-855, 2022.

[49] S. A. Bhosale and S. S. Sonavane, "Wormhole Attack Detection System for IoT Network: A Hybrid Approach," Wireless Personal Communications, vol. 124, no. 2, pp. 1081-1108, 2022/05/01 2022, doi: 10.1007/s11277-021-09395-y.

[50] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for internet of things," in Recent trends in wireless and mobile networks: Springer, 2011, pp. 288-296.

[51] K. S, V. S, A. Singh, R. A, H. Saxena, and S. S. S, "Detection and Mitigation of Man-in-the-Middle Attack in IoT through Alternate Routing," in 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 29-31 March 2022 2022, pp. 341-345, doi: 10.1109/ICCMC53470.2022.9753832.

[52] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in 2009 International symposium on computer network and multimedia technology, 2009: IEEE, pp. 1-4.

[53] R. Dorai and V. Kannan, "SQL injection-database attack revolution and prevention," J. Int'l Com. L. Tech., vol. 6, p. 224, 2011.

[54] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," IEEE Internet of things journal, vol. 3, no. 1, pp. 70-95, 2015.

[55] Acunetix. https://www.acunetix.com/vulnerabilities/web/tag/insecure-deserialization/ (accessed).

[56] J. Kumar, B. Rajendran, B. Bindhumadhava, and N. S. C. Babu, "XML wrapping attack mitigation using positional token," in 2017 International conference on public key infrastructure and its applications (PKIA), 2017: IEEE, pp. 36-42.

[57] WS-Attacks. https://www.ws-attacks.org/XML_Signature_Wrapping (accessed).

[58] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," Mobile Networks and Applications, 2022/03/14 2022, doi: 10.1007/s11036-022-01937-3.

[59] B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers," Computers Electrical Engineering, vol. 98, p. 107726, 2022.

[60] citrix. https://www.citrix.com/blogs/2015/07/24/securing-the-IoT-gateway/"(accessed)

[61] F. Kohnhäuser, S. Grüner, and J. Heuschkel, "Secure Onboarding of IIoT Devices using OPC UA," in 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), 2022: IEEE, pp. 1-4.

[62] A. Stanciu, T.-C. Balan, C. Gerigan, and S. Zamfir, "Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm," in 2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP), 2017: IEEE, pp. 1001-1006.

[63] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," ieee access, vol. 6, pp. 24639-24649, 2018.

[64] W.-J. Tsaur, J.-C. Chang, and C.-L. Chen, "A Highly Secure IoT Firmware Update Mechanism Using Blockchain," Sensors, vol. 22, no. 2, p. 530, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/2/530.

[65] W. Bekri, T. Layeb, J. Rihab, and L. C. Fourati, "Intelligent IoT Systems: security issues, attacks, and countermeasures," in 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022: IEEE, pp. 231-236.

[66] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," IEEE Access, vol. 8, pp. 131723-131740, 2020.

[67] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M. H. Yang, "A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems," IEEE Access, vol. 8, pp. 139244-139254, 2020, doi: 10.1109/ACCESS.2020.3012121.

[68] S. B. B. Priyadarshini, S. K. Dash, A. Sahani, B. K. Mishra, and M. P. Nath, "An Introduction to Security in Internet of Things (IoT) and Big Data," A Roadmap for Enabling Industry 4.0 by Artificial Intelligence, pp. 169-200, 2022.

[69] P. Chaudhary, B. B. Gupta, and A. K. Singh, "Securing heterogeneous embedded devices against XSS attack in intelligent IoT system," Computers Security, vol. 118, p. 102710, 2022/07/01/ 2022, doi: https://doi.org/10.1016/j.cose.2022.102710.

[70] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in 2017 International conference on i-SMAC (iot in social, mobile, analytics and cloud)(i-SMAC), 2017: IEEE, pp. 477-480.

[71] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018.

[72] S. Ali, "Using Firewalls," in Computer Network Security: Wiley, 2020, pp. 79-100.

[73] H. Abie, "An overview of firewall technologies," Telektronikk, vol. 96, no. 3, pp. 47-52, 2000.

[74] M. S. Desai, T. C. Richards, and T. von der Embse, "System insecurity–firewalls," Information management computer security, 2002.

[75] B. S. Rawal, G. Manogaran, and A. Peter, "Firewalls," in Cybersecurity and Identity Access Management: Springer, 2022, pp. 117-128.

[76] J. Liang and Y. Kim, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 26-29 Jan. 2022 2022, pp. 0752-0759, doi: 10.1109/CCWC54503.2022.9720435.

[77] P. C. van Oorschot and P. C. van Oorschot, "Firewalls and Tunnels," Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, pp. 281-308, 2021.

[78] M. Pudelko, P. Emmerich, S. Gallenmüller, and G. Carle, "Performance analysis of VPN gateways," in 2020 IFIP Networking Conference (Networking), 2020: IEEE, pp. 325-333.

[79] M. M. Ghonge, S. Pramanik, R. Mangrulkar, and D. N. Le, Cyber Security and Digital Forensics: Challenges and Future Trends. Wiley, 2022.

[80] A. Voronkov, L. H. Iwaya, L. A. Martucci, and S. Lindskog, "Systematic literature review on usability of firewall configuration," ACM Computing Surveys (CSUR), vol. 50, no. 6, pp. 1-35, 2017.
[81] B. Komar, R. Beekelaar, and J. Wettern, Firewalls for dummies. John Wiley Sons, 2003.
[82] A. X. Liu, "Formal Verification of Firewall Policies," in 2008 IEEE International Conference on Communications, 19-23 May 2008 2008, pp. 1494-1498, doi: 10.1109/ICC.2008.289.
[83] F. N. Nife and Z. Kotulski, "Application-Aware Firewall Mechanism for Software Defined Networks," Journal of Network and Systems Management, vol. 28, no. 3, pp. 605-626, 2020/07/01 2020, doi: 10.1007/s10922-020-09518-z.
[84] P. André, "Firewalls," in Network Security: Wiley, 2014, pp. 215-235.
[85] R. W. Anwar, T. Abdullah, and F. Pastore, "Firewall Best Practices for Securing Smart Healthcare Environment: A Review," Applied Sciences, vol. 11, no. 19, p. 9183, 2021.
[86] P. Francis, "Network address translation (nat)," ACM SIGCOMM Computer Communication Review, vol. 45, no. 2, pp. 50-50, 2015.
[87] C. Scott, P. Wolfe, and M. Erwin, Virtual private networks. " O'Reilly Media, Inc.", 1999.
[88] R. Lund, A. Fenzl, and C. Villanueva, "Distributed Firewall for IoT," 2020.
[89] A. Herzog and N. Shahmehri, "Usability and Security of Personal Firewalls," in New Approaches for Security, Privacy and Trust in Complex Environments, Boston, MA, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Eds., 2007// 2007: Springer US, pp. 37-48.
[90] PCmag. `https://www.pcmag.com/reviews/luma-home-wifi-system` (accessed.
[91] J. Bugeja, A. Jacobsson, and P. Davidsson, "On privacy and security challenges in smart connected homes," in 2016 European Intelligence and Security Informatics Conference (EISIC), 2016: IEEE, pp. 172-175.
[92] D. K. Madhugundu, F. Ahmed, and B. Roy, "A survey on security issues and challenges in IoT based smart home," in Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018, pp. 26-27.