**INTERNET OF THINGS (IOT) SECURITY MECHANISMS**

**Abstract**. The exchange of information between numerous items and network technologies is entailed by IoT notion. Today, everything should be interconnected via the internet is the vision of Internet of Things (IoT). Since it opens new possibilities for new services, the IoT is and will continue to be the cornerstone for future development. All objects will be connected, and communication between them will be needed, although the CIA triad (at the very least) should not be jeopardized in any way. This element raises significant security concerns, which will be discussed further below.

1. **Introduction**

In the ICT sector for quite some time the term Internet of Things (IoT) has been used. In 1982 a vending machine was connected through ARPANET by four Carnegie Mellon University students (Ivor Durham, John Zsarnay, David Nichols, and Mike Kazar) to remotely check in each dispensing column the availability of the soda cans and their coolness. In 1999 during a presentation at Proctor & Gamble [1] it was addressed by Kevin Ashton regarding recently introduced RFID technology importance in the industry of supply chain. The need has grown over the internet for integration of all things since then. A market value of approximately $3 billion in 2020 with 20 billion devices in number will be reached according to major consulting firms. The size and power needed to perform a computation is almost half every two years and computation power is doubled at the same time is the reason for boom in IoT sector. For a wider range of applications more powerful and smaller devices are accessible for interconnection and data sharing. The issues in terms of standardization on low-energy & low-power devices and interoperability between different stacks, are due to IoT devices wide range of disciplines and technologies. Questions about how to assure confidentiality, integrity, and availability while considering these factors together, new security difficulties appear. All revolutionary developments, including IoT, provide people with a better life today and in the future, but there is a significant security problem. The public is increasingly concerned about privacy, especially today. The security of the IoT must be improved for it to pervade day to day lives of people.

Since IoT is a new technology, its security is critical to the growth of the IoT business. A major obstacle in the development of IoT is the lack of comprehensive and established security standards and models. The IoT in comparison to traditional networks, integrates a variety of networks, including WSNs, RFID systems, mobile vehicle networks, 3G/4G/5G technologies, PANs, VPNs, WiMAX, and so on. The security challenges must be addressed which become more complex than any other network system now in use as the IoT environment gets more demanding and complicated. The motivation for pursuing IoT research stems from a lack of long-term and flexible solutions to some of the most pressing security concerns. Some early security methods and solutions are currently in place, which needs improvement and standardization. The entire potential of IoT is extending towards a user inclusive IoT and beyond enterprise centric solutions, in which user-contributed information and IoT devices flows are encouraged. This will enable a new set of high-value services for society and new user-centric IoT information flows. Security is one of the most significant challenge to IoT nowadays. Which protocol stack delivers the best security and privacy services is a key concern. Because security can be supplied at many levels, deciding the best choice is not an easy task. Because the Internet of Things is still a new idea, many organizations and people in the industry are unaware of it. Because of their lack of awareness, they may be fearful of, or completely uninformed of, the possible security and privacy risks associated with their IoT deployment. As a result related to IoT security, many businesses are interested in learning more about the benefits, drawbacks, potential threats, solutions and problems. In conjunction with their IoT rollout, achieving cost-effective security they also require understanding of what level is needed of information security ability. This ability and knowledge should aid in non-IoT to an IoT firm transition, as it will allow both employees and management to understand and solve their issues and uncertainties about their investments and potential security risks. Managers can do a balanced risk-benefit analysis of IoT adoption for a given application or family of applications in this manner.

1. **Information Security**
   1. **Historical background.** Information security processes and techniques are as old as the information each self. From the very first years of communication, the value of security mechanisms was very well comprehended. In 50 B.C., Julius Caesar was one of the first to use these practices by inventing the Caesar’s cipher to get his information scribbled if it were found in unwanted hands. From 16th century mid various administrations around the globe, created organizations to secure the information and communication (e.g., In 1653 Deciphering Branch and UK Secret Office). More recently, during 19th century and because of the two World Wars many authorities were created to protect the privacy of information; exchange of war related information between allies of the World War II, brought into the picture the necessity of encrypting the information to become unreadable. This brought us to the Enigma Machine [2], which was invented at the end of WWI by Arthur Scherbius, but Nazis implemented before and throughout the WWII for warfare related data encryption. Alan Turing successfully decrypted Enigma.

By 20th century’s end and 21st century’s early years, while data encryption is taking place, there had been rapid advancement in telecommunications, hardware, and software. Things are getting smaller and smaller, more powerful, and even cheaper, bringing computing closer to everyone, appealing not only to businesses but to individuals as well. The Internet expansion and availability also helped on all these objects to be interconnected and made information publicly available.

The rapid growth of electronic business was used even for criminal acts, stimulated the need for protecting computers, networks and information.

* 1. **Information Security Definition.** It is a diverse field of closely linked research and professional goals to the implementation and development of all types of security countermeasures (legal, human-oriented, organizational, and technical) in order to keep all of its areas data (inside or around the establishment's boundary) and consequently, data management free of malicious attacks where it is created, processed, stored, communicated, and demolished [3].

Confidentiality, Integrity, and Availability of relevant data and IT paradigms are three main pillars of information security, that ensure following goals:

* Only authorized parties have access to information (Confidentiality),
* No unapproved modification in the information (Integrity),
* Whenever authorized persons demand information it can be accessed (Availability).
  1. **The CIA (Confidentiality, Integrity, and Availability) Model.** For describing the model, the term used is the CIA trio (Confidentiality, Integrity, and Availability). Inside an organization for information security policy guidance, the CIA triad is the method used. In security these three are regarded as the most important aspects/ pillars.
     1. **Confidentiality**. Privacy and Confidentiality are synonymous. It ensures that right ones only have access to the critical data and is out of the hands of the wrong people. Only authorized persons are granted accessibility to the data.

Passwords and Usernames, soft tokens, hardware, security tokens, biometrics & two-factor authentication and other procedures used to keep confidentiality include, but are not limited to, data encryption.

* + 1. **Integrity**. Throughout data life cycle consistency, correctness, and dependability are referred to as Integrity. To change the data, authorized persons/ parties are only allowed.

For preventing authorized users to do accidental deletion or mistaken changes, user access controls and file authorizations may be used, which is also a problem; for integrity verification checksums (cryptographic checksums) must be available; in case of permanent loss to restore the data to its actual state backups must be available.

* + 1. **Availability**. Availability means that the service has always been present, that proper bandwidth is available, that network bottlenecks are avoided, and that redundancy and disaster recovery are in place to assure system availability. Proxy servers, intrusion detection systems, and firewalls can be employed to keep intruders out and backup copies should be kept somewhere else other than inside the primary data storage.

Realization that the usual methods of storing data and transmitting are extended by Data Protection Act's requirements is vital. The security measures for personal data collection, storage, and processing are set up by seventh data protection guideline.

As a result, the preventive controls you implement should ensure following:

* Destruction, alteration, access, and visibility of personal data is only done by authorized people.
* Authority can only be exercised by those people within the scope.
* Personal information can be recovered if it is accidentally lost, altered, or destroyed, preventing any harm or discomfort to the relevant parties.

Following must be ensured by the organizations:

* For ensuring data protection, relevant technical and physical security protocols must be employed.
* Security breaches must be dealt with pertinent practices.
* From the start of developing new applications, privacy and security must be considered.
* Internal and external data sharing must be tracked.
* Policies for ensuring data recovery through backups must be in place.

There are so many threads that need to be considered when coping with Information security. In Table 1, most important IoT security threats are summarized.

|  |  |
| --- | --- |
| **Security issue** | **Details** |
| **Web interface weaknesses** | * Default Easily Guessable Credentials * Account Record * Credentials are Exposed in Network Traffic (XSS) * Session Management * SQL Injections * Account Lockout Settings that are not as good as they should be * Cross-site Scripting |
| **Insecure Network** | * Services at Risk * Overflow of the Buffer * DoS * Open Ports via UPnP * DoS via Network Device Fuzzing * UDP Services that can be exploited |
| **Insufficient Authentication/Authorization** | * Inadequate password complexity * Credentials that aren't properly protected * Two-factor authentication is inadequate * Risky password recovery * Privilege escalation * There is no role-based access control. |
| **Lack of Transport Encryption** | * Internet Services That Aren't Encrypted * Unencrypted Local Network Services * SSL/TLS implementation flaws * SSL/TLS configuration error. |
| **Insecure Cloud Interface** | * Account Counting * There was no account lockout * Credentials discovered in network traffic. |
| **Privacy Concerns** | * More data than is needed for functionality is gathered. * Gathered sensitive information * The data is not anonymized. * Data collection without encryption * Unsecured personal information * Unauthorized access to personal data * There were no retention policies implemented. |
| **Insecure Mobile Interface** | * In Network Traffic Credentials are Exposed * Account Enumeration * No Account Lockout |
| **Security Configurability Insufficient** | Absence of   * Options of Password Security * Granular Permission Model * Logging security * Monitoring security |
| **Physical Security Poor** | USB Ports available on devices  Storage Media available on devices |
| **Insecure Software/Firmware** | * Undated devices * Updates to unencrypted files * Transmissions of unencrypted connections * Ensure that the update file does not have any sensitive information. * Updates that are unsigned and unverified |

Table 1: IoT security threats

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| **Authenticity** | Just authorized persons could have access to the system or sensitive information. |
| **Authorization** | The rights and protections of device services and tools should be restricted so that they can only access the resources needed to complete their assigned tasks. |
| **Confidentiality** | Intruders should be kept out of information transmission between nodes. |
| **Integrity** | It is not permissible to tamper with related information. |
| **Availability and**  **Continuity** | To prevent command and control failures and interruptions, security service availability and continuity must be guaranteed. |

Table 2: Extended CIA model

* 1. **Security elements.** For the security domains, it is important to find key elements for the information security (Figure 1). In the following sections, the key elements definitions are described.

Figure 1: Security elements

* + 1. **Asset**. Asset is any datum, device, or in general any module of the organization’s universe that supports information-driven processes. Assets can include hardware, software, and information as well. Assets should be always protected under the CIA triad framework.
    2. **Threat**. In computer security, a threat is anything that can make a damage. A danger is something that could happen, or not. Dangers can prompt assaults on computer systems and that is only the beginning.
    3. **Vulnerability**. A vulnerability is any flaw or gap in safety strategies that can be manipulated by attacks to gain unauthorized access to an asset.
    4. **Risk**. When a treat threat is exploiting a vulnerability then a risk may be found, the possibility for loss, damage, or destruction of an asset.
    5. **Exposure**. A situation in a computing system (or combination of systems) that is not a general risk but enables an adversary to get information or hide operations.
    6. **Countermeasures**. Countermeasure shows any action, device, process, or technique that potentially may lead to reduce threats, vulnerabilities, or any attacks by preventing it or minimizing the damage. Corrective actions need to be taken even if it decided to simply mitigate the risk.
    7. **Security Policies**. Security Policy refers to the set of rules adopted by an organization to ensure that IT and network infrastructure adhere to data security principles, and that users take all proper precautions when contacting any arrangement of business action outside or inside of the organization's borders by ensuring that the CIA triad is respected.

|  |  |
| --- | --- |
| **Layer** | **Risks** |
| **Perception** | Spoofing, signal jamming, outage, eavesdropping |
| **Network** | Wormhole, sending, man in the middle, floods |
| **Support** | DoS, unauthorized access, data tampering |
| **Application** | Sniffers/loggers, DDoS, social and session hijacking, injections |

Table 3: For each IoT protocol layer, different threats and risks are presented

1. **IOT**
   1. **Background.** Kevin Ashton was the first person to use the term in 1999 [1], defining it as "Inside Internet-like framework their virtual representations and unique identification of things." From a technological standpoint, an infinite number of globally linked things network is the IoT – actuators, sensors or devices - which supply numerous facilities over the Internet. Fundamentally, IoT refers to a move from reactive to proactive systems, from delayed problem management to automated sense-and-respond capabilities.

Authors refers the IoT in [4] as "a digital society’s worldwide network that enables improved facilities by linking things (virtual and physical) using emerging & current compatible communication and information platforms."

Diagram

Description automatically generated

Figure 2: Technical overview of the IoT [4]

IoT consists of two key elements: "internet" and "things" [5]. Communication allows things to coordinate their actions and reach decisions together it allows them to hear, see, think, compute, and act. The technology gives things making authoritative decisions that help various applications using intelligence and consensus. From the standpoint of passive observers, they transform objects or sensors into active members of a computing system, communicating, working collaboratively, and making critical decisions. As a result, they present challenges that require specialized communication standards [6].

Communication is the most important aspect in achieving IoT. No matter how smart or capable the devices are, if they cannot send and communicate then they cannot be a part of the IoT ecosystem. The actual physical and link layer communication inside the IoT may be achieved in a variety of methods, therefore how this communication is carried out is less critical.

Through a communication channel, physical components can interact:

* CCTV cameras that check a location, for example, can be accessed through a gateway.
* If there is not a gateway, directly, for example, two smart home gadgets that are near to one another can communicate via Bluetooth or ZigBee protocols.

By using virtual objects, the projection into the digital environment of physical objects can be done, and the relationship between virtual objects & actual objects may not be necessary. A physical object can have many virtual identities, therefore it may run numerous services.

* 1. **Fundamental characteristics**. Following are the fundamental characteristics of the IoT:
     1. **Interconnectivity**: The worldwide communication and information exchange architecture allows anything to be interconnected.
     2. **Scalability**: The amount of devices currently linked to the internet will be at least an order of magnitude lesser than the amount of gadgets interact with one another and required to be controlled. The proportion of gadget communication to human-triggered communication will noticeably shift in favor of device-triggered communication. The collection and interpretation of information is crucial for application purposes, which is linked with efficient management and semantics of data.
     3. **Dynamic changes**: Dynamic alteration of device states (such as sleeping & waking up, being connected & offline and location & speed). Furthermore, fluctuation in the number of devices can also happen.
     4. **Heterogeneity**: The IoT devices are based on many networks and physical platforms which makes them diverse. Communication with other service platforms or devices is done through various networks.
     5. **Things related services**: IoT can deliver thing-related services under the restrictions of things, such as lexical uniformity and data security between virtual & real things and will alter both digital and physical world technologies.
  2. **IoT Roadmap.** It is widely accepted that RFIDs were the ancestors of IoT. Originally used in supply chain industry for tracking purposes, very rapidly moved to the market such as food safety, transportation, surveillance, security and others facilitated by the network evolution as elaborated in Figure 3. These days is used for monitoring and controlling of remote or distant objects [7].



Figure 3: IoT Roadmap [7]

A significant increase is predicted in the total installed IoT devices and is estimated to increase from the 13.8 billion units estimated in 2021 to 30.9 billion units in 2025 [8].

|  |  |
| --- | --- |
| **Attacks** | **Risks** |
| **Signal/Radio Jamming** | Integrity and availability |
| **Spoofing** | Confidentiality, integrity, and authenticity |
| **Node Outage** | Authenticity and availability |
| **Path-based DoS Attack** | Authenticity and availability |
| **Eavesdropping** | Confidentiality |
| **Device-tampering/Node capturing** | Confidentiality, integrity, authenticity, and availability |

Table 4: IoT attacks

1. **Security in IoT**
   1. **Introduction.** In terms of hardware, software, and network many techniques to support the supplied services are required for IoT network implementation. Many complications occur as far as security of an IoT ecosystem is concerned, which must be addressed.

* The greatest barrier, whether virtual or real, are things themselves in the IoT environment. Number of difficulties in IoT network is directly proportional to the number of devices linked. Creation of as many items as conceivable is the basis of IoT. Ten years ago, we simply needed to safeguard our PC to access the internet; now, we must protect PCs, Smartphones, smart gadgets, cars, wearables, and everything else that is linked to the internet.
* The greater the number of gadgets, the more difficult it is to manage them. Firmware and operating system upgrades are critical for supporting elevated levels of security. Even consumers may find it challenging to keep tens of devices up to date with the newest security updates.
* Irrespective of the amount of IoT devices the transmission of information and communication, the information gathered for processing must be delivered to the next step. Including encryption, preservation of privacy and identification should be crucial elements in security of IoT.
* Smart gadgets unauthorized use.
* To the public, unprotected gadgets were sold by the vendors who did not care about security and even few years ago, overlooked security for certain devices.
* Inadequate experience and skills may serve as a backdoor to security vulnerabilities. When the milk is done, a typical customer can be notified by the smart is a considerable move ahead; however, it can be hacked, and if not properly secured same network devices can access its data.

For overcoming said problems, multiple implementation possibilities extending through famous globally used protocols (HTTP, TCP, SMTP) or copyrighted IoT protocols (ZWave and ZigBee) as well as open standards (from W3C, IEEE, or IETF) for standardized protocols (CoAP or 6LowPAN).

A set of several studies were considered to stipulate the following summarization for security requirements, challenges, threats and potential solutions ( [9], [10], [11], [12], [13], [14]).

|  |  |  |
| --- | --- | --- |
| **Used Process** | **Type** | **Objective** |
| SHA-1/ SHA-256 | Hashing | Integrity |
| DH | Asymmetric Key Agreement | Key Agreement |
| * ECC * RSA | Encryption (Asymmetric) | * Digital Signatures * Key Transport |
| AES | Encryption (Symmetric) | Confidentiality |

Table 5: Cryptographic Algorithms frequently used

* 1. **IoT Protocols associated to Security.** The most relevant significant IoT standards have been chosen to be assessed for security purposes. Every one of these protocols are components of the application or transport levels of the IoT protocol stack.
     1. **Datagram Transport Layer Security (DTLS).** Datagram security is ensured by DTLS protocol. TLS based protocol is built to supply similar security.

Even though security was kept in mind while creating. In 2013 by using OpenSSL implementation of DTLS the plaintext was extracted from DTLS while encryption was done using Cipher Block Chaining mode, by scientists of Royal Holloway, University of London.

* + 1. **Quick UDP Internet Connections (QUIC).** Between two destinations composite connections are collectively supplied by employing QUIC protocol that uses the User Datagram Protocol (UDP). Lowering transport latency and the number of connections capability, SSL & TLS like security protection may be supplied. To prevent congestion issues in both directions bandwidth estimation can be done using QUIC.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Features** | **Layer** | **Objective** | **UDP** | **Delivery** | **Interoperability** | **Security** |
| **QUIC** | Transport | Composite connections | Yes | Not guaranteed | Yes | Yes |
| **DTLS** | Transport | Communication privacy for UDP | Yes | Not guaranteed | Partial | Yes |

Table 6: Security protocols assessment

* + 1. **CoAP.** RFC 7228 defines the Constrained Application Protocol (CoAP), which has been enhanced by RFC 7252 for applications of IoT. CoAP is meant to allow communication with each other among different devices on a restricted network and among gadgets on the internet having multiple constrained networks. For SMS, CoAP is used over cellular networks.

With HTTP, CoAP is expected to be used in conjunction for web integration, to supply multicast, and to supply minimal overhead and simplicity, having significant importance in IoT. Devices that support protocols like UDP, CoAP can be used.

* + 1. **MQTT.** To take into consideration unreliable networks, high latency and low bandwidth, in 1999 the specifically suited IoT M2M light weighted messaging protocol was invented by Arlen Nipper and Andy Stanford-Clark. Message delivery assurance and dependability were the main criteria while implementing the protocol. Therefore, for environments like M2M in IoT, this protocol is excellent. In later versions SSL is used for encrypting the login information passed by the users to devices.

The subscriber/ publisher mode is the basis of working model of MQTT (see Figure 4: MQTT working model) this means that a publisher uses a broker to made available a set of information, which is made accessible to others who are ready to take part in it (subscribers) .

Figure 4: MQTT working model

* + 1. **JSON.** In 2000 JavaScript Object Notation (JSON) was introduced by Douglas Crockford, as described in RFC 7159. To communicate array data types and attribute value pairs of data objects human readable text is employed by JSON. It is widely used asynchronous communication protocol that is language independent. Though it was designed using JavaScript, wide range programming languages supports JSON format data structures.
    2. **CBOR (Concise Binary Object Representation).** As defined by RFC 7049, it is a binary data format built on JSON, resulting in small packet sizes. The CoAP Internet of Things protocol makes use of it.

1. **Security Mechanisms for IoT systems**
   1. **Blockchain Technology.** It consists of a decentralized, distributed, immutable and shareable P2P ledger [15].

In blockchain the most important part is a block. The previous block has an information which is encrypted and is stored inside each block.

In public records of a block task units are normally kept which is known as transactions. Once a majority users of blockchain network approves a transaction, each block is updated with the transaction in the blockchain [16]. In the consensus method the data is recorded in the ledger which is analyzed in the distributed ledger after the approval of all network members.

The decentralized structure of blockchain is an important aspect. Data is appeared as a database of distributed ledger on a blockchain network. Simultaneously, on all other stakeholders inside the network the same data is stored. Maximum traceability in blockchain technology is delivered for all involved parties due to these characteristics.

A significant benefit of blockchain technology is the operations transparency of corporate sector which ensures accountability and therefore builds confidence among all stakeholders. In this way blockchain network can be monitored in real time by all stakeholders.

In restricted blockchain networks a premium on data privacy is placed. In the blockchain network the security of data is ensured when it can be accessed only by the users approved by the node's administrator.

Data alteration in blockchain networks' is safeguarded by using public key structure, which ensures integrity. Data security is also ensured by consensus process and a blockchain network's members.

Between stakeholders’ business operations, smart contracts are described as bits of code in blockchain networks.

Smart contracts are being leveraged by several digital currencies in blockchain technology, which includes the cryptocurrencies being widely used i.e., Ethereum and Bitcoin. Hyperledger Fabric network is being used widely in the realm of blockchain business applications.

* + 1. **Related work.** In [17], a method for integrating supply chain technology into blockchain and IoT activities is provided. A Blockchain-based distributed planning platform is offered in the research in which supply chain actors are added as nodes to the system. Transported property’s virtual duplicate is produced by IoT devices on the proposed platform. Other data, comprising of the humidity, temperature, and location of the delivered products, is tracked, and stored on the blockchain via the virtual copy.

At [18], the most essential advantage of data storing using smart contracts data to a blockchain network from IoT devices, according to the authors, is that the data may be automatically assessed and relayed to the sender or recipient. The temperature measurements from the sensors are corrected by the smart contract running in the system and saved to the blockchain. The REST API is used by mobile clients to connect with the server. Users can use these mobile clients to manage their data in the system.

At [19], a network management and monitoring architecture based on blockchain is suggested. The network administrators manage the network devices indirectly by registering changes to the system configurations on the blockchain, where they manage the modifications to the network device settings.

At [20], its goal is to use blockchain to control and configure IoT devices. Three Raspberry Pi and a smartphone are included in the suggested system. The system's three Raspberry Pi each serve as a light bulb, air conditioner and meter. The system’s policy may be changed by the user via their smartphone. Modifications to the IoT device's configuration are logged on the Ethereum network.

At [21], it is said that the change-resistant and decentralized characteristics of blockchain maybe employed to tackle few challenges associated with IoT. The authors proposed to overcome this challenge, a fog and cloud based method. As the IoT gadget Intel Edison Arduino card is employed in the research, and the blockchain operates on the fog and cloud independently. The IoT gadget uses a Python server in the trials to send data to the blockchain.

For Identification, Authorization, and Authentication the Hyperledger Fabric API server running the MQTT publisher must communicate with a previously declared authorized user of Hyperledger Fabric organization [22]. Around the same time, extra authentication is supplied by leveraging MQTT's permission fields for username and password. Unwanted access to the data will be avoided, by authenticating the data supplied over the protocol (Figure 5). Additionally, MQTT TLS support is available as an option, making it simple to encrypt data and authenticate users via authentication protocols.

Graphical user interface, application

Description automatically generated

Figure 5: IoT Integration to Hyperledger Network [22]

Model made use of blockchain architecture to keep track of data from IoT devices in a public ledger [23]. Because of the decentralized nature of blockchain [24], illegal manipulation of IoT devices is less likely, and blockchain appears to be an effective opportunity for securing and managing IoT device data [25]. There seems to be a trade-off among a hashing algorithm's output size and security. A reduced hash size is right for blockchains associated to IoT contexts in terms of storage memory. These smaller hashes, on the other hand, are simpler to compute and penetrate. To compensate for the lower temporal complexity, a higher difficulty parameter of smaller output sizes hashing algorithms shouldbe used.

Authentication-based techniques can be used to tackle fog layer security challenges; however, in cross-domain connectivity situations under the SDN framework they do not function well. Furthermore, due to the high-security sensitivity of human health data and the peculiar nature of fog nodes, significant problems are faced by the data privacy and system security, and how to support data integrity & signaling and avoid tampering should be properly studied. Likewise, medical IoT peripherals may be untrustworthy or malicious, causing them to file false claims in order to abuse network resources, attain better services, and compromise system security by initiation of cyber-physical attacks; as a result, to ensure the system's security effective security measures should be designed [26].

To guarantee system integrity, a  two-layer multidimensional and blockchain-based security scheme, the data layer BottomChain and the control layer TopChain, is explained to resist well to diverse cyber-physical attacks, such as tampering, non-repudiation, and DDoS threats, whereby critical information including human health parameters, the corresponding task processing results & original task information, intra SDN and inter SDN control signaling, and the blacklisting of the edge devices are protected, profiting from the controlling, protected storage size of the blockchains. Additionally, under blockchain-based security mechanism, human data and node activities may be properly traced. Furthermore, single-point failure an inherent problem of SDN is dropped by TopChain.

In the last decade, there have been several cyber-attacks against healthcare services. Unfortunately, earlier solutions do not consider security over data storage and transfers, which has become a critical part in guaranteeing privacy and preserving patient medical data in medical. As a result, the information's of smart healthcare is presented in an operational framework for safeguarding, which is one of the major issues faced in current healthcare, such as breaching of patients' sensitive health records for stake and protecting patient's records available in the healthcare organization may cause patient's healthcare unproductive data delivery [27]. One of the problems seen because of unprotected documents is a lag from one service provider to another in the patients' records processing. As a result, the EHR has faced such limitations that can be solved by modern technology like as Blockchain, which has lately been implemented by many governments, public-private partnerships, and private organizations [28].

* 1. **AI based security mechanisms.** IoT devices are globally accessible, are made up mostly of limited capabilities, and are connected via lossy networks [29]. As a result, critical changes to current security ideas for networks (wireless and information) to achieve efficient IoT security approaches should be made. It is difficult and inadequate for mega networks to implement current defense measures including application & network security, access control, encryption, and authentication with many linked gadgets, each of which has known weaknesses.

Possessing the capacity to analyze IoT devices, as proved in Figure 6, can effectively give a remedy to new or zero-day assaults. ML/DL are strong data analysis methods to discover 'normal' and 'abnormal' behavior in the IoT ecosystem based on how IoT elements and devices communicate with each other. Each part of the IoT system's input data may be gathered and studied to discover normal patterns of interaction, allowing for early detection of malicious conduct. Furthermore, because they can intelligently forecast future unknown assaults by learning from current instances, ML/DL algorithms might be useful in predicting new attacks, which are typically mutations of earlier attacks. As a result, for successful and safe networks, IoT devices must migrate from just supporting connection security between devices to security-based information provided by DL/ML approaches.

Diagram

Description automatically generated

Figure 6: Illustration of the potential role of ML/DL in IoT security

* + 1. **Machine Learning technique.** Machine learning (ML) is a branch of artificial intelligence that combines a variety of approaches and procedures to give computers and smart devices intelligence. In the network security environment, machine learning techniques such as supervised learning, unsupervised learning, and reinforcement learning have been widely used. It is used to precisely detect and specify the exact data plane security regulations to be enforced. The task at hand is to fine-tune the many aspects of important security protocols to minimize a certain sort of attack, either by tagging network traffic or by setting access policy. Various machine learning approaches may be used to counteract a range of IoT assaults. For instance, neural networks can be employed to identify network intrusion [30] and DoS attacks and K-NN can be used in malware detections [31].
* **Supervised Learning**: The intrinsic relationships of the data might not be accessible in supervised techniques, but the model's outcome is known. Typically, this model's training involves a set of data to "learn" and another set of data to test and assess the resultant model. Matching an attack pattern to a group of previously known assaults is a classic case in the security environment.
* **Unsupervised Learning**: Apart from supervised learning, the model in unsupervised learning is undefined, which means unlabeled data. A relationship between the data and its categorization into categories is done by relevant models.
* **Reinforcement Learning**: It is concerned with analyzing issues and developing strategies to enhance its model. It has a one-of-a-kind model learning mechanism that incorporates trial and error as well as incentive functions. It keeps track of the output's outcomes and uses the reward to generate a value termed a "value function." The model recognizes the correctness of its choice based on this value and adjusts itself accordingly.
  + 1. **IoT Security based on Deep learning (DL).** To learn data interpretations with multiple degrees of complexity, various processing levels (layers) are integrated by supplied mathematical framework. DL methods have considerably advanced ultramodern applications as compared to traditional ML methods [32]. For generative or discriminative feature manipulation and abstraction for analysis techniques, DL is an ML area that employs numerous non-linear processing layers. Because they may capture hierarchical patterns in deep architecture, DL approaches are sometimes known as hierarchical learning techniques. The operating premise of DL is based on the signal rendering systems of the human brain and neurons. Deep networks can be used for supervised learning (discriminative learning), unsupervised learning (generative learning), or a blend of the two (hybrid DL). Examples of discriminative DL methods are CNNs and recurrent neural networks (RNNs). Deep autoencoders (AEs), Ensemble of DL Networks (EDLNs), Generative Adversarial Networks (GANs), Deep belief networks (DBN), and Restricted Boltzmann Machines (RBMs) falls in hybrid DL approaches.
    2. **Related work.** IoT security is a hotly debated research topic that is gaining traction in the scientific field. Many books have been written about this vital topic.

Numerous research publications [33], [34] focuses on analyzing the effectiveness and practicality of operating virtual security equipment on the edge using containers, such as Intrusion Detection Systems (IDS) and firewalls, in the context of Network Function Virtualization. Although this lightweight virtualization method proved to be quite efficient, it was difficult to compensate for the resource constrained IoT equipment. Indeed, heavy traffic can lead to significant energy and CPU use, compromising the device's usability. Machine learning algorithms supply an alternate approach to securing IoT networks. [35] proposes a number of methods that make use of SDN architecture and machine learning approaches to enable network intrusion detection systems. The paper also discusses the difficulties that come with implementing network intrusion detection systems.

The authors of [36] suggested a system that uses deep learning to estimate the location of a city bus. For forecasting data rate & locations, neural network based on Long Short-Term Memory (LSTM) have been studied in the proposed approach. Authors in [37] have supplied a method that utilizes block-chain for monitoring scaled IoT systems. The authors of [38] propose a method for securing connections among IoT devices and the MEC. A learning mechanism approach is used to select candidates for service distribution & composition.

To examine the network traffic (moving from gateway to edge devices), Artificial Neural Networks is used [39]. They employed temperature sensors as edge devices and a Raspberry Pi as an IoT gateway in their method. Various data samples are collected from edge devices and stored in a database on the gateway. They then separated the data into training and testing categories. The testing data is being used to confirm the model's accuracy after the neural network has been developed using training data. Although the findings prove an increased degree of security in terms of anomaly detection, the system's capabilities were restricted by the IoT gateway's limited resources, significantly affecting the user experience and the device's longevity. [40] proposes an intrusion detection system that runs on top of linked automobiles. For finding threats, the proposed system uses deep belief and decision tree machine learning algorithms.

AI may be used in IoT to find aberrant behaviors depending on factors from both network systems and tangible metrics supplied by IoT devices. Mehta et al. [41] propose an AI-based IDS technique for IoT that detects abnormalities by exploiting the association between a group of sensor data time-series. Furthermore, AI platform is designed to deal with both anomalous-based and knowledge-based IDS by examining signatures and patterns of previously known vulnerabilities and attacks on a continual basis [42]. In this regard, most of the earlier study has concentrated on the identification stage of incidents.

* 1. **Intrusion Detection System.** The security becomes extremely important of those devices which people use as we approach closer to a day where everything people use is connected to the internet. For combating DDoS attacks, in the literature, there are two key systems used. Intrusion Detection System (IDS) is a preventative mechanism in which the system does not act if an intrusion has occurred, instead an alarm is raised. Intrusion Prevention System (IPS) is a punitive tool in which the system acts in case of an incursion [43]. In IPS, there is a problem with false positives because genuine users might be restricted as well. A full comparison of IDS and IPS systems is shown in Table 7.

|  |  |
| --- | --- |
| **IPS** | **IDS** |
| Functions of IPS does not need human interaction and are dependent on the rule set. | To perform any action, human intervention is needed. |
| High concern is false alarms. | The false alarm rate has less of an influence on performance than the IPS rate. |
| The system might slow down. | IDS do not affect system performance. |
| Because it analyzes and defends the device, IPS is a regulatory framework. | IDS recognizes the threat and checks the system. |
| False alerts may cause legitimate traffic to be stopped. | The false alarm rate has less of an influence on performance than the IPS rate. |

Table 7: Relative assessment of IPS and IDS approaches [44].

IDS is also emphasized in this research since in malware categorization major problem is false alarm rate. Punitive step performed against genuine users might sometimes defeat the purpose of developing a detection system. Figure 7 depicts a graphical depiction of the Intrusion Detection Systems (IDS) category. Due to varying location of target, it can be classified into Host IDS (HIDS), Network IDS (NIDS), or Hybrid IDS. HIDS is system-specific and is costly since one IDS is needed per host, but can detect an inside intruder with high accuracy, and the scope of the intrusion can be precisely estimated [45]. External intrusion is well found and a NIDS can defend all users, but too much communication packets are travelling in the network to analyze [46]. Because it includes characteristics from both HIDS and NIDS, the hybrid IDS is more versatile and secure [47]. In Active IDS, specific actions are conducted in response to specific warnings, while in Passive IDS, just reports are created, or alarms are raised. Individual monitors are used by centralized IDS to check each host since it does not grow according to demand, resulting in less flexibility. Furthermore, a single point of failure is a risk with centralized IDS. On the other hand, with each observing unit also serving as an evaluation unit, a peer-to-peer (P2P) architecture is the basis of Distributed IDS.

Diagram

Description automatically generated

Figure 7: How different IDS approaches are classified is illustrated[44].

* + 1. **Anomaly Detection Techniques.** Signature-based Detection and Anomaly-based Detection are the two main techniques used for Malware Detection. Because Botnets mutate, and as a result, In case of botnets, bots signature changes, therefore detection approach based on signatures [48] is not amazingly effective. In real-world circumstances to discover varieties of botnet varieties, these methods are ineffective. On the other hand detection algorithms based on anomalies [49], are widely used since they assume Botnet traffic would behave differently from regular traffic.

In the literature, there are several approaches for detecting anomalies. A full comparison of several Anomaly detection strategies is shown in Table 8. The machine learning-based technique is beneficial and widely recognized for a wide variety of malware categorization, as shown in the Table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Paper** | **Method** | **Cases** | **Methodology** | **Advantage (+), Disadvantage (-)** |
| Choudhary et al. [50] | Protocol based model | * Communication protocol * Application protocol | * The protocol-based architecture employs several levels of surveillance protocols. * Discrepancies linked with a protocol are found using computing methods. | * For a certain sort of assault, recognition efficiency is excellent. * Because it is only good for some sorts of assaults, it is useless against others. |
| Kumar et al. [51] | Model based on rules | Rules based on:   * Behavior * Fuzzy * Association | * Patterns are formed from data flow patterns in a rule-based paradigm. * When a rule is breached, it is referred to as anomalous behavior. | * The model is straightforward. * For rule generation, more traffic monitoring is necessary. * A high rate of false positives |
| Kim et al. [52] | Model based on payload | Models:   * N-gram * Grained | * Features of a typical packet payload are analyzed, and any divergence is regarded as abnormal. | * For known assaults, the model performs admirably. * Because of the computational overhead, the handling time is greater. * For fresh attacks, the accuracy is lower. |
| Kalkan et al. [53] | Model based on statistics | * Multivariate * Univariate * Markov process * Time series | * Mathematical computations are used in the statistical model method. * The user's earlier data is used to develop a model for usual behavior. | * The model is straightforward. * The correctness of the model is influenced using statistical or mathematical modelling. |
| Hai et al. [54] | Model based on Machine Learning | * Neural networks * Outlier detection * Clustering * Classification * Genetic algorithms | * Training and testing are the two steps of machine learning models. * Learning is of two types: supervised & unsupervised. | * Can quickly recognize patterns. * A wide range of applications is possible. * Appropriate for online datasets. * Can continue to improve. * Lengthy periods of training are necessary. * For better results, a larger data collection is needed. |

Table 8: A comparison of anomaly classification methods.

**Conclusion.** The progress of IoT has been tremendous, and it has cleared the path for several technological undertakings. IoT security is critical for ongoing technological advancement since investors will only invest in this sector if ultramodern security procedures are implemented. In general, cybersecurity follows the CIA paradigm, which stands for confidentiality, integrity, and availability. Attackers start assaults by exploiting flaws in communication protocols. Improved prevention approaches are necessary for minimizing assaults, as these attacks threaten the reputations of service providers. The assaults affect all three CIA components, which is service providers’ key concern. IoT sensors generate data at many sizes dependent on the application being addressed, ranging between few bytes to multiple Kbytes every second. For example, medical or military data, might be critical at times, due to their ability to bring down victims, major hazards to the cyber world are posed by DDoS attacks. Many computers are needed to launch DDoS attacks for which IoT devices are ideal. Consumers in most circumstances will be unaware that the device has been hacked; for example, limited access is provided by the user interface of baby monitors and smart toys and even after becoming a bot in a botnet army might still be functioning. While IoT devices are growing in the network, there is a need to detect attacks launched by botnets as soon as possible and remove the bots and the infected devices.

The security of the devices is getting critical as we progress towards an era in which everything people use is linked to the internet. In the literature, there are two primary techniques for avoiding DDoS attacks: IDS and IPS. The IDS is reviewed, and multiple intrusion detection models have been explored. Furthermore, we addressed Intrusion Detection System categorization, various anomaly detection approaches, multiple IDS methods depending on datasets, various ML, and DL procedures for pre-processing data and detecting malware. Finally, after examining several intrusion detections approaches and future ambitions, a larger viewpoint was envisioned.

# **BIBLIOGRAPHY**

|  |  |
| --- | --- |
| [1] | K. Ashton, "That ‘internet of things’ thing," *RFID journal,* vol. 22, no. 7, pp. 97-114, 2009. |
| [2] | Wikipedia, "Enigma machine," 2022. [Online]. Available: https://en.wikipedia.org/wiki/Enigma\_machine. |
| [3] | "IEEE Standard for an Architectural Framework for the Internet of Things (IoT)," IEEE Std, 2020. |
| [4] | "An Overview of Enabling Technologies for the Internet of Things," Internet of Things A to Z: Technologies and Applications , IEEE, 2018. |
| [5] | K. K. Vaigandla, R. K. Karne and A. S. Rao, "A Study on IoT Technologies, Standards and Protocols," *IBMRD's Journal of Management & Research,* vol. 10, no. 2, pp. 7-14, 2021. |
| [6] | T. Salman and R. Jain, "A Survey of Protocols and Standards for Internet of Things," *Advanced Computing and Communications,* vol. 1, no. 1, 2017. |
| [7] | G. Mavridis, "Security mechanisms for Internet of Things (IoT)," University of East London, Greece, Piraeus, 2017. |
| [8] | L. S. Vailshery, "IoT and non-IoT connections worldwide 2010-2025," 2021. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/. |
| [9] | T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy and G. P. Hancke, "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," *IEEE Access,* vol. 8, pp. 152351-152366, 2020. |
| [10] | A. H. Imam and M. A. Azer, "Internet of Things security framework," *13th International Computer Engineering Conference (ICENCO),* pp. 378-382, 2017 . |
| [11] | D. Bassole, K. K. Kabore, Y. Traore, O. Sie and H. B. Sta, "Design and implementation of secure communication protocols for Internet of Things systems," *IEEE International Smart Cities Conference (ISC2),* pp. 112-117, 2019 . |
| [12] | S. Rizvi, A. Kurtz, J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),* pp. 163-168, 2018 . |
| [13] | B. Nathani and R. Vijayvergia, "The Internet of Intelligent things: An overview," *2017 International Conference on Intelligent Communication and Computational Techniques (ICCT),* 2017. |
| [14] | J. P. Nzabahimana, "Analysis of security and privacy challenges in Internet of Things," *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT),* 2018. |
| [15] | N. E. Ioini and C. Pahl, "A Review of Distributed Ledger Technologies," *On the Move to Meaningful Internet Systems. OTM 2018 Conferences Confederated International ,* vol. 11230 , pp. 277-288, 2018. |
| [16] | S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," *IEEE 5th International Conference on Computer and Communications (ICCC),* pp. 1258-1263, 2019 . |
| [17] | N. Rožman, R. Vrabič, M. Corn, T. Požrl and J. Diaci, "Distributed logistics platform based on Blockchain and IoT," *Procedia CIRP,* Vols. 81,, pp. 826-831, 2019,. |
| [18] | T. Bocek, B. B. Rodrigues, T. Strasser and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," *IFIP/IEEE Symposium on Integrated Network and Service Management (IM),* pp. 772-777, 2017 . |
| [19] | K. Košťál, P. Helebrandt, M. Belluš, M. Ries and I. Kotuliak, "Management and Monitoring of IoT Devices Using Blockchain," *Sensors for Information Technology, Electronics and Mobile Communication,* vol. 19(4), p. 856, 2019. |
| [20] | S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," *19th International Conference on Advanced Communication Technology (ICACT). Global IT Research Institute - GiRI,* pp. 464-467, 2017 . |
| [21] | P. Gupta, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Towards a blockchain powered IoT data marketplace," *International Conference on COMmunication Systems & NETworkS (COMSNETS),* pp. 366-368, 2021 . |
| [22] | K. O. Toka, Y. Dikilitaş, T. Oktay and A. Sayar, "Securing Iot with Blockchain," *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences,* vol. 46, pp. 529--532, 2021. |
| [23] | A. Alrehaili and A. Mir, "POSTER: Blockchain-based Key Management Protocol for Resource-Constrained IoT Devices," *First International Conference of Smart Systems and Emerging Technologies (SMARTTECH),* pp. 253-254, 2020 . |
| [24] | M. Singh, A. Singh and S. Kim, "Blockchain: A Game Changer For Securing IoT Data," *IEEE 4th World Forum on Internet of Things (WF-IoT),* 2018 . |
| [25] | K. Gagneja and R. Kiefer, "Security Protocol for Internet of Things (IoT): Blockchain-based Implementation and Analysis," *Sixth International Conference on Mobile And Secure Services (MobiSecServ),* 2020 . |
| [26] | J. Ren, J. Li, H. Liu and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," *Tsinghua Science and Technology,* vol. 4, no. 27, pp. 760-776, 2022. |
| [27] | A.Yogeshwar and S. Kamalakkanna, "Healthcare Domain in IoT with Blockchain Based Security- A Researcher’s Perspectives," *Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021),* 2021. |
| [28] | N. Kshetri, "Blockchain and electronic healthcare records [cybertrust] Computer," vol. 51, no. 12 , p. 59–63, 2018. |
| [29] | A. M. d. S. Cardoso, R. F. Lopes, A. S. Teles and F. B. V. Magalhães, "Poster Abstract: Real-Time DDoS Detection Based on Complex Event Processing for IoT," *IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI),* pp. 273-274, 2018. |
| [30] | S. Latif, Z. Idrees, Z. Zou and J. Ahmad, "DRaNN: A Deep Random Neural Network Model for Intrusion Detection in Industrial IoT," *International Conference on UK-China Emerging Technologies (UCET),* pp. 1-4, 2020 . |
| [31] | Z. H. Abdaljabar, O. N. Ucan and K. M. A. Alheeti, "An Intrusion Detection System for IoT Using KNN and Decision-Tree Based Classification," *International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI),* pp. 1-5, 2021 . |
| [32] | T. J. Sejnowski, The Rise of Machine Learning, MIT Press, 2018. |
| [33] | A. R. Boudi, I. Farris, M. Bagaa and T. Taleb, "Assessing Lightweight Virtualization for Security-as-a-Service at the Network Edge," *IEICE Transactions on Communications,* vol. E102, pp. 970-977, 2019. |
| [34] | R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar and J. Ott, "Consolidate IoT edge computing with lightweight virtualization," *IEEE Network,* vol. 32, pp. 102-111, 2018. |
| [35] | N. Sultana, N. Chilamkurti, W. Peng and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Netw. Appl.,* vol. 12, pp. 493-501, 2019. |
| [36] | S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily and J. B. Othman, "QoS enhancement with deep learning-based interference prediction in mobile IoT," *Comput. Commun.,* vol. 148, pp. 86-97, 2019. |
| [37] | L. Tseng, L.Wong, S. Otoum, M. Aloqaily and J. B. Othman, "Blockchain for managing heterogeneous Internet of Things: A perspective architecture," *IEEE Netw.,* vol. 34, pp. 16-23, 2020. |
| [38] | I. A. Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," *Sustain. Cities Soc.,* vol. 56, 2020. |
| [39] | X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Commun. Surveys Tuts,* 2020. |
| [40] | M. Aloqaily, S. Otoum, I. A. Ridhawi and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw,* vol. 90, 2019. |
| [41] | A. M. Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos and P. Gouvas, "Security management architecture for NFV/SDN-aware IoT systems," *IEEE Internet Things,* vol. 6, pp. 8005-8020, 2019. |
| [42] | B. B. Zarpelao, R. S. Miani, C. T. Kawakani and S. C. d. Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl,* vol. 84, pp. 25-37, 2017. |
| [43] | C. V. Martínez and B. Vogel-Heuser, "Towards industrial intrusion prevention systems: A concept and implementation for reactive protection," *Appl. Sci.,* vol. 8, pp. 1-29, 2018. |
| [44] | N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access,* vol. 9, pp. 59353-59377, 2021. |
| [45] | T. R. Glass-Vanderlan, M. D. Iannacone, M. S. Vincent, Q. Chen and R. A. Bridges, "A survey of intrusion detection systems leveraging host data," *ACM Comput. Surv.,* vol. 52, p. 128, 2018. |
| [46] | R. Panigrahi, S. Borah, A. K. Bhoi and P. K. Mallick, "Intrusion detection systems (IDS)-An overview with a generalized framework," *Adv. Intell. Syst. Comput.,* vol. 1040, pp. 107-117, 2020. |
| [47] | A. N. Cahyo, A. K. Sari and M. Riasetiawan, "Comparison of hybrid intrusion detection system," *Proc. 12th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE),* pp. 92-97, 2020. |
| [48] | J. Ghasemi, J. Esmaily and R. Moradinezhad, "Intrusion detection system using an optimized kernel extreme learning machine and efficient features," *Sadhana-Acad. Eng. Sci.,* vol. 45, 2020. |
| [49] | E. Herrera-Viedma and H. Fujita, "Multilayer framework for botnet detection using machine learning algorithms," *IEEE Access,* vol. 9, pp. 48753-48768, 2021. |
| [50] | S. Choudhary and N. Kesswani, "A survey: Intrusion detection techniques for Internet of Things," *Int. J. Inf. Secur. Privacy,* vol. 13, pp. 86-105, 2019. |
| [51] | V. Kumar, D. Sinha, A. K. Das, S. C. Pandey and R. T. Goswami, "An integrated rule based intrusion detection system: Analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Comput.,* vol. 23, pp. 1397-1418, 2020. |
| [52] | A. Kim, M. Park and D. H. Lee, "AI-IDS: Application of deep learning to real-time Web intrusion detection," *IEEE Access,* vol. 8, pp. 70245-70261, 2020. |
| [53] | K. Kalkan, L. Altay, G. Gür and F. Alagöz, "JESS: Joint entropy-based DDoS defense scheme in SDN," *IEEE J. Sel. Areas Commun.,* vol. 36, pp. 2358-2372, 2018. |
| [54] | T. H. Hai, L. H. Hoang and E.-N. Huh, "Network anomaly detection based on late fusion of several machine learning algorithms," *Int. J. Comput. Netw. Commun.,* vol. 12, pp. 117-131, 2020. |