IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IOT SECURITY USING MACHINE LEARNING APPLICATIONS

Dr. FLORENCE VIJILA S,
HOD of Computer Science,
CSI Ewart Women's Christian College,
Melrosapuram, Chengalpet District,
Tamil Nadu, India.

Mrs. JAYALAKSHMI. V,
Assistant Professor, Department of
Computer Applications,
DRBCCC Hindu College, Pattabiram,
Chennai, Tamilnadu, India.

Abstract— IoT security is the field of study concerned with the protection of linked devices and networks in the Internet of things (IoTs). It entails the rising frequency of things with unique IDs as well as the capacity to automatically transfer data over a network. Computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communications, smart energy grids, home and building automation, vehicle-to-vehicle communication, and wearable computing devices are driving most of the increase in IoT communication. The fundamental issue is that, because networking appliances and other items are still relatively new concepts, security has not always been considered in product design. IoT devices are frequently sold with outdated embedded operating systems and software. To strengthen security, an IoT device that requires direct Internet connectivity should be segregated into its own network and network access controlled. The network segment should then be watched to identify potential unusual traffic and, if necessary, action should be taken. The suggested method outlines the use of machine learning in IoT security systems to evaluate and learn from trends in order to help prevent similar assaults and respond to changing behaviour. Machine Learning can assist IoT security teams in being more proactive in preventing risks and responding in real time to active attacks.

Keywords— Threats, IoT Security, Devices, Machine Learning, VANET.

I. Introduction

Before incorporating IoT in an existing system or developing a totally new system, organisations must be completely convinced of the security issues. As a result, IoT solution suppliers confront numerous hurdles in instilling trust in the technology. Every firm visualizes and conceptualizes IoT deployment differently, which adds to the uncertainty and scepticism about the suitability of security measures. Most vendors are more concerned with the solutions that their pool of sensors, data gathering and analysis servers, and optimization subroutines can bring to the company. They are less concerned about security risks after implementing the system, which is a more pressing concern. Simply delivering a tailored suite of suitable electronic components with software services in IoT implementation is insufficient for organisations wishing to enhance their technology. Every IoT vendor is aware that security has been the primary concern of enterprises in recent years, and they must supply IoT solutions that are equipped with secure and reliable operations via a variety of firewalls and security protocols. However, there is no standard security phenomena via which they may persuade their clients on security issues; rather, a more tailored strategy with unique security limitations is required. To make IoT more productive, organisations must be able to rely on it with trust, which is only feasible if vendors build the IoT system and implement security measures that are appropriate for the enterprise. As a result, it is also a matter of psychological trust in the technology, and vendors are essentially required to do that.

II. IoT Security

A Serious Concern Since the dawn of computing, security has been a primary concern. People are increasingly reliant on technologies that provide a more secure working environment while protecting their privacy and identity. Since the advent of the Internet of Things, the computing paradigm has moved from stand-alone computing to more flexible collaborative computing. This has prompted security concerns once more, with a more aggressive approach to the intrusion. It includes anything from individual personal information hacks to hacked financial transactions and spoofing. Intelligent gadgets that are controlled by sophisticated programmes are more likely to be misprogrammed. Furthermore, hand-shaking and shared collaborative platforms among these gadgets enhance the likelihood of security breaches. However, this is a chance not just for unscrupulous individuals, but also for programmers to reach the highest level of security in order to mitigate these security threats. The IoT framework's smart gadgets have been efficiently providing their activities since its inception. However, as the network grows, they confront new challenges to consumers and their personal data.

2.2.1 Confidentiality

The Internet of Things framework includes the linking of devices, sensors, information, and software services. Confidentiality refers to the property of guaranteeing that data or network transactions are only readable by the intended recipient. The primary purpose of confidentiality is to preserve the focus on device identification, communication, and sensing, as well as semantic services. The identification process is in charge of matching network services to user demand. Communication is concerned with connecting disparate items to a certain set of services. The information acquired from various smart devices is computed according to the user's requirement and delivered to the IoT database or cloud as sensed data during the sensing process. The processing unit of IoT is this aggregated piece of communication and computation. For secrecy, IoT networks commonly employ the Datagram Transport Layer Security (DTLS) protocol. It provides two-way authentication and is based on symmetric encryption and elliptic curve cryptography. Data confidentiality is provided through the use of the HTTPS protocol, which enables an encrypted and secure communication connection between IoT devices and gateways, as well as between gateways and the cloud.

2.2.2 Authentication

Authentication ensures a user's legitimacy in an IoT network. An authorised user is identified if it has the authority to communicate with its peers. To enforce authenticity and access control, session keys are generated using session key distribution systems. The nerve centre of Internet security has always been public key infrastructure (PKI). It ensures mutual trust as well as device authentication.

2.2.3 Data Integrity

This feature of a secure IoT network deals with data housed in devices as well as data travelling between interacting nodes (Figure 1.1).

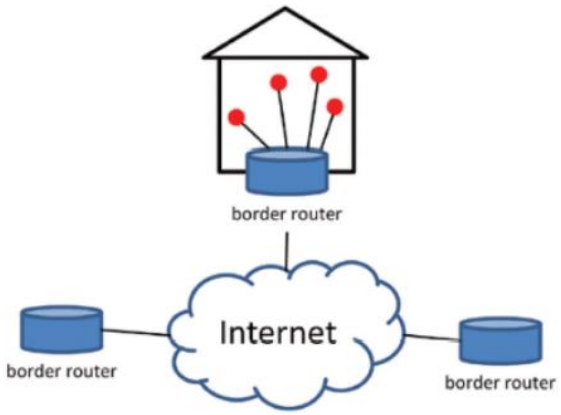

Figure 1.1 IoT network infrastructure.

If the integrity of the data is compromised, it will lead to the exploitation of network devices and the entire IoT platform. The data in transit must be safeguarded from change. Data integrity can be ensured by utilising the

keyed-Hash message authentication code technique (HMAC), which operates on the premise of keeping a private key; because it requires a shared private key, it must be secured just like any other cryptographic key.

2.2.4 Cyber Threats and Their Detection

Along with its appealing benefits, IoT technology has introduced a number of security issues. Smart technologies, from the standpoint of the user, have made our daily life activities easier and more precise. However, from a network standpoint, the increasing nature of IoT networks makes them vulnerable to significant cyber attacks. Cyber attacks can be used to: Degrade physical devices and appliances connected to the IoT network. Misuse incoming and outgoing network traffic. Stop network functionality. At the router and switch levels, many attack detection mechanisms can be used. Intrusion prevention systems (IPSs) Firewalls Intrusion detection systems (IDSs) Access control lists, for example (ACLs)

IDS is a potential threat detection system that limits the misuse of IoT smart devices. The intrusion detection system (IDS) is installed on border routers. It analyses inbound and outbound network traffic and issues alerts when malicious activity is detected. This proactive detection approach, however, is insufficient for deep packet analysis.

2.2.5 Threat Mitigation

It is a precautionary action used when a danger has been reported. It studies the impact of a threat on the network and the regions of the IoT network that are afflicted. Current IoT networks necessitate models that mix cyber and physical security. For example, the banking industry employs information security that employs Honeypots to identify potential attack spots. Honeypot focuses on a variety of services, including HTTP, SMTP, SSH, FTP, and others. It has the advantage of providing a transparent forecast of current and future attacks.

2.2.6 Malware Resistance

In an IoT network, malware disguises itself as a genuine network user/device and attempts to authenticate using a common username and password. It successfully circumvents the login method before issuing damaging commands in order to exploit data integrity and lead to disruptive device chapters. It may further disrupt the Internet connection and render the gadget inoperable. It may overwrite or destroy device configurations, as well as wipe out external hard drives. On October 16, 2016, the Mirai software began a damaging DDoS attack. It was written in C and aimed at embedded devices running Linux, such as CCTVs, DVRs, routers, and so on. It was capable of self-propagation via brute-force telnet passwords.

Malicious code is executed by the malware. This code can be delivered to a device by spam email or pictures and activates the installation when it is opened. To defend against Mirai, use a strong password to secure IoT devices. Backups should be performed on a regular basis, and network traffic should be caught and examined

by experts. To remotely access Linux accounts, disable Telnet login and use SSH. Network equipment are less vulnerable to attacks if they are constantly updated and login credentials are changed over time. It is critical that robust encryption standards are adopted for the IoT system to prevent intruders from accessing it.

III. Security Requirements in IIoT

The goal of the industrial Internet is to improve the efficiency and productivity of the manufacturing process throughout the supply chain (Figure 1.2).

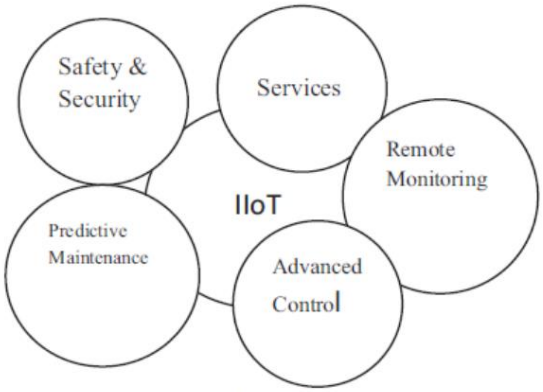

Figure 1.2 IIoT operations.

IIoT comprises businesses with high stakes, such as oil and gas supply chains, power grids, heavy machinery, and sensors. Any security compromise in these applications could have serious consequences for business solutions. Data security may be jeopardised. Ignoring security and privacy concerns could jeopardise not only user activity but also device performance and functionality. IIoT security encompasses concerns about safety and dependability.

Vehicular Sensor Networks (VANETs)

A car is regarded as a node in a vehicular ad hoc network (VANET) that transmits messages among vehicles. It is a subset of IoT that might be referred to as IoV. Vehicles are intelligent devices with sensors and IP-based communication. A VANET transfers messages between intra-vehicle components, vehicles, and humans. Message processing is based on vehicle sensing capabilities. A VANET strengthens the foundation of an Intelligent Transportation System (ITS), which has the capacity to provide a diverse set of applications to its clients and serves as a roadside infrastructure for utilizing security and services.

3.1.1 Sensors in VANET

Sensors in VANET can be divided into two types: 1. Autonomous Sensors: Acceptance range threshold (ART) and mobility grade threshold (MGT) are examples of these sensors (MGT). These parameters take into account the maximum communication range and limit the number of entities in a specific area. 2. Cooperative Sensors:

These sensors incorporate actions and techniques for practising the exchange of neighbour tables about data and position among peer vehicles.

3.1.2 Security in VANET

The security of a VANET is determined by its cost, trust, privacy, and deployment. Vehicles in certain nations are issued with electronic licence plates (ELPs), which contain a cryptographically verified number. The PKI in the context of VANET is known as VPKI, and it includes certification key distribution, certificate revocation, data recording, and so on.

3.2 IoT-Enabled Wearable Devices

The market for wearable smart gadgets is a hot topic in the Internet world. These devices offer a comprehensive set of capabilities for a variety of IoT solutions. Wearable device trends have a wide range of applications in the health care and fitness industries. Wearable biometric sensors can assess heart rate and oxygen levels in the bloodstream, track body temperature, and warn of the danger of contracting the flu or cold. A wearable device could detect if the back seat of a car is improperly adjusted, causing back discomfort. It may assess perspiration levels and hence provide an alarm for altering temperature and humidity in an AC room or car when worn as a bracelet. Fitness trackers, smart watches, smart glasses, infant monitoring devices, and clothing-based wearables are examples of IoT wearables utilised today. Wearables will replace smart phones for 43% of people, according to a survey.

3.3 IoT in Smart Homes/Cities

A smart city based on the IoT paradigm employs a variety of communication protocols for various data formats. It also models data processing using artificial intelligence concepts. The smart city or smart house gathers data from a variety of data sources, which are essentially sensors. These sensors could be placed across cities, offices, gardens, public spaces, and markets. Data is collected from smart phones, smart cards, wearable sensors, cars, and other sources. A smart city IoT network attempts to improve building energy, water, and electrical supply management. It also outlines the operations that will be undertaken to improve public transportation, traffic analysis, and population density statistics. Waste management is another growing issue in both rural and urban regions. This might be accomplished with the help of smart homes and smart cities.

3.4 Green IoT

Green IoT refers to the integration of the greenhouse business with IoT. It includes energy-efficient processes that are used to lessen the greenhouse effect of existing systems. It has the advantage of being able to manage the following activities: Crop management involves assessing farming and environmental conditions. To increase agricultural productivity by extending the production time and monitoring less use of chemicals and fertilisers. To judge and analyse soil, water supply, and humidity requirements. To monitor temperature variations. Following an assessment of meteorological and geographic conditions, the green IoT seeks to initiate a series of operations that will result in increased crop output and improve the sustainability of farming areas. Not only that, but it also initiates initiatives to decrease deforestation and increase greener land areas. Certain Green IoT devices track temperature, humidity, and soil management levels using the ZigBee sensor network. Their threshold values are saved to the cloud. The network raises an alarm when the sensor parameters exceed or fall below the threshold. A greenhouse's humidity sensor generates an alarm when the humidity level changes.

3.5 Video Streaming and Data Security from Cameras

Video data is generated at a significantly higher rate than other types of data. Surveillance and security cameras are continually producing video data. For businesses, video data has a high asset value. The unstructured nature of video data makes management difficult. The structured video data is simple to maintain. Companies and business processes are focusing on adopting Video Management Software (VMS) to scan these large amounts of data for statistical processing. This processing is based on specific times, locations, persons, and keywords. A constraint should be kept in mind in the prevention of vital information loss during the marketing, operations, and customer service processing. Cameras are a useful tool for the majority of commercial applications and use cases. Cameras with a wide dynamic range (WDR) supply more details to analytics for decoding information. The resolution of an HD and HDTV camera increases to a higher range. Higher resolutions, on the other hand, require video compression methods due to increased storage use. A network camera's security levels or range are analysed and optimised in real time. The cameras are used to continuously record data. Certain data in this information may be unimportant or ineffective. The data is filtered based on the purpose. Analytics does the filtration. The brain of interconnected IoT devices is analytics technology. Analytics' duty is to assess the security of video data. It provides security power ranging from passive monitoring to intelligent analysis solutions. The collected data can be used to optimise everyday life activities and traffic analysis. Secured video streaming benefits are used for remote access and third-party integration, as well as to implement security policies in the design and implementation of the IoT network video system. As a result, the contemporary smart camera vendors have advanced functionality, bug fixes, and security patches.

3.6 IoT Security Activities

3.6.1 Device Manipulation

A device manipulation attack jeopardises IoT device setup, control, authenticity, and monitoring. Certain devices must be updated on a regular basis. A device's update time is prone to causing device failures and may also increase system downtime. As a result, it is critical that the devices be changed and updated in such a way that the IoT network's revenue is not jeopardised. Device manipulation is concerned with the secure establishment of the device's identification in such a way that it can be trusted. As a result, the purpose of device manipulation is to monitor: Authentication Service provisioning Configuration and version control Software update maintenance.

3.6.2 Risk Management

Risk is a dynamic issue that includes not only vulnerabilities but also the consequences of a threat on the economics, privacy, and network expansion. Risk assessment and a risk avoidance strategy are critical so that firms' legal compliances, business processes, standards, and infrastructure are not broken by an unanticipated external incident.

a) Risk management elements Under risk management, the following aspects are investigated:

1. Vulnerability: An application, service, configuration, or physical component of an IoT that can be abused by an attacker and is vulnerable to threats. A system's vulnerabilities include a lack of computer capacity, poor encryption techniques, and so on.

2. Intention: Attackers carry out attacks in order to gain social, financial, or political rewards. The attack had the desired effect for them. The intent indicates the attacker's terror-oriented and harmful motivations.

3. Repercussions: It is a tradeoff between the level of exploitation an attack can cause and a system's ability to deal with its consequences. Certain attacks are designed to be amusing, but others can cause significant economic damage and even death.

Risk management procedures For risk management, authentication and encryption procedures are utilised. Weak authentication opens the door for network attacks from the outside world. It is simple to obtain login credentials and create a bogus identity. Inefficient encryption algorithms can be broken, hence encryption techniques must be powerful enough to be computationally impossible to hack.

b) Flaws in present risk-management techniques

1. In the realm of cyber security, inadequate authentication is still a serious issue.

2. Passwords are easily hacked and cracked.

3. Strong encryption techniques necessitate the use of additional processing resources and memory.

4. Key management is a challenging and demanding process. Data and privacy risk management in IoT With IoT, the amount of data increases quickly, increasing the space needs for conveying and storing this data. Although data protection is a time-consuming activity, it is critical for business policies and choices. When the Iota network is scaled up, the risks increase. IoTa risk management for data problems, including the separation of individual and aggregate data, as well as important and inconsequential data. Iota risk management assists in determining unacceptable risk situations and the magnitude of their influence on the safety and privacy of IoT network users.

IV. Machine Learning in IoT

Almost all of the new technologies that are being developed today rely on machine learning. It is fundamentally founded on the idea of utilising all data acquired by the machine for analysis. This data source spans in size from raw data to highly processed information and can be many terabytes in size. However, implementing such a sophisticated machine learning system specifically for IoT security is a difficult undertaking. It necessitates a combination of fast processors, efficient classification algorithms, and, most crucially, an effective statistical decision-making process. The amazing rise in IoT deployments around the world is attracting attention to IoT Security, much as Cyber Security was followed by the growth of the Internet in the last few decades. Most technologists, researchers, and practitioners feel that protecting IoT systems will be the most pressing matter in the next years, which will be addressed intelligently using machine learning methodologies. This circumstance is significantly more difficult to programme because IoT brings more treats than the Internet does. Unauthenticated intermediary message processors, open WiFi, various protocols, and faked sensors are becoming more common in IoT systems. Any susceptible or hacked device in an IoT system is more harmful than an invader from the outside, increasing the likelihood of an assault. Furthermore, all IoT system devices have their own memory and processing power, allowing them to bypass or change the control according on the intruder's goals. This also opens up the prospect of newer treats being added to the system.

4.1 Need

A computer system can be guarded by utilising the most recent security software, which is effective as long as the system is not linked to the Internet. Connecting to the Internet introduces significant vulnerability into the system, necessitating the constant operation of updated security procedures in order to maintain the system secure. There are numerous sophisticated software patches available to ensure high-level security, but this also necessitates sufficient memory and computer capability on the host end. Unfortunately, most IoT devices have insufficient CPU power and memory to implement such enormous security methods. This is the most significant factor that makes IoT systems more vulnerable to security threats. Furthermore, having Internet connection to the IoT system exacerbates the dilemma. Search engines such as Shodan are excellent examples of how the

openness of IoT systems may be seen. And anything viewable on the Internet has a one hundred percent probability of being hacked. As a result, in order to avoid such a hostile IoT environment, a complete investigation using machine learning can be beneficial. IoT devices generated millions of data points that might be used by machine learning algorithms to predict aberrant activities and potential threats.

4.2 Levels of IoT Security

The Internet of Things system is made up of several protocols and various peer-to-peer communications amongst the devices involved. Because of the several layers of operating systems, an effective security mechanism is required that provides a comprehensive security solution while working well on all key points of the IoT system. Securing an IoT system necessitates the inclusion of security subroutines primarily at the four levels listed below.

a) Device

It is directly tied to all of the hardware and drivers associated with the devices that are part of the deployed IoT system. It adds security to the physical layers of systems by implementing device authentication via MAC addresses and encryption keys, secure booting, and device identification.

b) Communication

It refers to the idea of safeguarding communication channels between devices linked by an IoT system. Because the majority of communication channels are wireless, the potential hazards of attacks on these channels are very great. To secure these open communication lines, sophisticated technologies such as enhanced public encryption, firewalls, web sockets, virtual tunnelling, and Secure WiFi are used. Furthermore, due to frequent communication delays, these security methods must be quick enough to meet the needs within the time range specified.

c) Cloud

The cloud is the backbone of an IoT system, where all data is collected, categorised, analysed, and processed before being directed back into the system. It is the primary programme responsible for achieving the goals of the whole IoT system. Securing this component of the IoT system is the most difficult assignment, since it is the site of the majority of security breaches.

d) The life cycle

This is a somewhat more complete technique in the IoT system to providing overall system security while controlling the system prompt and upgrading all the time. It ensures that the security measures installed at all of the aforementioned sites function in tandem to create a better level of security protection. The IoT system continually monitors several merits such as risk analysis, auditing, and activity evaluation to give quick and accurate results.

4.3 Automation of Security Mechanisms

The demand for security procedures has expanded in tandem with the growth of IoT devices. These tasks, such as certificate allocation and revocation, blacklisting of rogue nodes, and isolating compromised devices, are typically conducted manually. Better security mechanisms must be integrated into IoT systems, which must be not only efficient but also intelligent enough to reduce the need for human intervention in making minor decisions. For example, an intelligent subroutine that can learn from historical data can handle simple classification of hostile nodes based on their behaviour. This automation will allow the IoT system to make suitable security decisions while also making it self-sufficient. We can achieve automation in a variety of methods, such as by using an inference system, a neural network, or a mix of machine learning approaches.

Machine learning techniques are divided into two types: (1) supervised machine learning, in which predictions are made based on a given set of samples by searching for patterns within the labels assigned to data points, and (2) unsupervised machine learning, in which no labels are assigned to data points. It first aggregates the data into clusters to characterise its structure for subsequent analysis, and then (3) reinforcement machine learning, in which an action is performed first, and then the effectiveness of the action is determined. It adjusts the strategy over time in order to learn better and attain the best reward. Machine learning can be used to secure IoT systems at the device or network level. a) Hardware-based solutions The main source of worry in device-based security solutions is a lack of memory and storage capacity for executing subroutines. Devices with sufficient processing power and storage are necessary for better threat analysis and signature and authentication record keeping. Threading and other techniques can help to implement high-level security with fewer resources. c) Solutions based on networks Securing IoT systems can also be accomplished at the network level by registering all devices on the network and conducting frequent audits of data traffic to and from the IoT system. And, if anything goes beyond what is expected or suspicious, alarms can be activated to protect the system's data and control points. Based on their behaviour and previous experiences, this traffic monitoring system might be used to identify and classify hacked nodes.

4.4 IoT Security Techniques Classifications

a) Network security

The key to a high-end security mechanism is protecting and securing the IoT network. However, due to the diversity of communication protocols, standards, and, most crucially, device capacity, it is frequently a more difficult task. To avoid potential hazards from intruders, networks can be protected by firewalls and intrusion prevention systems.

b) Authentication

It allows users to authenticate trusted IoT devices through the use of pin numbers, certificates, or biometrics. It is a manual yet effective approach for avoiding attacks.

c) Encryption

To ensure greater security, it is always preferable to encrypt the data and control. To keep data safe from intruders, many encryption protocols may be utilised. The IoT system can be secured using either public or private key encryption.

d) Analytics

This includes gathering, organising, and analysing data from the IoT system, as well as issuing warnings if any action falls into the worrisome category. To do such analyses, new and improved machine learning approaches might be used.

CONCLUSION

The fourth industrial revolution has paved the way for machine-to-machine (M2M) communication, allowing for high automation. Machines may now talk and share information in order to understand one other and achieve certain goals. These goals must be well-programmed in order to protect privacy and be prepared for potential security breaches. However, because of the minimal human participation in this entire scenario, security is frequently jeopardised. As a result, improved approaches in M2M communication must be implemented at negotiation, authentication, execution, and information exchange points. These technologies are getting more intelligent in their ability to perceive and identify security assaults while also strengthening the overall system and making it more resilient to new IoT attacks. Version incompatibility concerns, as well as system and firmware versioning, make this situation more vulnerable. Machine learning has evolved into an essential tool for IoT security. Through pattern identification, real-time cyber crime mapping, and extensive penetration testing, machine learning and approaches prevent cyber threats and strengthen security infrastructure.

REFERENCES

[1] The Guardian, ―Us unemployment and employment statistics,‖ https://www.theguardian.com/business/us-unemployment-andemployment-statistics, 2020, [Online; accessed June 30, 2020].

[2] O. Novo, N. Beijar, and M. Ocak, ―Capillary Networks - Bridging the Cellular and loT Worlds ,‖ IEEE World Forum on Internet of Things (WF-IoT), vol. 1, pp. 571–578, December 2015.

[3] F. Hussain, Internet of Things; Building Blocks and Business Modles. Springer, 2017.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ―Internet of things: A survey on enabling technologies, protocols, and applications,‖ IEEE Communications Surveys Tutorials, vol. 17, pp. 2347–2376, Fourthquarter 2015.

[5] J. Granjal, E. Monteiro, and J. S. Silva, ―Security for the internet of things: A survey of existing protocols and open research issues,‖ IEEE Communications Surveys Tutorials, vol. 17, pp. 1294–1312, thirdquarter 2015.

[6] A. Mosenia and N. K. Jha, ―A comprehensive study of security of internet-of-things,‖ IEEE Transactions on Emerging Topics in Computing, vol. 5, pp. 586–602, Oct 2017.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, ―A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,‖ IEEE Internet of Things Journal, vol. 4, pp. 1125–1142, Oct 2017.

[8] M. Ammar, G. Russello, and B. Crispo, ―Internet of things: A survey on the security of iot frameworks,‖ Journal of Information Security and Applications, vol. 38, pp. 8 – 27, 2018. [12] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, ―A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,‖ IEEE Communications Surveys Tutorials, vol. 20, pp. 3453–3495, Fourthquarter 2018.

[9] F. Restuccia, S. DOro, and T. Melodia, ―Securing the internet of things in the age of machine learning and software-defined networking,‖ IEEE Internet of Things Journal, vol. 5, pp. 4829– 4842, Dec 2018.

[10] International Monetary Fund, ―World economic outlook, april 2020: The great lockdown,‖ https://www.imf.org/en/Publications/WEO/Issues/2020/04/14/weo-april-2020, 2020, [Online; accessed June 30, 2020].

[11]. D. Evans, "The Internet of Things How the Next Evolution of the Internet is Changing Everything," CISCO, 2011. 2. K.Gurulakshmi and A.Nesarani, "Analysis of IoT Bots against DDOS attack using machine learning algorithm," in 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018), 2018.

[12] M. Ferguson, D. A. Cummings, C. Fraser, J. C. Cajka, P. C. Cooley, and D. S. Burke, ―Strategies for mitigating an influenza pandemic,‖ Nature, vol. 442, no. 7101, pp. 448–452, 2006.

[13] Granjal J, Monteiro E, Silva JS (2015) Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Survey Tutor 17(3):1294–1312.

[14] Hodo E et al (2016) Threat analysis of IoT networks using artificial neural network intrusion detection system. In: 2016 International Symposium on Networks, Computers and Communications (ISNCC), pp 1–6.

[15] Koroniotis N, Moustafa N, Sitnikova E, Turnbull B (2018) "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset," arXiv preprint arXiv:1811.00701.