IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 17, Issue 5 Ser. II (Sep. – Oct. 2022), PP 13-20
www.iosrjournals.org

Internet of Things: Vulnerabilities & proposed mitigations

Dr. Rishabh Das

Abstract— *The number of vulnerable embedded computing devices connected to internet have exploded recently as a plethora of low-cost Internet-of-Things (IOT) products have reached the marketplace. This shifting technological paradigm presents a possibility of life-threatening scenarios due to insecure design frameworks. This report focuses on highlighting the attack vectors that can be exploited and discusses some research direction being pursued by researchers which can help in mitigating the eminent threat posed due to the boom of IoT devices.*

Keywords— *Internet of Things, Cloud offloading, Intrusion detection systems, Vulnerabilities & Mitigation.*

Date of Submission: 20-09-2022 Date of Acceptance: 05-10-2022

I. INTRODUCTION

Internet of Things (IoT) refers to any peripheral device for controlling specific or multiple tasks with physical objects or “things” embedded with electronics, software, sensors, actuator, low powered computing chip and network connectivity, which enables these objects to collect and exchange data thereby creating an interconnected and sometimes self-aware computing network. This allows the process control parameters observable and controllable remotely, thereby creating direct integration between the physical and cyber worlds [1]. Since the physical process controlled by the IoT devices are so diverse the scope of IoT devices is not well defined. According to Cisco white papers on IoT devices,” The scope of IoT is the computing infrastructure to enable an ecosystem in which there are more “things” connected to the Internet than people.” [2].

II. RECENT BOOM IN IOT DEVICES

According to the census in early 2003, 500 million computing devices connected to the Internet in a world of about 6.3 billion people with a device-to-people to ratio of 0.08. Most companies and agencies predicts that by 2023 the number of connected devices will implode to an astounding 50 Billion with the predicted population being 7.5 Billion, thus leaving a device-to-people ratio of 7 [3]. This growth is over 80 times the growth of the population growth and the number of connected devices will keep growing to 125 Billion by 2030 [4]. These projections are based on what is currently known to be true and do not account for the rapid advancements in Internet or gadget technology. The number of connected devices per person also increases significantly when the population sample is reduced to those who are already online. The device-to-human ratio is calculated using data from the entire world's population, the majority of whom is not yet online. The predicted growth trend of connected IoT devices from several sources are shown below in Table I.

TABLE I. PREDICTED NUMBER OF IOT CONNECTED DEVICES BY 2023

Source	***Time of Release***	***IoT Devices***
NCTA [5]	Oct 17, 2017	50.1 Billion
Statistica [6]	Jan 8, 2018	50 Billion
Juniper Research [7]	Dec 21, 2016	46 Billion
IHS Markit [8]	Mar 15, 2017	52 Billion

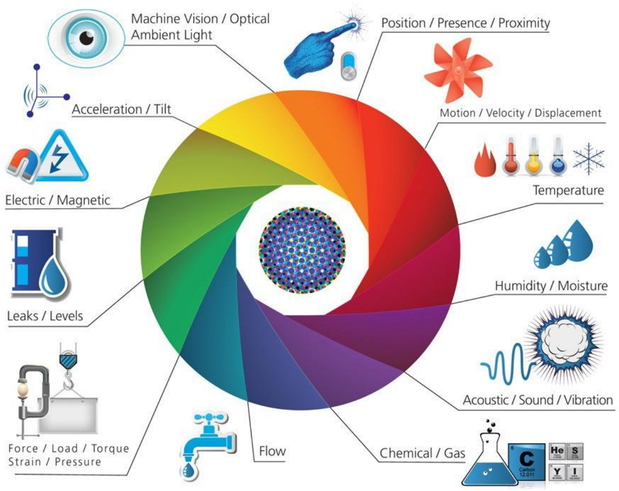
Machine Vision / Optical Ambient Light
Position / Presence / Proximity
Acceleration / Tilt
Motion / Velocity / Displacement
Electric / Magnetic
Temperature
Humidity / Moisture
Leaks / Levels
Acoustic / Sound / Vibration
Force / Load / Torque Strain / Pressure
Flow
Chemical / Gas
C
He
S
Y
I

Fig. 1. Variety of physical systems controlled by IoT devices*) [5]*

One of the primary reason for such astounding growth is the diverse utility that is served by the connected IoT devices. Few environmental process parameters controlled by IoT devices are illustrated in Figure 1 above.

III. HISTORICAL ATTACKS ON IOT DEVICES

The boom of IoT devices started from early 2013 encompassing everything from automobiles, environmental sensors, medical devices and household devices. The hardware or software component of these devices are developed by different suppliers resulting in a scattered and overly prolonged supply chain. Once interconnected, huge amounts of data is captured and transmitted over these devices and any compromised node (hardware or software) can make the entire interconnected system vulnerable to a wide array of attacks. The scattered supply chain and the low computing power of these interconnected devices makes the implementation of secure framework a challenge. In recent years, these insecure IoT devices have been exploited by a number of attackers. This section discusses few popular attacks on IoT devices.

A. Mirai Botnet

In October of 2016, the largest ever distributed denial of service (DDoS) attack was launched against a DNS provider Dyn. This network flood caused multiple major websites hosted by Dyn like Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, CNN, Reddit, the Guardian to go down [9].

This major DDoS attack was made possible by a malware called the Mirai which compromised IoT devices like digital cameras and DVR players. Mirai takes advantage of devices running out-of-date versions of the Linux kernel and once infected, the computer searches for more vulnerable IoT devices. The fact that most of these IoT devices uses default user name and password was taken advantage of by the Mirai botnet [10].

IoT security lessons from Mirai Botnet attack: -

- A lot of times the IoT device manufactures would trim the device storage down to bare minimum to reduce manufacturing cost. This hinders the ability of getting device updates. These systems with no patching capability should never be implemented.

- Any device installed online should require users to change the default username and password.

- Passwords of IoT device should be unique per device.

- All manufacturing companies should have an approved department for developing patch and firmware updates to mitigate vulnerabilities.

B. "Cold" in Finland

In November 2016 the heating system of multiple buildings were compromised by cyber criminals in the city of Lappeenranta. The attackers managed to DDoS the system which resulted in frequent rebooting of the system.

Since The temperature in Finland is really low, heating systems are really important and this makes the attack really significant [9].

IoT security lessons from Cold DDoS attack in Finland: -

- The network connecting the IoT devices to the Internet should be monitored for suspicious activities.
- Response to any suspicious network activity is to be well defined so that once detected the operator or any automatic monitoring framework can respond to it appropriately.

C. Brickerbot

The Brickerbot works similar to the Mirai botnet by compromising IoT devices using default user name and password. An advanced module in the bricker bot not only allows the malware to send malicious DDoS network packets to other computers but also kills the IoT device making it really dangerous [9].

IoT security lessons from Brickerbot: -

- Any device installed online should require users to change the default username and password.

D. The Botnet Barrage

As per the reports of Verizon Wireless 5000 IoT devices were compromised in an unnamed university. The botnet broke through weak password on IoT devices using brute force attack. Each infected IoT device were making hundreds of DNS lookup every 15 minutes. The network connectivity of the university was slowed down and high volumes of alerts were generated by the name server [9].

IoT security lessons from Botnet Barrage attack: -

- The network connecting the IoT devices to the Internet should be monitored for suspicious activities. Response to any suspicious network activity is to be well defined so that once detected the operator or any automatic monitoring framework can respond to it appropriately.

- For the installation of any device on the Internet, changing the default username and password should be required.

E. The Hackable Cardiac Devices from St. Jude

The FDA confirmed that the medical implantable devices by the St. Jude is vulnerable and the hackers can compromise the implanted device due to some existing vulnerabilities. Once the hackers compromise a medical device they can deplete the battery or administer incorrect pacing or shocks. These devices which are supposedly implanted to prevent heart attacks can prove fatal if compromised. Moreover, a lot of the implants remotely transmits data to the physician. The hacker can compromise the transmitter remotely to gain access to the implant [10].

IoT security lessons from vulnerabilities in cardiac devices: -

- It is better to keep life critical medical implants disconnected from internet.
- A strong security team should be employed to update firmware and the vulnerabilities if found.

F. The Owlet WiFi Baby Heart Monitor

These heart rate monitors are designed to keep parents aware if their babies are having heart trouble or not. But again these devices can be exploited by attackers and sinister party to transmit wrong data [10].

G. The TRENDnet Webcam Hack

TRENDnet started marketing their webcam in early 2010 primarily for monitoring home and babies. These webcams were marketed as secure and the company assured updates and security patches when ever necessary. Because of their faulty software hacker were able to obtain the IP address of the cameras. These IP addresses were used and finally the cameras were compromised. Moreover, TRENDnet used to transmit user login credentials in clear, readable text over the Internet, and its mobile apps for the cameras stored consumers’ login information in clear, readable text on their mobile devices. This made it easier for the hackers to compromise the system [10].

IoT security lessons from vulnerabilities in TRENDnet Webcam: -

- Latest security advancements should be incorporated in the end products where ever possible.
- Login credentials should always be encrypted end-to-end.

IV. ATTACK VECTORS

From the discussion in section 2 it is quite evident that IoT though new to the world of technology, its sheer diversity, interconnectivity and the overextended manufacturing supply chain has resulted in a cyber space rife with vulnerabilities and exploits waiting to be taken advantage of. This section discusses the attack vectors that might be exploited by any potential attacker.

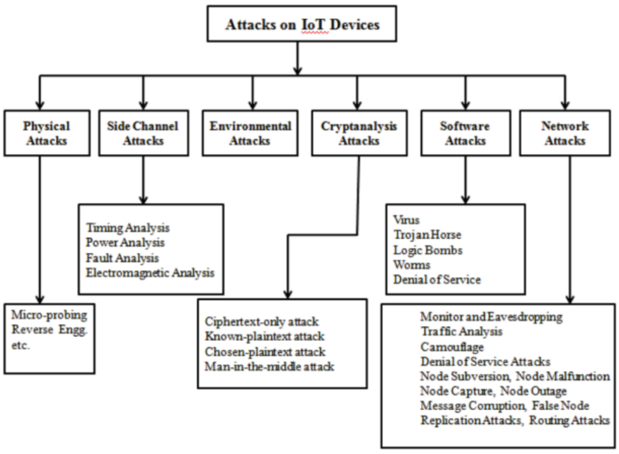

Fig. 2. Attack Vectors in IoT Devices *[11]*

Figure 2 shows the attack vectors using which the vulnerabilities associated with the IoT device might be taken advantage off by attackers.

A. Physical Attacks

Physical attacks involve either tampering with the components of the connected IoT devices or embedding malicious hardware components in the IoT device. Some other examples are depacking of chip, layout reconstruction, micro-probing, and particle bean techniques.

B. Side Channel Attacks

Side channel attacks are based on “side channel information” that can be retrieved from the encryption device itself. The encryption device produces timing information that is easily measurable, radiation of various sorts, power consumption statistics, and more. These attacks make use of some or all of this information to recover the key the device is using. Logic operations are based on physical characteristics that depend on the data used. Timing attacks, power analysis attacks, fault analysis attacks, electromagnetic attacks and environmental attacks are a few examples of side channel information. [12]

C. Cryptanalysis Attacks

Cryptanalysis attacks are focused on breaking the encryption. They try to find the encryption key to obtain the plaintext. Examples of cryptanalysis attacks include Ciphertext-only attack, Known-plaintext attack, Chosen-plaintext attack, Man-in-the-middle attack and others.

D. Software Attacks

Software attacks are the major source of security vulnerabilities in any system. A software attack exploits a flaw in the design and implementation of a system by using its own communication interface to inject malicious code into that system. These attacks may include buffer overflows, which allow attackers to inject malicious code into applications; trojan horse programs, worms or viruses that deliberately exploit bugs in software to spread infection; or other kinds of malicious code injection attacks.

E. Network Attacks

Wireless communications systems are vulnerable to network security attacks due to the broadcast nature of the transmission medium. These attacks are classified as active and passive attacks. Passive attacks include eavesdropping, traffic analysis, and camouflage adversaries; active attacks include denial-of-service attacks, node subversion, node malfunction, node capture, node failure, message corruption, false nodes and routing attacks.

V. RESEARCH EFFORTS FOR SECURING IOT DEVICES

A. Intrusion detection/prevention system

Intrusion detection or prevention system have always been a part of the security architecture. Due to low computing power of the IoT devices it is often challenging to embed or implement such algorithms in a IoT framework. In this section a few intrusion detection system for IoT devices are discussed.

Gupta et al. (2013) proposed an architecture for a wireless IDS. In the proposed novel architecture Computational Intelligence algorithms was used to construct normal behavior profiles for network devices. Each devices were distinguished from the other using their IP address and a separate normal profile was created for device have unique IP address. The authors employed a novel framework to deploy the proposed IDS in networks with low capacity devices [13].

Summerville et al. (2015) developed a deep-packet anomaly detection approach that aims to run on resource constrained IoT devices. The author argues that even though the the low powered small IoT devices use a handful of simple protocols but the network payloads are still very similar to more complicated devices using different protocols. A novel technique called the bit-pattern matching is performed to carry out a feature selection. The network payload are treated as bytes and the sequence of bytes are arranged similar to overlapping tuple of bytes called the n-grams. The feature selection process is performed on these n-grams.The n-gram matched the bit pattern once all the corresponding bits matches in all positions. The framework was evaluated using two distinct experiments both of which exhibited low false positive rates for four different attack types:worm propagation, tunneling, SQL code injection, and directory traversal attacks [14].

Thanigaivelan et al. (2016) briefly introduced a distributed internal anomaly detection system for IoT. Any discrepancy or anomaly in the network is monitored by observing the neighboring node one hop away from the parent node. Features like packet size and data rate is monitored in the neighboring nodes. The normal behavior of the system is learned from these features. no details are provided on how the learning or the detection process works. Although the author claims that the IDS will work on low powered devices no evaluation is performed to support the claim [15].

Pongle and Chavan (2015) presented an IDS designed to detect wormhole attacks in IoT devices. This research assumes that the wormhole attack always exhibits specific characteristics on the system. During the wormhole attack the author assumes that high number of control packets would always be exchanged between the two ends of the tunnel or the number of neighbors would always increases drastically. Three distinct algorithms are proposed to detect such wormhole attacks on the system.Performed experiments confirms true accuracy rates as high as 94\% for the detection of wormhole attacks and 87\% for detection both the attacker and the attack. Because the power and the memory consumption of the system is low the proposed system is suitable for IoT devices [16].

Zarpelão et al. performed a comprehensive survey of all popular intrusion detection system for low powered and IoT devices [17].

B. Cloud offloading architectures

The controllers used in IoT devices have limited processing resources. Hence the state of the art resource-intensive algorithms like deep learning, recurrent neural network and support vector machine cannot be used. This limitation of hardware hinders the capability of the IDS and greatly limits the premise of IDS research. Secondly, any state of the art security framework being used in a more resource intensive environment cannot be ported over to these low powered devices. Researchers are investigating on leveraging the computational power of cloud computing.

Loukas et al. introduces a novel data offloading technique which allows the low powered controllers to leverage the power of cloud computing and in this manner more advanced techniques can be used to improve the performance of embedded (onboard) IDS [18].

The three main contributions of this research can be enumerated as follows:

- Implementation of two deep learning based neural network to classify data collected from multiple sensors onboard the vehicle.

- Implementation of the proposed offloading cloud-based architecture to perform real-time intrusion detection for the low powered controllers. Three different attack vectors were validated on the framework.

- Detection latency is used as a criterion to develop a mathematical model that determines if computation offloading is beneficial when the operational parameters of the network and the processing demand of the deep learning model are known.

A four-wheel mechanical autonomous land vehicle is developed to demonstrate the suitability and efficiency of offloading the continuously monitoring IDS to a cloud-based computer. Two distinct resource-intensive deep learning algorithms (multilayer perceptron and recurrent neural network) are validated using the proposed framework. Continuous time series data is provided as an input to the recurrent neural network (RNN) and because the RNN uses directed graphs (which exhibits dynamic temporal behavior for a time sequence data) the RNN stores the previous states of the time series data using its internal memory (called the Long short-term memory) and boosts the accuracy of the IDS. The deep learning algorithm exhibits much better results when compared to standard machine learning approaches and it has the capability to detect multiple attack vectors across a wide variety of protocols. For the present analysis, the algorithm was trained to detect cyber-attacks like denial of service, command injection and malware affecting autonomous vehicles [18].

To handle large volumes and dimensionality of data in cyber-physical systems a novel distributed intrusion detection based on hybrid gene expression programming and cloud (DID-HGEPCloud) computing is proposed. MapReduce algorithm is used to handle massive volumes of data with higher dimensionality.Moreover to improve the efficiency and accuracy of intrusion detection, model based on non-linear least squares is applied [19].

The main contributions of the research are as follows:

- A novelty attribution reduction algorithm (ARND-RS) is developed to reduce the time requirement of IDS framework for complicated cyber-physical systems having high data dimensionality and massive volumes of data.

- A novel IDS framework based on the hybrid gene expression programming (ID-HGEP) is combined with gene expression programming and the novelty reduction algorithm (ARND-RS). Appropriate function model representing the data flow and the attack type is chosen by the ID-HGEP algorithm. Data streams having normal or abnormal data can be distinguished using these function models.

- For efficient handling of massive and high dimensional net flow data from the complicated cyber-physical system, a novel distributed cloud computing framework is proposed.

VI. OPEN RESEARCH QUESTIONS AND CONCERNS

A. *Insecure wireless connections*

The IoT relies heavily on wireless communications to provide connectivity for smart objects. In some use cases such as body area networks (BANs)— wireless networks of wearable devices—wireless communications are necessary because of their mobility requirements. Yet, even in scenarios where smart objects remain mostly static, such as in smart homes, wireless communications are abundant, mainly because of their convenience and for aesthetic purposes (the lack of wires). However, their open nature makes wireless communications more susceptible to eavesdropping or other forms of privacy degradation [20].

The most representative example of this is the case of Global System for Mobile communications (GSM), which is a second-generation (2G) cellular technology. Although obsolete by today’s wireless standards, GSM still holds 77 percent of all cellular machine-to-machine (M2M) traffic, and will continue to be the dominant choice for cellular IoT communications until 2023, according to Forward Concepts. GSM has been proven to be vulnerable to a large variety of attacks. Its main security issues stem from the adoption of the problematic A5/3 (Kazumi) algorithm, support for unencrypted communication mode (A0), and the fact that authentication is unilateral. In particular, the latter allows an attacker to pose as a fake base station using inexpensive hardware and open source tools such as Universal Software Radio Peripheral (USRP), OpenBTS, and Asterisk. A practical attack in which the attacker set up a fake base station against GSM was demonstrated at DEFCON 18. As soon as a benign client was lured by the fake station’s stronger signal, it was instructed to operate in the least secure cipher mode (preferably A0) so the attacker could easily intercept all unencrypted traffic.

B. *Hardware diversity*

IoT applications and related hardware are extremely diverse. Even with confined application domains such as home automation, there are devices that rely on an 8-bit CPU clocked at 8 MHz, along with devices that are equipped with a 32-bit CPU running at 1 GHz. This creates a very challenging landscape for a single framework to satisfy such diversity without facing compatibility and security issues.

Research has shown that minimalistic processors such as the ones used in IoT applications (for example, Atmel ATmega128L, which empowers Arduino boards) can handle both symmetric and asymmetric encryption, yet further investigation is needed regarding the type, viability, and extent of cryptography that can coexist with real-life IoT applications. Critical questions revolve around whether heavy cryptographic procedures drastically undermine the time constraints of some applications, as well as their impact on the devices’ energy consumption rate.

Furthermore, the majority of the IoT transport protocols were designed to support multiple protection levels. With these options, an attacker might be able to manipulate protocol execution to downgrade the negotiated level of security (to, for example, no protection)
and freely unleash attacks.

Finally, the diversity of hardware in combination with the dependency of IoT applications on mesh topologies create a potentially dangerous scenario where data originating from higher-end devices might have to be routed through lower-end devices that support weaker cryptographic algorithms or don't support cryptography at all.

C. Identifying every "thing"

One vision for the IoT is to tag all objects with a unique identifier and allow the objects to be reachable through a persistent Internet connection. IPv6, with its gigantic pool of addresses, could make this vision a reality. However, a flaw in IPv6's stateless address autoconfiguration mechanism allows eavesdroppers and other information collectors to identify and track nodes. The most significant bytes of the addresses in IPv6 are defined by the network, whereas the least significant ones are derived deterministically from the interface's media access control (MAC) address.

Exposing a device's MAC address through a universal IP address imposes a privacy risk. This has led to the amendment of IPv6 with an additional protection mechanism—the IPv6 privacy extensions8—whereby a host can generate and assign itself a randomized IP address at every specified interval. Nevertheless, even this mechanism has weaknesses because the interval parameter can't be set to a small value when usability is necessary, while large values defeat the purpose of the mechanism. In any case, it's debatable whether a unique identifier is necessary for the majority of IoT applications

D. Data in the cloud

The IoT ecosystem encompasses several cooperating modules of functionality, the most prominent of which deals with the management of sensor derived data. In fact, the storage, processing, and reselling of the data gathered by sensors is considered by some to be the driving force behind the IoT.

Researchers and practitioners envision cloud services being able to auction large volumes of user data and resell it to third parties. Potentially, even end users will be able to sell their raw, daily data feeds. These scenarios could be catastrophic in terms of end users' privacy. Anonymization schemes are often treated as a panacea, but many have been found incapable of providing a holistic solution. For example, the popular k-anonymity11 scheme was proposed to protect against the correlation of anonymized records. That scheme seeks the right subset of characteristics for each record of a given dataset, which makes the records indistinguishable from a number of at least k-1 other records. k-anonymized schemes can break when faced with low-diversity data or attackers with the advantage of background knowledge.

REFERENCES

[1]. C. Kolias, A. Stavrou, and J. Voas. Securely making ”things” right. Computer, 48(9):84–88, Sept 2015.

[2]. Rolf H. Weber. Internet of things – new security and privacy challenges. Computer Law and Security Review, 26(1):23 – 30, 2010.

[3]. S. Ray, Y. Jin, and A. Raychowdhury. The changing computing paradigm with internet of things: A tutorial introduction. IEEE Design Test, 33(2):76–96, April 2016.

[4]. Jenalea Howell. Number of connected iot devices will surge to 125 billion by 2030, ihs markit says - ihs technology, Oct 2017.

[5]. Justin Baker. Internet of everything: The iot market is projected to expand 12x from 2017–2023, Oct 2017.

[6]. Yogesh Jain. 13 iot statistics defining the future of internet of things, Jan 2018.

[7]. Donal Power, Brad Anderson, Arash Asli, Peter Daisyme, and John Occhipinti. Iot devices go forth and multiply, to increase 2002016.

[8]. Louis Columbus. Roundup of internet of things forecastsand market estimates, 2016, Nov 2016.

[9]. Jack Wallen. Five nightmarish attacks that show the risks of iot security, Jun 2017.

[10]. The 5 worst examples of iot hacking and vulnerabilities in recorded history, Feb 2018.

[11]. S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad. Proposed embedded security framework for internet of things (iot). In 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), pages 1–5, Feb 2011.

[12]. Armin Wasicek. Security considerations in embedded systems. April 2018.

[13]. A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle. Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks. In 2013 IEEE International Conference on Computational Intelligence and Computing Research, pages 1–7, Dec 2013.

[14]. D. H. Summerville, K. M. Zach, and Y. Chen. Ultra-lightweight deep packet anomaly detection for internet of things devices. In 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), pages 1–8, Dec 2015.

[15]. N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho. Distributed internal anomaly detection system for internet-of-things. In 2016 13th IEEE Annual Consumer Communications Networking Conference(CCNC), pages 319–320, Jan 2016.

[16]. P. Pongle and G. Chavan. Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications, 121(9):1–9, jul 2015.

[17]. Bruno Bogaz Zarpel˜ao , Rodrigo Sanches Miani, Cl audio Toshio Kawakani, and Sean Carlisto De. A Survey of Intrusion Detection in Internet of Things. Journal of Network and Computer Applications, 84(January):25–37, 2017.

[18]. G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. IEEE Access, 6:3491–3508, 2018.

[19]. B. Li, R. Lu, W. Wang, and K. K. R. Choo. Ddoa: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. IEEE Transactions on Information Forensics and Security, 11(11):2415–2425, Nov 2016.

[20]. W. Trappe, R. Howard, and R. S. Moore. Low-energy security: Limits and opportunities in the internet of things. IEEE Security Privacy, 13(1):14–21, Jan 2015.

Dr. Rishabh Das. "Internet of Things: Vulnerabilities & proposed mitigations." *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, 17(5), 2022, pp. 13-20.