**ANALYSIS OF SECURITY THREATS ON DATA CENTERS**

**IN INTERNET OF THINGS**

**Abstract**

The recent increase in Internet of Things (IoT) adoption has accelerated integration and expanded the Internet's reach beyond PCs, tablets, and smartphones. The Internet of Things (IoT) enables the Internet to become increasingly pervasive in our daily lives. While the Internet of Things (IoT) devices open up limitless new possibilities and simplify life, they also significantly enhance the opportunity for unscrupulous people, criminal organizations, and even state actors to spy on and interfere with unsuspecting IoT system users. Indeed, they are. Predictive models taught using machine learning algorithms have tremendous promise for reducing some of these issues as the impending crisis deepens, as a recent study shows. The research begins by assessing IoT security concerns using analytics and then proposes a machine learning-based method for categorizing and detecting IoT threats. The research seeks to explain the IoT system in detail using this real-world IoT system as a platform, including its capabilities for documenting security concerns and system attacks. The research assesses the accuracy of prediction models trained using machine learning utilizing a nine-month test period of data collection as our testbed. Following that, this research offers design suggestions and a foundation for developing secure IoT systems.

Table of Contents

[**Chapter one** 3](#_Toc86229550)

[**Introduction** 3](#_Toc86229551)

[**Research Objectives** 7](#_Toc86229552)

[**Research Questions** 7](#_Toc86229553)

[**Problem Statement** 8](#_Toc86229554)

[**Summary of chapter one** 9](#_Toc86229555)

[**Chapter Two: Literature Review** 9](#_Toc86229556)

[**IoT security threats** 9](#_Toc86229557)

[**Vulnerability to IoT Security Threats** 12](#_Toc86229558)

[**Solutions to Data Center Security Threats** 13](#_Toc86229559)

[**Impacts of IoT of Data Centers** 15](#_Toc86229560)

[**Summary of Chapter Two** 16](#_Toc86229561)

[**Reference List** 17](#_Toc86229562)

# **Chapter one**

## **Introduction**

The world's growing reliance on networked technology has never been more substantial than today, owing to the development of cloud and on-premise information services, which have spawned a new class of services dubbed the Internet of Things (IoT). Through IoT services, consumer electronics, home appliances, industrial controls, and industrial sensors may all be connected to the Internet of Things. When used in conjunction with more conventional Internet-connected equipment like routers and servers, these IoT systems and services may offer a higher level of automation and functionality. Despite its immaturity at the time of writing, IoT is projected to grow from $450 billion in 2020 to $650 billion in 2025. According to specific projections, about $1.85 trillion will be exchanged by 2030.

Regardless of the apparent benefits of the Internet of Things (IoT) devices and services, it is critical to recognize that Internet connection continues to pose security concerns. Connecting everyday home gadgets to the Internet exacerbates the inherent dangers of the Internet. While it's no secret that Internet of Things (IoT) users are concerned about their services becoming ineffective or unusable as a result of poor Internet conditions (such as network segment failures or other technical difficulties), they're now even more concerned about becoming a victim of criminal activity while utilizing IoT products and services. In 2018, attackers' interest in Internet of Things (IoT) systems grew, suggesting the need for more strong security measures to prevent infiltration. This is a massive endeavor in terms of scope and size. Due to many connected devices, the Internet of Things presents a perfect target for hackers (IoT).

As a consequence of a single vulnerability, the number of attackers prepared to start additional assaults may rapidly increase. Numerous factors may jeopardize your life. Unprotected IoT devices make it easier for hackers to get access than protected IoT devices. Consequently, updating and maintaining the software on low-cost IoT devices is more challenging than it is on more costly devices. Since these concerns have been highlighted, much thought and effort have been spent on identifying the difficulties inherent in this new paradigm and providing a more conventional way to addressing the issues presented by the Internet of Things.

This admirable objective may be difficult to achieve due to the increasing number of IoT-enabled products and systems. As the dependence on Internet of Things (IoT) devices increases, so are the associated dangers. As a consequence, a proper IoT security setup is required. The findings of this research indicate that a data-driven defensive architecture may be utilized to evaluate the security of IoT networks. Exposing the dangers and threats that IoT networks face may help academics and practitioners understand the parallels and differences between IoT network security and the broader Internet of Things (IoT).

Additionally, the research aims to create a reference architecture for the Internet of Things that will identify and respond to future threats and security breaches in real-world IoT devices. Researchers examine Internet of Things (IoT) technologies and networks to see whether they pose any dangers or hazards. For the same reason, the development of IoT (IoT) systems is highly dependent on data. By monitoring network traffic for an Internet of Things-based business, the effectiveness of a smartphone-enabled secure entry system for commercial buildings and gated communities may be determined. We'll inform you of our results after we've sifted through 100 petabytes of unstructured packet data. The study examines novel approaches to developing and deploying IoT networks and the associated risks and problems.

Additionally, this research examines how a few variables may help to increase the case in study's security. Based on an assessment of the IoT ecosystem and a case study, the paper presents an IoT framework for building secure IoT systems. Predictive machine learning methods are used to assess and verify the design's components. There are currently only a few publicly accessible security datasets; therefore, validation datasets would be much welcomed. The significance of internet security will only increase in the following years. Since the Internet became widely accessible for commercial reasons, many individuals have expressed worry about its safety. In 1972, Bob Thomas developed the worm. Ten years later, the Internet was taken down using the same technique in a non-malicious proof-of-concept assault. Robert Morris's 1990 computer worm was seen as a failure of experimentation because it almost totally took down the Internet for many days. Since then, many cyber-attacks have occurred.

As our dependence on the Internet increases, the dependability and integrity of Internet-based services must also increase. As a consequence of the Internet of Things, there is an increase in risk. Along with the economy and vital infrastructure, standard household devices such as refrigerators, sensors, locks, and cameras are attacked. There were real security issues early on in the Internet's existence, but they were confined to the network as a whole. As a result, they have grown much more prevalent in reality. According to different projections, there will be about 25 billion Internet-connected IoT devices by 2025. The human population has already surpassed the number of devices connected to the Internet of Things (IoT), such as PCs and smartphones. Gartner estimates that the Internet of Things (IoT) industry will reach $4 trillion by 2035.

By contrast, individuals who hate the industry have a much greater chance of success. Advanced hacking techniques aimed at circumventing established security measures and vendor negligence in bringing goods to market all have the potential to introduce inherent vulnerabilities. The advancement of computing power and criminal organizations' need for network-connected computing resources fueled the growth of botnet armies and paved the way for new avenues of illegal profiting. On the other side, security is often neglected.

These features worry security specialists tasked with protecting our digital infrastructure. Stuxnet is the most well-known of many high-profile assaults on the Internet of Things (IoT). According to claims, a virus developed by the US and Israeli spy agencies penetrated the computer network of an Iranian nuclear enrichment plant in 2011. In 2015, a hacker assault on the Jeep Cherokee's control systems resulted in a mass recall of Jeep Cherokee cars to fix the security vulnerability identified. At the end of 2018, the malware Mirai was created, targeting specific microprocessors brands and taking advantage of weak default passwords. A DDoS security firm developed it. The FDA approved a voluntary recall of about 800,000 pacemakers in 2019 owing to safety concerns.

Although IoT security concerns have garnered considerable attention, this list is not exhaustive. It has taken a long time to develop and apply efficient methods and procedures for protecting networks and computers in the digital era. Apart from being susceptible to the overwhelming majority of today's attacks, IoT devices introduce a deluge of new security issues owing to the many unknowns. IoT systems must overcome three significant obstacles: The restricted capabilities of previous control devices have been phased out and replaced with the Internet of Things (IoT) devices and systems. Certain activities may be accomplished using simple, low-cost equipment. As a result, the activities are constrained in processing and networking capabilities throughout the whole production process, from conception to deployment. It takes much thinking, planning, and design to transform them into IoT systems, but rushing to market risks jeopardizing all of that effort and exposing the methods to severe security risks.

## **Research Objectives**

Research aims to understand different security threats affiliated with IoT system on Data Centers in present era. To achieve this research aim, this study is guided by the following objectives:

* To understand different emerging security challenge in IoT and ways Cyber-threat has become a significant security challenge in IoT system in data centers
* To simulate a business environment and test different solutions to prevent DDoS and other cyber attacks
* To analyze different high-security models and to propose a model for mitigating cyber-security threats in IoT system.
* To propose the incorporation of advanced technologies in addressing cyber security threats to IoT systems through accurate detection and real-time neutralization of the threat.

## **Research Questions**

The research questions on which this research is founded include:

1. What are the shortcomings of existing high-security models for mitigating security threats to IoT data systems?
2. Are data centers diligent enough to ensure that their cyber and physical systems are protected in a united way? Does the unification of cyber and physical systems pose additional security risks to the data centers?
3. How can advanced technologies such as machine learning (ML) and artificial intelligence (AI) be deployed to pinpoint security anomalies in both cyber and physical data systems?
4. Can the solutions found in advanced technologies like AI and ML be generalized for all data center system environments or do different systems have to customize the solutions according to their specific industries?

## **Problem Statement**

Privacy and security make up one of the most significant challenges faced by IoT systems and data centers. Continued advances in digitalization and computer technology have increased the popularity of IoT systems, with the effect of this being that these systems are now being applied in more fields than they had ever been used in the past, which include communication, education, transportation and logistics, as well as business in general. IoT is also the central part of the concept of hyper connectivity, which means that individuals and organizations can communicate with each other effortlessly from remote locations. These factors have made IoT an integral part of modern life and people’s lifestyles have been massively improved by access to the internet that it is inconceivable trying to figure out what life would be without it. However, the unchecked and uncontrolled expansion of IoT and its applications have come along with serious challenges regarding the security and privacy of the people using it as well as their information. For the IoT systems to function effectively, data centers need to be functioning just as effective.

When these centers are accessed by malicious applications, the sensitive data can be bleached and the consequences can be damning. Numerous researches have been conducted to this effect and many solutions continue to be developed. The essence of finding the most amicable solution is high, especially given the diverse nature of applications that target the IoT data centers and systems and also the increasing sensitivity of the data contained in IoT data centers, both physical and in the cloud. This study aims to develop an understanding of the security challenges that IoT data centers face and simulate a suitable solution for the identified challenges.

## **Summary of chapter one**

The researcher believes that this study will assist in better understanding of the many security issues associated with Internet of Things (IoT) technologies used in Data Centers today. Cyber danger has developed into a major security issue for IoT devices in data centers. IoT data centers have a variety of security difficulties, and this research seeks to increase awareness of those issues while simulating a viable solution.

# **Chapter Two: Literature Review**

## **IoT security threats**

The continued expansion of IoT penetration and applications in the modern world has resulted in significant security challenges that evolve similar to the evolution of IoT in complexity and diversity. Data centers continue to evolve to provide infinite scalability and flexibility in order to support the changing strategic goals and the operating needs of diverse organizations. however, like it is the case with any progressive technology, IoT and data centers attract attacks from multiple sources and for multiple reasons. These attacks are the main reason for security concerns, given the extent of information entailed in IoT systems, its privacy, and the destructive nature of infiltration into such systems leading to information being in the hands of malicious people [1]. There are many causes of security breaches, some of which will be highlighted in the vulnerability section below, and any IoT systems manager has to be aware of the types of security threats that pose his or her systems. Knowing the types of security threats to one’s system helps them in anticipating attacks and performing vulnerability or strengths and weakness assessments to highlight the weak points of their systems and bolster them to keep off any attacks [1].

Security threats to IoT systems can be physical in nature. These are the physical attacks or the terror attacks on IoT systems with the target of undermining the data centers and disabling their functioning. These attacks are more rampant in some geographical regions than in others, with the middle East, Africa, and South Asia being among the places where these attacks are a significant security challenge [2]. These physical attacks are characterized by violent intrusions which have a high likelihood of causing damage to the systems in place in the data centers, leading to businesses downtime and other economic losses that may result from customer distrust as well as other stakeholders due to a tainted reputation [2]. Physical threats to data centers include natural disasters, which rank among the top concerns for data centers around the world. Some regions have a higher frequency with natural events such as massive flooding, tsunamis, hurricanes and tornadoes, as well as earthquakes. Organizations require to have data recovery and disaster management plans in the event such disasters affect their facilities in order to mitigate the onslaught of the disaster [2].

Distributed Denial of Service (DDoS) attacks are also a major security challenge for data centers and IoT systems in general. These are attacks which are committed by third parties who have malicious intentions to damage significant IoT infrastructure. The primary aim of DDoS attacks is to cause significant infrastructural damage on the data centers to the point where the business of the target organization is crippled or severely limited. While other attacks are after data breaches and stealing the information, DDoS attacks target the operability and time for an organization with a goal to have the organization out of business for a period. The attacks cause an outage to the organization’s data, which is detrimental to most organization which have an uptime guarantee of 99.99% [3].

Such attacks have been recorded to halt the operations in large organizations, such as the series of DDoS attacks that made online learning impossible in Miami-Dade County public schools in September 2020. The attacks plagued the learning operations by overloading the public-school district’s data center, which eventually disabled the system [3]. As a result, teachers and students were prevented from logging to the system. Many businesses which are reliant on data centers would continue to experience difficulties in their operations if they lack proper security infrastructure to protect their systems from DDoS attacks.

Artificial Intelligence-based attacks have been around for more than a decade, but they are still evolving and are being considered a major challenge for the future more than the present. The threat that emanates from AI-based attacks is becoming more prominent with time. The importance of these attacks in the safety of data centers results from the ease of building tools that are powered by AI as artificial intelligence continues to become a mainstay technology [4]. These tools are faster, more efficient than humans, and they are also easy to scale to carry out the targeted attacks. Within the IoT ecosystem, these attacks and the presence of such tools elicits major concerns because while they appear similar to traditional cyber-attacks, these are especially harder to prevent, predict, and control.

Other security threats come from software intermediaries, such as application programming interfaces (APIs) whose task is to allow for communication between two applications. These interfaces can be a point through which attackers can access the IoT devices in an organization’s network, and this includes the servers. Botnets, which are a series of devices that are connected to the internet, compromise networks, steal data, and send spam into the network [4]. These contain malware that allows their operators to access devices and use them to infiltrate the network. That said, the threats that IoT systems and especially data centers face in their operations are varied and continue to evolve both in complexity and in the range of attack modes. Every organization has to ensure the safety of its data centers to protect them from physical and soft attacks or interference by natural disasters.

## **Vulnerability to IoT Security** Threats

Data centers face security challenges that emanate from a variety of sources. Lack of device management and visibility of the devices in a network is one of the areas which make data centers vulnerable to security threats. With the rise of IoT and cloud computing, many devices continue to be linked in growing networks, but most of them remain untracked and unmonitored, while others are more about improper management than lack of it. As the number of IoT devices connect and disconnect from networks, it is an enormous task trying to monitor them. The lack of visibility into the status of devices in a network can prevent the organization and the data center administrators from detecting potential security threats and devising ways to neutralize them before they pose a greater danger to the entire institution [5].

Data centers are sensitive installations that can be targeted by people who want to physically access the building. This access can be through the use of brute force in the event of a robbery or burglary, or through softer access where the intruders bypass the security systems designed to keep unauthorized people out of the installation. Many organizations use a single-factor authentication system that is password-based. While it works for them, this security system puts them at a vulnerable position where they risk intrusion through simple password guessing, automated attacks, password cracking, and stolen credentials [5]. Data centers may also be vulnerable to weather elements and natural disasters such as earthquakes, storms and others which have a great potential to break down components and render the data centers unusable. Each of these threats has to be faced separately for the collective security goal of the facilities to be assured.

## **Solutions to Data Center Security Threats**

While IoT systems entail a lot of wireless infrastructure, data centers are physical and securing them involves both virtual and physical technologies to protect the centers from external attacks and threats. Data centers have to be secured both physically and digitally due to the sensitivity and importance of the information they hold, such as proprietary information like intellectual property and customer data. physical security encompasses processes and strategies that protect the infrastructure from external attacks and interference. Digital security encompasses software that prevents access into the system by cybercriminals through bypassing the firewall, cracked passwords, or other security loopholes in the system [6].

The most obvious security characteristics of a data center are associated to its layout and design. In this regard, the building containing the infrastructure that makes it a data center may be designed for single-use or multiple purposes. Multipurpose locations may house businesses that are not related to the data center [1]. For security reasons, data centers have to be built in areas where they are away from major roads and other installations in order to create a buffer zone for them where landscaping combines with installed crash-proof barriers to protect them from intrusion. Accessing the data centers needs to be fairly limited since they do not require exterior windows and the entry points also have to be fairly few. Additional physical security is provided by security guards in the building whose role is to monitor activities within the facility through surveillance cameras [1].

Since accessing the facility needs to be exclusive to the people with authority to access the areas, visitors need to use specific authentication when accessing the facility. The authentication system may include scanning the visitors’ personal identity verification (PIV) cards and then requiring them to enter personal passcodes in a two-factor authentication process [7]. Some facilities have employee badge readers and biometric systems such as fingerprint scanners, facial recognition, and iris scanners that may be used to permit visitors entry to the facility. In some facilities, the people accessing the infrastructure there have limited access and exclusivity is given for others. Depending on the sensitivity of data contained by servers in the data center, or upon the request of the company owning the server in the case of data centers that house servers and infrastructure for more than one entity, the servers may be caged separately within the data center [7].

After the physical aspects of security for the data center have been resolved to meet the desired standards, the next thing involves establishing secure zones in the network. Software security aims to prevent hacking, spyware, and malware from attacking or intruding into the network. In the current age, these are, together with ransomware, among the most significant threats to the information stored in data centers. The security posture of a data center is provided in real time by a security information and event management (SIEM) tool. This tool helps manage the security of a data center by providing control and visibility of all components of the data center from the access and alarm systems to all the security sensors installed out in the perimeter fence [8].

Security in the data center can also be layered such that there are secure zones in the network. The administrators in the centers can split the networks into zones which may entail a test area, a development area, and a production area. The flexibility of the network and the security approach can vary with the test area having the most flexible one while the production zone has the most stringent approach to data security [8]. Applications and codes seeking to access the networks have to be scanned for vulnerabilities before they are deployed so that these vulnerabilities are not used to infiltrate the security buffer zones for the center. Software security systems also have to provide metrics and remediation capabilities of the vulnerabilities that are found in applications and codes before they are deployed. Running codes through a scanner can help identify buffer overflows among other vulnerabilities. Data centers require data visibility as a necessity with the rise of cloud computing since there are possibilities of malware being disguised in traffic that is otherwise legitimate [8].

## **Impacts of IoT of Data Centers**

The continuing developments in cloud computing and IoT applications have a great potential to change how data centers approach their operations. A significant point to note is that by the end of 2020, there were about 24 billion IoT devices in data centers while in comparison, only 10 billion such devices were being used by humans [8]. This comparison highlights the impact that IoT will have on data centers, given that the continued growth in this technology will cause a rise in demand for devices connected to networks as well as those within data centers. Data centers will require to expand their capacity to avoid the significant costs and stressors that would result from downtime if the center is incapable of handling the large scale of data. IoT also demands that data centers use modern infrastructure. This is going to be vital for organizations that still use traditional systems because that infrastructure is out and cannot handle the scalability and flexibility demands of IoT devices and networks [2].

## **Summary of Chapter Two**

Data centers face a wide range of security threats which include both physical and digital threats. Physical threats involve intrusion by people into the data centers where infrastructure is stored and causing malfunctioning of the systems in the centers. Digital security threats involve cyberattacks through malware, hacking, and data theft among others. For all types of security threats data center administrators have to approach security using the most stringent methods to ensure that the data center systems and data remain secure at all times. This is especially very important given that IoT is expanding rapidly, increasing demands on data centers and requiring them to keep up with the pace of technological developments.

# **Chapter Three: Methods and Methodology**

## **Sampling**

In this study, probability sampling method will be applied as it I preferred to non-probability sampling due to its specific benefits that support the nature of the study and its objectives. To this effect, this study will employ the systematic form of probability sampling where the firms that will be selected will systematically be selected from a field that is assumed to be infinite. The firms selected in this case will be chosen at regular intervals on the basis of predefined parameters. The parameters on which the firms can be classified and be selected for purposes of collecting data in this case study include the number of employees or relative market size of the company, the value of the data center to the company and/or other companies, geographical location, and the length of time since the company established its data center.

Using this information, systematic clusters of organization for sampling emerges as large companies against medium-sized and small companies. Large companies will be classified as those which have their presence in more than one market and with at least 10,000 employees overall. Organizations with less than 1000 employees will be classified as small companies. In terms of geographical locations, this study will focus on the continental locations, such that there will be data centers in North America, Western Europe, Eastern Europe, South America, Asia, and Australia. The value of the data center to the company will be informed by the dependence of the company on the data center. Organizations that have only one data center can be said to be fully dependent on it, while those with more than one such centers are less dependent on each of their data centers. Also, organization that share their data centers will be considered as a separate cluster. Each of the categories will be represented by at least two companies such that a total of 20 data centers will be selected for the collection of data.

## **Data collection**

Data collection will be carried out using secondary research methods. Due to the diversity of the research sample, especially with regards to geographic location, primary methods of collecting data cannot be feasible for this study. Therefore, data will be collected through reviewing of the organizations’ literature, which is available on library materials and their official websites. The only source of primary data from the organizations would be the email interviews and questionnaires whereby a set of questions on the organizations’ data management, security, and how their centers add value to the organizations can be formulated and sent to these organizations’ management through emails. The only challenge with this method is that it does not have any guarantee that specific firms will respond to the emails within the research period, which makes it less dependable for purposes of this research.

Reviewing the organizations’ literature that is mostly provided through their official websites provides a dependable source of information about specific details on the data centers. Additionally, information is available through academia libraries with regards to specific events in data security, especially major breaches affecting companies where data was lost and people were put at risk. Such information also details the nature of losses that firms experience when they get their data security breached and unauthorized people access their systems. significant data to be collected here include periods of major data breaches, specific companies that were affected by such breaches, the quantification of the losses in terms of money that the companies had to pay in compensation to the owners of the data that is lost or to the cybercriminals in cases of ransomware attacks, and the time it took to recover the system and stop the intrusion by the unauthorized third parties. The information collected in this study will entail both textual and numerical data for analysis.

## **Data Analysis**

Data analysis will be done using MATLAB. The analysis will include both numerical and nonnumerical data whereby the numerical data will be used to find the types of attacks that were most prevalent among the sampled firms, the time period when most breaches occurred, and the time spent by organizations to regain control and security of their systems. The analysis will also highlight the financial impact of the security compromises for data centers so as to generate a business solution simulated using MATLAB for firms to adopt. The simulation focuses on preventing the losses and intrusion into the data centers and networks by unauthorized parties as one of the objectives of this research.

## **Summary of Chapter Three**

Data collection will be carried out using a combination of primary and secondary research methods, where the primary research will involve email questionnaires sent to selected companies. Structured literature review of the organizations’ official websites as well as scholarly sources on the issue of data security and breaches of data center security will also be used as a source of research data. The data will be collected on companies selected through a systematic sampling method so that a proper representation of the industry is achieved. Data analysis will be done using MATLAB, from which a simulation of a potential solution to the challenges noted during the collection of data will be provided.

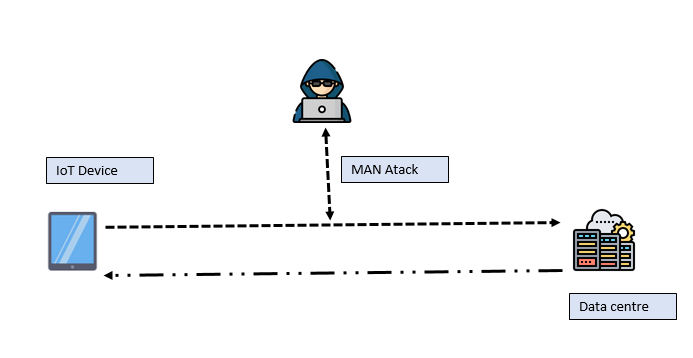
**Dataset description**

The dataset obtained for this particular study contains a total of 179,983 records collected on IoT devices and their possible attack scenarios. Further, the dataset is divided into 49 columns that are supposed to be used for this particular study. The variables each representing the columns are identified as follows: attack level, start time , end time, duration, source address, destination address, source port, protocol, TCP flags, forwarding status, source tos, input packets, input bytes, source mask, client latency, server latency, application latency, router IP address and time the flow was received by the collector. The above mentioned coolumns are the specific colums that the rsearcher intends to use for this partilcuar analysis.

The attack level represents the weight of the attack on the system, For instance, an aattack cold be considered as highly risk on the datacenter or less risky. In this case, 0 is used to respresnta an attack type that is less risky and 1 is used to reprsnt an attack that is material to the data center. Based on these two scenrios, an engineer could then analyse the conseqnunetial impats of these two attacks on the host server. Start time determines the time the attack was recorded on the server. Usuaully server monitors softwares will log out the timestamps upne which the anomaly was first detected and this variable captures the year,month, day, hour, minutes and seconds. This variable is of siginificance escpiclaly when it comes to uaditung, or trend /pattern generation.Usulay one of the key items at a later system audit phase is to identify which of the servers is prone to attack and what can be done to correct this. The achievement of this kind of inquiry shall rely on the time start timestamp functions. Time end also recorded as (te) in this case captures how long the attack took on the server. The difference between the start time of an attack and the end time of an attack gives the attack duration, which is basically an interpretation of the infrastructure strength of the software programs within the server.

The longer the duration of an attack, the stronger the underlying security measures put up and vice versa. Nonetheless, we can still say that the duration of the attack can also rely on the strengths and skills of the attacker or the fact that more loosely opened ports can give the attackers a field day trying to understand the system.

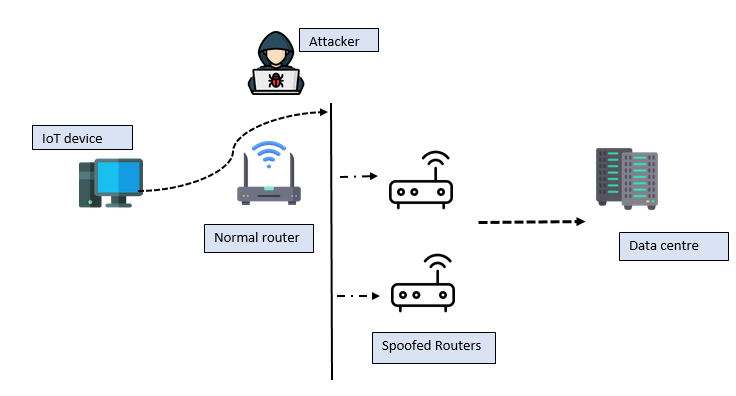
The source address is the origin of the attack. Most attacks could either be generated from an IoT device itself or from a man in the middle attack, as shown below:



Even though the source address can always be hidden and masked, when it comes to data analysis, a trend can always be established. Further, source addresses also help to discover of the attack is coming from within or out of the organization the destination address is the targeted IP address. Since the objective of this study is to discover the possible attacks on data center hosts, primary assumption is made to the fact that all destination IPs are data targeted. Since the column labeling are those related to host server and their respective database applications. Even though more security measures have been put up on data centers, no system is air tight and the tacker still managed to infiltrate some of these data centers as seen from the data collected. The source port comuns in this dataset represents the port of the originating attack. Similar ports can establish a pattern and then these patterns can be used to establish co-linearity of the two systems. This way, it becomes easier to patch these kind of attacks. The protocol shall determine the type of attack being experienced, usually email commnuincations, telnet communications, shell and over the internt connection communications utilize difrent types of communication protocols and going forwards, these types of connections can be analysed to establish a given pattern and trend of over the dataset. The TCP flags shall determine if an attack was given an urgent flag for execution or not, for flags that were given urgebt pointers and the attacks neded up happening without raising alrams on the target servers, there needs to be a review of the underlying systems in scale so as to help solve this kind of scenario. The reasoning here is that no attack on the datacenter originating from an IoT device should be given priority without establishing tits risk flag nature on the target host.

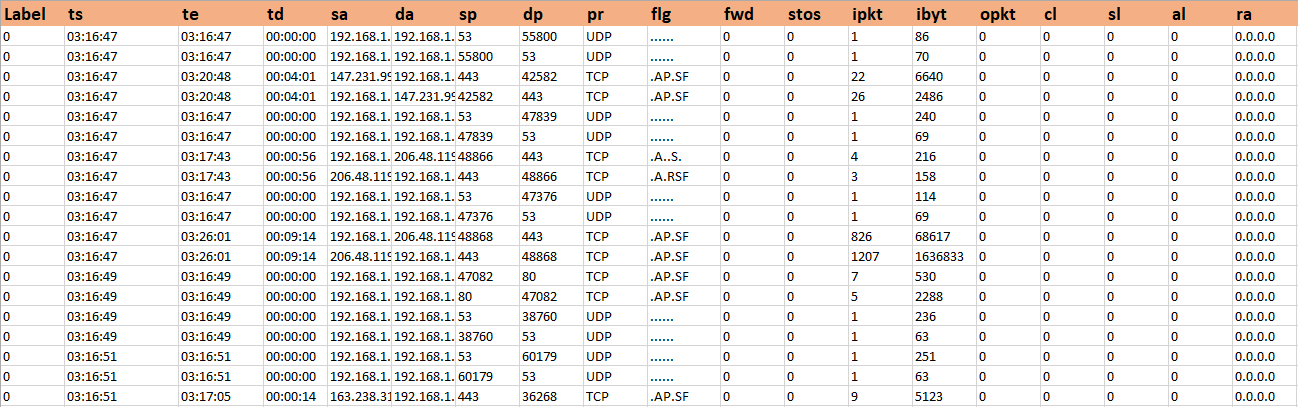
The client latency is how long the data took to be captured and transmitted for decoding on the target server. The values represented in this dataset for this particular exercise is either 0 for normal latency or 1 for abnormal latency. The indicators of which rely on the available network infrastructure and the internet connection between the two peers. The analysis of the client latency and the server latency shall help determine the frequency of the attack and its nature. For instance if a denial of services DDOS was to take place on the host application, then it’s expected that the latency from the client host would be 1 which in this case represents a higher/ more risky condition. On the hand, the response of the host server latency communicates that the server has been compromised if and infected if the feedback is lower than usual and the same could be true server is responding at a higher latency rate.

Consequently, since packets can always b re-routed either through session hijacking, main in the middle attack or through IP hijacking, the router IP addres determines in this case the source router IP of the packts being recived by the host server. Since its known the specific IP addreses ranges of the primary host routers, we can then establish if an anomaly has coocured and from which partciluar router this is coming from. Even if IP spoofing is happening, then an analysis would still reveal the kind and nature of these routing attacks. Legacy security systems can then be used to combat such attacks based on the post-configured and allowed IP table ranges. Illustration is as per the below:



The variables discussed above are used in the next phase of the data analysis process to determine the expected project aims and objectives.

A quick summary and snippet of the dataset looks like below:



**Analysis and presentations:**

  Label             ts                te                td

 Min.   :     0   Min.   :0.0000   Length:359967     Length:359967     Length:359967

 1st Qu.: 89992   1st Qu.:1.0000   Class1:hms        Class1:hms        Class1:hms

 Median :179983   Median :1.0000   Class2:difftime   Class2:difftime   Class2:difftime

 Mean   :179983   Mean   :0.9962   Mode  :numeric    Mode  :numeric    Mode  :numeric

 3rd Qu.:269975   3rd Qu.:1.0000

 Max.   :359966   Max.   :1.0000

The first step is to conduct a simple summary on the dataset to try and establish how the data

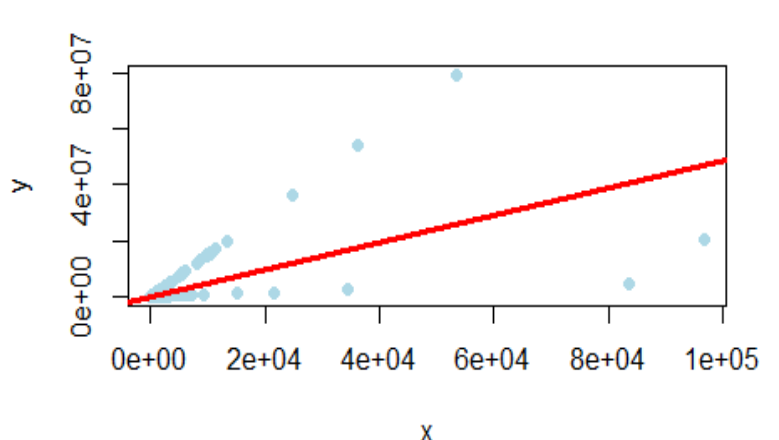
performs based on its measures of central tendencies. In this case, the mean, median and mode of the ts, te, td are established. The measures of central tendencies gave the reasecher an overiew of the look of and feel of the variables in selection and their expected behavior as the study continued.

**Measuring relationships:**

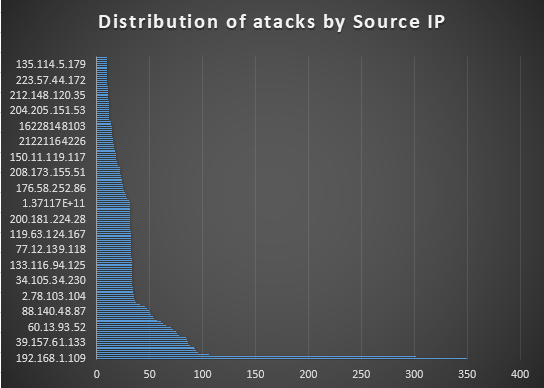
A further analysis of the of the input packets and the inputs bytes were done and the resultant relationship plotted on a linear model as shown below. The linear model revealed that there is a positive relationship between the input packets and the output bytes. The percentage relationship established 60%, basically what this means is that as the input packets increased so does the input bytes and vice versa.

The interpretation of this is that there is a uniform connection between the umber of packets being sent from the IoT device to the data center. Further interpretation of this could also mean that the integrity of the data is maintained, giving the researcher the confidence that no packets or pieces of data were intercepted and blocked, such that during system audits, an expert opinion could easily be formed without any blame on any false positives.

This analysis further revealed how man in the middle attack could be detected and curbed within a specific network, since this kind of attack also relies on measuring the integrity of the data being received at the destination address. In this instance, the input packets and the input bytes must match, and where such does not happen, then the data is unreachable for security analysis.

****

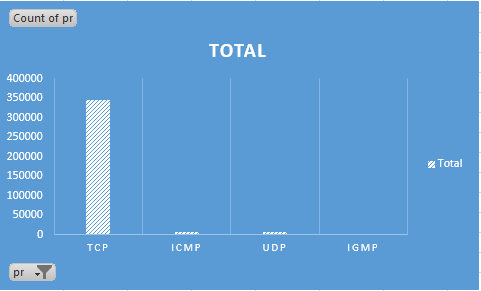
**Attack Distributions:**

****

The analysis of the source IPs revealed that the largest source of this attacks came from local connections, this is the IP address indicated by 192.168.1.109. The interpretation of this analysis is that there is a possibility that most of the data center attacks originated from inside the organization. This could have been through the penetration by an external attacker or or some employee staff with prividlge access to the servies and systems. The reason why such an attack could have happened may range from weak internal socurity control systems to the availability of rogue staff. The source address could not have been specifically been the exact location of the attacker, but could also mean the location of the source object device. A simple item such as USB drive can easily find its way into the organisatin and be used to pass a virus or malware to the corporate network.

During system audit activities and response feedbacks, considerate attention should be given to the largest source address that were transmitting these kinds of attacks.

**Analysis of attack protocols:**

****

Further analysis of the different connection protocols revealed that TCP was the largest method of connection used when launching these kinds of attacks. This was followed by ICMP and UDP protocols.

The observation realized from this analysis reveals that most of the attacks that landed on the data centers were as a result of the transmission that occurred over the internet. Instances possible to this include session hijacking where system users were sending communications to target severs and data packets were intercepted and manipulated with privileged access like those of a genuine user who was trying to access the same resources on the server.

Other attacks included Phishing and IP hijacking on the IoT devices that transmitted the information. The UDP protocol was used to send instant messages from the source addresses; the implication of this is that phishing attacks and malicious links could have been shared on chats, customer support portals and social media platforms hosted on the targeted IoT devices and targeted at the database servers.

# **Reference List**

1. Maddox, T. (2016). Here are the biggest IoT security threats facing the enterprise in 2017. *Consulted at https://www. techrepublic. com/article/here-are-the-biggest-iot-security-threats-facing-the-enterprise-in-2017*.
2. Gupta, S., & Lingareddy, N. (2021). Security Threats and Their Mitigations in IoT Devices. In *Techno-Societal 2020* (pp. 411-424). Springer, Cham.
3. Zhang, J., Chen, H., Gong, L., Cao, J., & Gu, Z. (2019, June). The current research of IoT security. In *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)* (pp. 346-353). IEEE.
4. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721-82743.
5. Sehgal, N. K., Shankar, S., & Acken, J. M. (2019, July). Trust Modelling for Security of IoT Devices. In *CS & IT Conference Proceedings* (Vol. 9, No. 9). CS & IT Conference Proceedings.
6. Mamun, S. A., Ganguly, A., Markopoulos, P. P., Kwasinski, A., & Kwon, M. (2020, June). Security vulnerabilities of server-centric wireless datacenters. In *2020 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.
7. Chen, Z., Dong, W., Li, H., Zhang, P., Chen, X., & Cao, J. (2014). Collaborative network security in multi-tenant data center for cloud computing. *Tsinghua Science and Technology*, *19*(1), 82-94.
8. Abdelrahman, A. M., Rodrigues, J. J., Mahmoud, M. M., Saleem, K., Das, A. K., Korotaev, V., & Kozlov, S. A. (2021). Software‐defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions. *International Journal of Communication Systems*, *34*(4), e4706.