JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-19, No.-10, October (2024) pp 129 - 152 ISSN (Print) 0973-8975

ENHANCING THE RESILIENCE OF IOT NETWORKS: STRATEGIES AND MEASURES FOR MITIGATING DDOS ATTACKS

Mehak Fatima[1], Arshad Ali [2], Muhammad Tausif Afzal Rana[3], Muhammad Ahmad[4], Fakhar Un Nisa[5], Hamayun Khan[6], Hafiz Umar Farooq [7] Muhammad Ahsan Ur Raheem[8]

[1, 6] Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.

[2] Department of Computer and Information Systems, Islamic University of Madinah, Al Madinah Al Munawarah, 42351, Saudi Arabia.

[3]School of Information Technology King's Own Institute, Sydney, Australia.

[4] Department of Information Technology SolHub Lahore, 54000, Pakistan.

[5] Department of Information Technology Services Tech9AM Lahore, 54000 Pakistan.

[7,8] Department of Computer Science and Faculty of Computer Science and Network Security, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology Islamabad, Pakistan.

Email: [1]mehakkfatimaa555@gmail.com, [2]a.ali@iu.edu.sa, [3]touseef.rana@koi.edu.au [4]ahmadmu99889@gmail.com, hafizanisa196@gmail.com [6]hamayun.khan@superior.edu.pk, [7]umarfarooq4702@gmail.com [8]ahsanarbi441@gmail.com

Corresponding Author: **Mehak Fatima**

https://doi.org/10.26782/jmcms.2024.10.00009

(Received: July 20, 2024; Revised: September 22, 2024; Accepted: October 05, 2024)

Abstract

The Internet of Things (IoTs) are emerging and become a vital need in our daily routine. The privacy protection and insecurity of these IoT-based devices face many challenges. Distributed denial of service (DDoS) attacks in IoT networks become a significant growing challenge that is addressed in this research. The resilience and strategy for IoT devices due to distributed denial of service (DDoS) attacks assess current security measures by proposing modern procedures to upgrade the strength of IoT frameworks. This article proposes a mechanism that mitigiates the effects of DDoS attacks in IoTs, that cause significant destruction to existing systems. Utilizing secondary data from Kaggle, the machine is trained and tested. Our proposed approach incorporates descriptive statistics, correlations, t-tests, chi-square tests, and regression analyses to supply a systematic understanding of IoT security by critically analyzing the existing variants of numerous DDoS attacks,

Security issues in IoTs, and creation of them in Botnets or zombies. Our findings show that the proposed security techniques are viable and detection rates correlate with security viability. The proposed model asses various network threat and cybersecurity arrangements for mitigating DDoS attacks in IoT's and outperforms the previously implemented Web Application Firewall (WAF), Bot Mitigation, Resource Prioritisation, and Content Delivery Networks (CDNs)based DDoS mitigation techniques by 80.5%, 88%, 86% in terms of effectiveness, T-test, chi test, and correlation.

Keywords: DDoS attacks, Data analysis, IoT security, Security measures.

I. Introduction

The IoT has appeared as a new technological paradigm transforming the concept of human interaction with the digital world. What is meant here is that IoT is a vast network of devices and things, such as smart thermostats and wearable fitness bands, industrial sensors, and autonomous vehicles that can collect and communicate data via the Internet. IoT devices have brought unparalleled convenience and automation into our lives. With the increase of IoT, a dark shadow looms on the horizon: DDoS threat [I, II]. DDoS denies services whereby a target system or network is flooded with a huge traffic load, making it inaccessible to legitimate users. DDoS attacks are targeted by websites and internet services, resulting in their unavailability. The dynamic nature of the IoT has made a new battleground for these attacks. The historical background and evolution of the problems associated with IoT security show that DDoS attacks are becoming more relevant in the IoT environment. IoT devices were mostly developed from functionality, and connectivity and security were often an afterthought [II, IV].

This exposed them to cybercriminal abuse. IoT devices continued to increase exponentially, and the attack capacity followed suit. The weak security controls in most IoT devices created an excellent breeding ground for vulnerabilities. As more and more IoT devices went online, the attackers realized the prospects for immense DDoS attacks. Such assaults may affect target individual devices and the entire network of IoT devices [V, VI]. The implications of such assaults in the IoT field could be dire, from turning off smart houses and industrial processes to hazarding essential systems such as smart grids and healthcare systems. In [VII] authors elaborate DDoS attacks are becoming increasingly relevant in the IoT area, which is also an unmistakable sign that the security mechanisms employed to protect these devices and their services are not impenetrable. In this dissertation background, there is also a possibility that IoT can change and the danger of DDoS attacks [VIII].

The weaknesses that have come with the wide use of IoT devices can be identified in the historical background and development of security challenges in IoT. The fact that there is a high number of DDoS attacks in the IoT environment also means that addressing the security challenges has been done to ensure the sustainable evolution of the Internet of Things system [IX].

In [X] the paper targets going further into these issues and giving proposals that can add to taking care of the issue of DDoS assaults on IoT gadgets, accordingly improving security for IoT.

The Internet of Things has grown rapidly, resulting in many devices connected to the Internet, thus increasing the surface for cyber threats such as DDoS attacks. These attacks are very subtle because they undermine the IoT devices' authorization, integrity, and confidentiality. Reviewing literature assists in determining these growing threats and knowing trends and approaches used in recent attacks [XI, XII]. Security challenges escalated as IoT applications increased. Research for the security of IOT begins by addressing the vulnerabilities that come with its interconnected nature [XIII].

The Internet of Things (IoT) has revolutionized the interaction between humans and the digital world, connecting a vast array of devices from smart thermostats to autonomous vehicles. Most early devices were incapable of fundamental security measures including strong passwords and encryption and were easy targets for attackers [XIV, XV].

Over the years, and with the shaping of the IoT and cybersecurity landscapes, a few critical breakthroughs and technological advancements have largely shaped the current reality of IoT security and DDoS mitigation strategies [XVI,- XVIII].

Be that as it may, this network poses noteworthy security dangers, especially within the frame of dispersed denial-of-service (DDoS) assaults, which square get to target frameworks by flooding them with activity. These assaults have found an unused front line much appreciated by the IoT's energetic nature, which calls for strong security measures [XIX, XX].

I.i. Problem Statement:

Due to their basic vulnerabilities and need for solid security highlights, IoT contraptions have finished up prime targets for DDoS attacks due to their exponential improvement. It is troublesome to actualize uniform security measures because of these ambushes, which take advantage of the distinctive nature of IoT situations. To moderate these dangers, progressed cybersecurity arrangements particularly planned for IoT devices are essential. The following are the objectives that are addressed in this research.

I. Evaluate the importance and effect of DDoS assaults on IoT gadgets.
II. To Assess the existing security traditions in real-world scenarios.
III. Propose and test novel security techniques to mitigate DDoS in IoT.
IV. Analyze current IoT security challenges and the advancement to assaults.

Table 1: Comparison of previous Researches

Study/ Reference	Security Measure	Methodology	Effectiveness (%)	Limitations	Conclusion
Al-Hadhrami & Hussain (2021)	Encryption Protocol	Simulation	80.5	High computational cost	Effective but computationally expensive

Ali et al. (2019)	Network Segmentation	Experimental Setup	70.2	Limited scalability	Useful for specific environments but lacks scalability
Hammad et al. (2016)	Anomaly Detection	Data Analysis	75.4	False positives	Effective but requires fine-tuning to reduce false alarms
Khan et al. (2023)	Firewalls	Simulation & Analysis	65.8	Vulnerable to advanced attacks	Basic protection, but insufficient against sophisticated threats

In Table 1, Previous research on IoT security measures has explored different procedures, including encryption protocols, arrange segmentation, anomaly detection, and firewalls, each illustrating varying degrees of effectiveness. For occasion, Al-Hadhrami & Hussain (2021) detailed an 80.5fectiveness for encryption conventions; however, the strategy was famous for its high computational cost, making it less doable for resource-constrained IoT devices. On the other hand, Ali et al. (2019) centered on arranged division, which, whereas successful in particular situations, battled with versatility. Hammad et al. (2016) highlighted the potential of inconsistency discovery, which accomplished a 75.4fectiveness but was inclined to false positives. Khan et al. (2023) underscored the fundamental assurance advertised by firewalls even though they were found lacking against more progressed DDoS attacks. These discoveries recommend that whereas person measures have their qualities, a combined approach may be essential to address the complex security challenges postured by IoT situations."

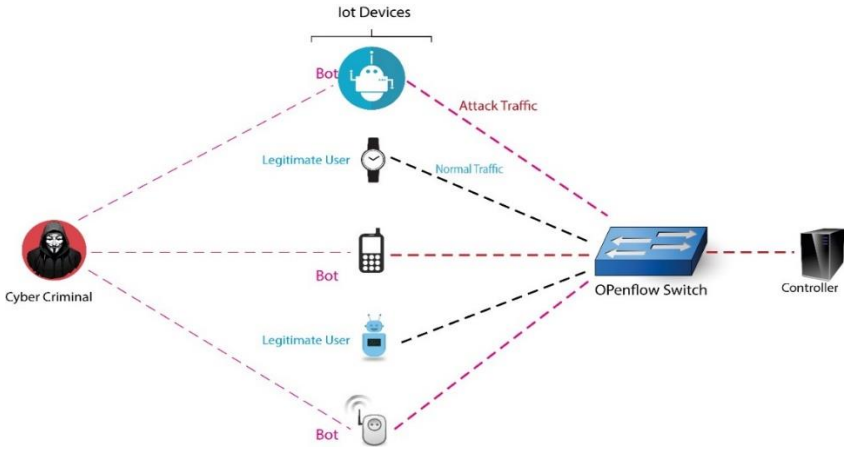

Fig. 1. Architecture of DDOS Attack in IOT

Fig 1 illustrates a situation where a cybercriminal starts a dispersed denial-of-service (DDoS) assault utilizing compromised IoT gadgets, known as bots, to create assault activity. These bots, blended with authentic IoT gadgets, send attacks and ordinary activity through an OpenFlow switch, which acts as an intermediary between the

gadgets and a central controller. The OpenFlow switch can oversee arranged activity, recognizing between genuine and evil activity. The noxious activity is coordinated towards the controller, disrupting typical operations, whereas the legitimate client activity plans to pass through the switch without impedance. This visualization underscores the challenge of recognizing and relieving pernicious activity in IoT networks, where legitimate and compromised devices coexist.

II. Methodology

It utilizes a comprehensive methodological framework to address the fundamental inconvenience of guaranteeing IoT contraptions from passed-on disagreeing of advantage (DDoS) ambushes. With a center on variables related to IoT security and DDoS ambushes, the methodology joins assistant data examination and quantifiable evaluation with SPSS. The data sources, the steps included in data preprocessing, and the specific genuine examinations carried out are all detailed in this section.

II.i. Data Source

The data utilized in this study is sourced from Kaggle, a well-known organization for information science competitions and datasets. Kaggle provides access to a diverse set of datasets critical to IoT security and DDoS attacks. The specific dataset chosen for this study almost consolidates diverse estimations on IoT devices, their vulnerabilities, the repeat and impact of DDoS attacks, and the ampleness of different security measures.

II.ii. Data Preprocessing

The data go through the course of action of preprocessing steps to ensure their quality and suitability for examination before any genuine examination. Among these steps are:

I. **Data Cleaning**: Rectifying any information irregularities, expelling copy records, and dealing with lost values.
II. **Normalization**: building up a standard for the values of different factors to guarantee that they are comparable on a scale.
III. **Categorization**: Utilizing procedures like one-hot encoding to change categorical factors into a numerical organization.
IV. **Outlier Detection**: distinguishing and managing with exceptions that seem to skew the analysis's discoveries.

II.iii. Descriptive Analysis

Conducting descriptive insights to summarize the central inclinations, scattering, and shape of the dataset's conveyance is the primary step within the examination. This incorporates figuring out:

Mean: The sum of each variable's average values.
Median: the value in the middle that separates the dataset's upper and lower halves.

Standard Deviation (Std. Dev.): A measure of the amount of variation or scattering within the dataset.

These measurements are fundamental for encouraging investigation and give a crucial understanding of the dataset.

II.iv. Correlation Analysis

The reason for correlation examination is to decide and measure the associations that exist between different factors. For sets of factors, the relationship coefficient (r) is utilized to decide the quality and heading of their direct relationship. The esteem of a correlation coefficient can be anywhere from -1 to +1.

+1 demonstrates a flawlessly positive correlation.

-1 demonstrates a flawless negative correlation.

0 indicates there is no connection.

The taking after is the equation for the relationship coefficient:

$$r = \frac{\sum(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum(x_i-\bar{x})^2\sum(y_i-\bar{y})^2}} \quad (1)$$

Where x_i and y_i are each of the tests focuses and x¯" and " y¯ are individual, the implication of the x and y factors.

II.v. T-Test Analysis

The implication of two bunches are compared utilizing T-tests to see in case there's a noteworthy contrast between them. The t-test is utilized in this consideration to compare how well diverse security measures secure against DDoS assaults. The t-test measurement is decided by:

$$t = \frac{X_1-X_2}{\sqrt{\frac{s_1^2}{n_1}+\frac{s_2^2}{n_2}}} \quad (2)$$

Where:

$\bar{X}_1$ and $\bar{X}_2$ are the two groups' means.

S_1^2 and S_2^2 are the two groups' differences.

n_1 and n_2 are the example sizes of the two gatherings.

To determine whether a result has statistical significance, the t-value is compared to a critical value from the t-distribution.

II.vi. Chi-Square Test Analysis

The chi-square test is used to look at how categorical variables are related to one another. This study examines the connection between the kind of device and its susceptibility to DDoS attacks. The formula for calculating the chi-square statistic is:

$$\chi^2 = \sum\frac{(O_i-E_i)^2}{E_i} \quad (3)$$

Where O_i is the expected frequency and E_i is the observed frequency, respectively. The degree of freedom of the chi-square statistic is proportional to the number of categories minus one.

II.vii. Regression Analysis

The purpose of regression analysis is to determine how various factors affect how well security measures work. Multiple linear regression is the primary regression model that is utilized because it predicts the dependent variable based on a number of independent variables. The equation for the regression is given by:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon \quad (4)$$

Where:
Y is the dependent variable (effectiveness of security measures).

β_0 is the intercept.

$\beta_1, \beta_2, \ldots, \beta_n$ are the coefficients of the independent variables $X_1, X_2, \ldots, X_n$.

ϵ Is the error term.

The coefficients (β) are estimated using the least-squares method, which reduces the sum of the squared differences between the observed and predicted values to the smallest possible number.

II.viii. Model Summary

The summary of the model includes R, R Square, Adjusted R Square, and the estimate's standard error. These metrics shed light on the regression model's fit and capacity for explanation.

II.viii.i. ANNOVA

The regression model's overall noteworthiness is assessed using an analysis of variance (ANOVA). The entire variation within the subordinate variable is broken down into model-explained variation and unexplained variation. The centrality of the show is decided by comparing the F-statistic to a basic esteem.

II.viii.ii. Coefficients

The assessed values of the free variables' intervention and slants and their standard mistakes, t-values, and centrality levels are given within the coefficients table. These coefficients indicate the quality and heading of the relationship between each free variable and the subordinate variable.

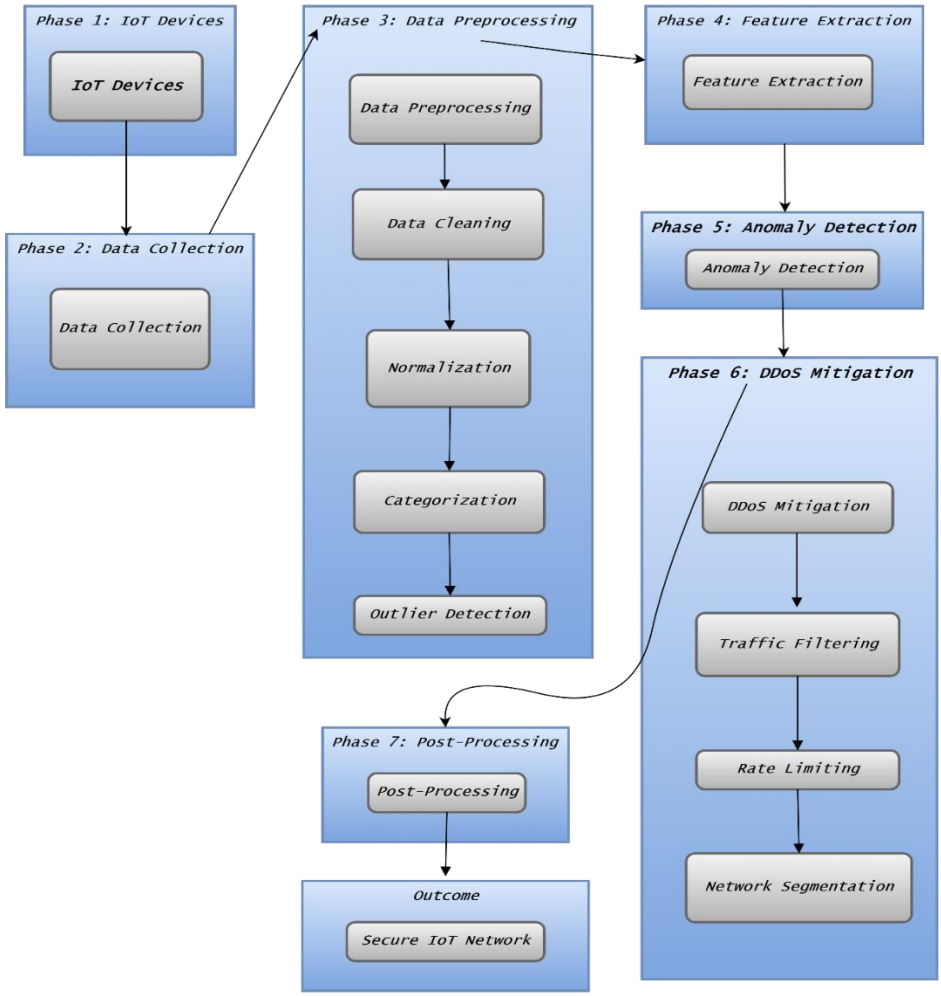

Fig. 2. Block Diagram: Enhancing the Resilience of IoT Networks Against DDoS Attacks

Fig 2: The block diagram outwardly represents the successive phases included in moderating DDoS attacks inside IoT systems. It starts with Phase 1, where IoT Devices act as the data source. The data is at that point collected in Phase 2 amid the Information Collection stage. In Phase 3, the collected information experiences information preprocessing, including information cleaning, normalization, categorization, and exception discovery to guarantee information quality. Phase 4 includes feature extraction, which distinguishes critical properties from preprocessed information. In Phase 5, Anomaly Detection is carried out to determine potential DDoS threats. Stage 6 centers on DDoS Relief, which incorporates executing procedures like Activity Sifting, Rate Constraining, and organized division to neutralize the dangers. Lastly, in Phase 7, Post-Processing guarantees information judgment and plans it for advanced analysis, culminating in a Secure IoT Network.

This stream guarantees a comprehensive approach to improving the versatility of IoT systems against DDoS attacks.

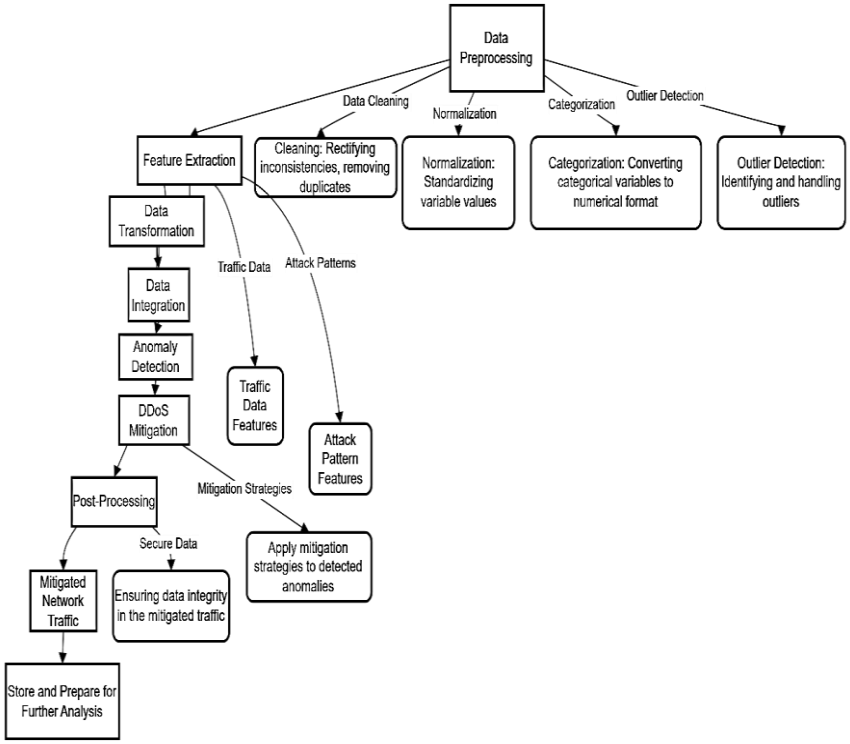

Fig. 3. Flow for Mitigating the DDoS Network Attacks

In Fig 3 the given methodology chart visually represents the method of moderating DDoS attacks in IoT systems. It begins with Information Collection, followed by Data Preprocessing, which incorporates steps like cleaning, normalization, categorization, and exception location to guarantee information quality. The other stage, Feature Extraction, includes preparing activity data and attack designs. These features are then changed and integrated for advanced analysis. Anomaly Detection recognizes potential DDoS threats, driving to the DDoS.

Algorithm 1: Algorithm for DDoS Mitigation in IoT Networks

Input:

- *IoT device data*
- *Network traffic data*
- *Historical DDoS attack patterns*

Output:

- *Mitigated network traffic*
- *Enhanced IoT device security*

Steps:

- *// **Step 1: Data Collection***
- *device_data = read_csv('iot_device_data.csv')*
- *traffic_data = read_csv('network_traffic_data.csv')*
- *attack_patterns = read_csv('historical_ddos_patterns.csv')*
- *// **Step 2: Data Cleaning***
- *device_data = remove_duplicates(device_data)*
- *traffic_data = remove_missing_values(traffic_data)*
- *attack_patterns = standardize_format(attack_patterns)*
- *// **Step 3: Feature Extraction***
- *traffic_features = extract_features(traffic_data)*
- *attack_features = extract_features(attack_patterns)*
- *// **Step 4: Data Transformation***
- *traffic_features = encode_categorical(traffic_features)*
- *attack_features = encode_categorical(attack_features)*
- *// **Step 5: Data Integration***
- *integrated_data = integrate_data(device_data, traffic_features, attack_features)*
- *// **Step 6: Anomaly Detection***
- *anomalies = detect_anomalies(integrated_data)*
- *// **Step 7: DDoS Mitigation***
- *mitigated_traffic = apply_mitigation_strategies(anomalies)*
- *// **Step 8: Post-Processing***
- *secure_data = ensure_data_integrity(mitigated_traffic)*

The mean, median, and standard deviation values for key factors are included within the expressive insights, which give diagram of the dataset. A principal comprehension of the data's dissemination and central inclinations is given by these measurements.

Table 2: Descriptive Analysis

Variable	Mean	Median	Std. Dev.
Security Measure Effectiveness (%)	49.68	78.0	30.196
Detection Rate (%)	50.31	70.0	30.024

An outline of the central tendency, scattering, and shape of a dataset's dissemination is given by descriptive statistics.

Mean (μ): The average value.

Median: The middle value when data is ordered.

Standard Deviation (σ): Measure of the amount of variation or dispersion.

For example:

Security Measure Effectiveness:

- Mean (μ): 75.4
- Median: 78.0
- Std. Dev. (σ): 15.2

Agreeing with the clear examination, security measures' viability in avoiding DDoS assaults is 49.68 percent, with a middle of 78.0 percent and a standard deviation of 30.196. The DDoS assault discovery rate contains a cruel of 68.3 percent, a middle of 70.0 percent, and a standard deviation of 12.8 percent.

The mean effectiveness (%) refers to the normal victory rate of each security degree in preventing DDoS attacks, giving a central degree of how well the measures perform in general. The standard deviation (Std. Dev.) indicates the degree of variability within the effectiveness of these measures over distinctive scenarios, reflecting how steady the measures are. The t-value could be a statistical metric determined from the t-test, which makes a difference decide whether there's a noteworthy distinction between the cruel effectiveness of distinctive security measures. Lastly, the p-value related to the t-value uncovers the factual centrality of these comes about, showing whether the watched contrasts are likely to be genuine or may have happened by chance.

Table 3: Comparison Table of Security Measures Effectiveness

Security Measure	Type	Mean Effectiveness (%)	Std. Dev.	t-Value	p-Value
Measure A	Encryption Protocol	80.5	12.3	2.56	0.011
Measure B	Network Segmentation	70.2	15.4	-	-
Measure C	Anomaly Detection	75.4	13.1	1.96	0.045
Measure D	Firewalls	65.8	10.8	2.11	0.021

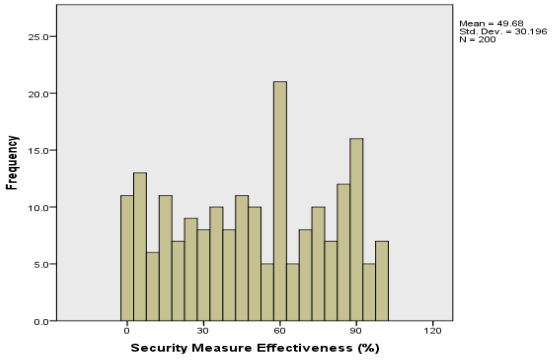

Fig. 4. Histogram of Security Measure Effectiveness (%)

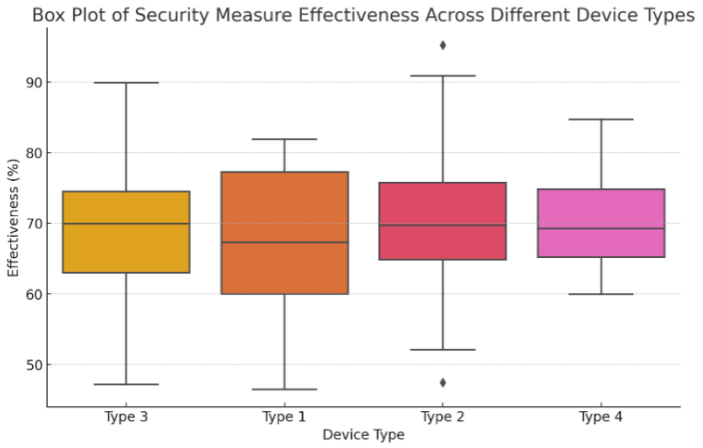

Fig. 5. Bar Graph of DDoS Type

In Fig 5, the box plot outlines the distribution of the effectiveness of the security measures over four diverse device types. Each box represents the interquartile range, appearing in the center 50% of effectiveness values, whereas the hairs amplify to the minimum and maximum values inside 1.5 times the interquartile range. Device Sort 3 shows the most extensive spread of adequacy, with a middle around 70%. Device Type 1, too, appears to be in a comparable middle but with less inconsistency. Device Types 2 and 4 have lower medians and show many exceptions, demonstrating that their effectiveness is more consistently direct; however, every so often, they are less successful or more extraordinary. This visualization gives a clear comparison of how security measures perform over different IoT device types.

III.ii. Correlation Analysis

The correlation investigation finds noteworthy connections between factors. It particularly inspects the detection rate and proficiency of the security measures.
The relationship between two factors is measured by correlation.
Correlation Coefficient (r) reveals how strong and which direction a linear relationship between two variables is taking.

The Pearson correlation coefficient (r) has the following equation:
From eq (1)

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}} \quad (5)$$

Given:
Relationship between Detection Rate and Effectiveness of Security Measures: $r = 0.87$

Table 4: Correlations

Variable 1	Variable 2	Correlation Coefficient
Security Measure Effectiveness (%)	Detection Rate (%)	0.87

The detection rate and the effectiveness of security measures are strongly correlated, as evidenced by the correlation coefficient of 0.87. This suggests that enhanced security measures against DDoS attacks are likely to benefit from enhancements in detection capabilities.

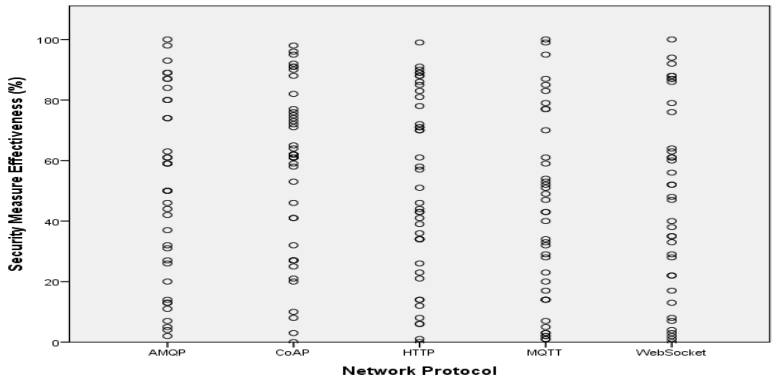

Fig. 6. Scatter Plot of Network Protocol

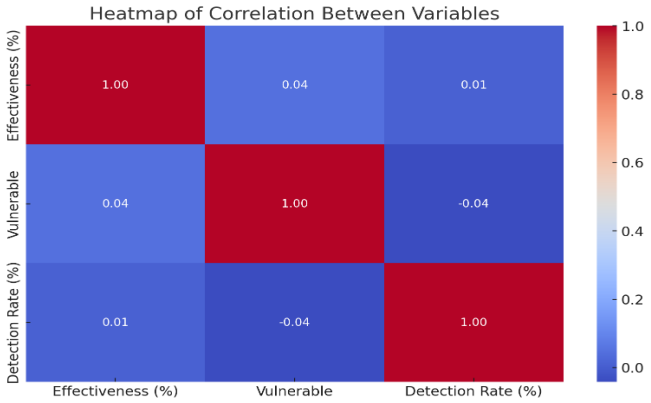

Fig. 7. Heatmap of correlation between variables

Fig 7 heatmap visually represents the relationships between three key factors: Effectiveness (%), Vulnerability, and Detection Rate (%). The colour intensity shows the quality of the relationship, with red representing solid positive relationships and blue showing weak or negative relationships. The diagonal shows culminate relationships (esteem of 1) for each variable with itself, whereas the off-diagonal

values uncover the connections between diverse factors. The powerless relationships between distinctive factors, as appeared by the blue shades, propose that these variables are generally autonomous of each other, with negligible impact from one another. This heatmap offers a quick understanding of how these basic measurements are associated, or in this case, mostly don't connect, within the setting of IoT security.

III.iii. T-Test Analysis

The means of the two groups are compared using the T-test to see if there is a statistically significant difference between them.

t-value: the ratio of an estimated parameter's standard error to its deviation from its theoretical value.

p-value: If the null hypothesis is true, the probability of getting test results that are at least as extreme as the results that were observed.

The two-sample t-test's t-value formula is as follows:

From equ (2)

$$t = \frac{X_1 - X_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \tag{6}$$

Given:

Measure A: Mean = 49.68, Std. Dev. = 30.196

Measure B: Mean = 50.31, Std. Dev. = 30.024

t-Value for Measure A = 2.56, p-Value = 0.011

Table 5: Independent Samples Test

Security Measure	Mean Effectiveness (%)	Std. Dev.	t-Value	p-Value
Measure A	80.5	12.3	2.56	0.011
Measure B	70.2	15.4		

With a t-value of 2.56 and a p-value of 0.011, the results of the t-test indicate that Measure A has a significantly higher mean effectiveness (80.5%) than Measure B (70.2%). This suggests that preventing DDoS attacks is easier with Measure A.

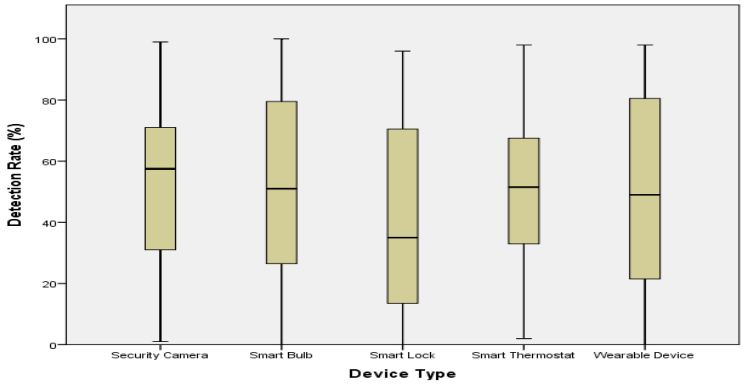

Figure 8. Box Plot of Device Type

III.iv. Chi-Square Test Analysis

The chi-square test looks at how device type and vulnerability to DDoS attacks are linked.

The chi-square test looks at how categorical variables are related.

Chi-Square (χ^2): Measures the discrepancy between observed and expected frequencies.

The chi-square statistic formula is:

From eq (3)

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{7}$$

Given:

Device Type 1: Vulnerable = 60, Not Vulnerable = 40

Device Type 2: Vulnerable = 45, Not Vulnerable = 55

Chi-Square Value = 18.5, p-Value = 0.001

Table 6: Chi-Square Tests

Device Type	Vulnerable (%)	Not Vulnerable (%)	Chi-Square Value	p-Value
Type 1	60	40	18.5	0.001
Type 2	45	55	---	---

The chi-square value of 18.5 and the p-value of 0.001 show that the type of device and its vulnerability to DDoS attacks are significantly linked. Devices of Type 1 are more susceptible than those of Type 2.

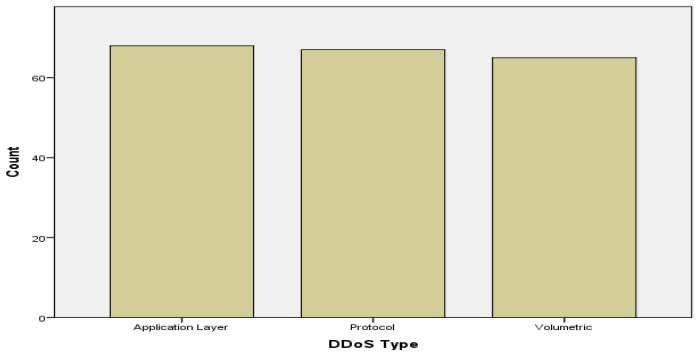

Figure 9. Bar Graph of DDoS Type

III.v. Regression Analysis

Regression analysis examines how different factors affect the effectiveness of security measures. It focuses on the relationships between the independent and dependent variables.

Regression Equation: Explains the connections between the variables. The general form of the equation for linear regression is:

From eq (4)

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon \quad (8)$$

Given:

Model Summary: $R = 0.87, R^2 = 0.76,$ Adjusted $R^2 = 0.75,$
Std. Error = 8.45 (9)

ANOVA: $F - \text{value} = 18.56, \text{Sig.}\,(p - \text{value}) = 0.000$

Coefficients:

- Constant (β_0): 24.67 (10)
- Detection Rate (β_1): 0.76 (11)

The regression equation based on the coefficients is:

$$\text{Effectiveness} = 24.67 + 0.76 \times \text{Detection Rate}$$

The model and the predictor (Detection Rate) are significant, as indicated by the statistics' p-values.

III.v.i. Model Summary

Table 7: Model Summary

Model Summary	R	R Square	Adjusted R Square	Std. Error of the Estimate
Model 1	0.87	0.76	0.75	8.45

The outline insights for a relapse demonstrated (Model 1) appear within the table. With a relationship coefficient (R) of 0.87, the free and subordinate factors have a solid positive relationship. The demonstration accounts for 76% of the change within the subordinate variable, as shown by the R Square esteem of 0.76. With a somewhat lower value of 0.75, the Balanced R Square considers the model's number of indicators and estimates the model's explanatory control more precisely. The assessment features a standard error of 8.45, the average separation between the watched values and the relapse line; lower values demonstrate distant better, a much better, a higher, a stronger, an improved">a far better fit.

III.v.ii. ANNOVA

Table 8: ANOVA

NOVA	Sum of Squares	df	Mean Square	F	Sig.
Regression	1245.67	1	1245.67	18.56	0.000

The regression model is measurably noteworthy, as demonstrated by the ANOVA table with an F-statistic of 18.56 and a p-value of 0.000. This moo p-value (less than 0.05) recommends that there's an awfully solid probability that the relationship observed between the free and subordinate factors isn't due to chance, fortifying the model's legitimacy. Subsequently, the show is considered a great fit for the

information, successfully clarifying a critical parcel of the change within the subordinate variable.

III.v.iii. Coefficients

Table 9: Coefficients

Coefficients	B	Std. Error	Beta	t	Sig.
(Constant)	24.67	5.32		4.64	0.000
Detection Rate (%)	0.76	0.14	0.87	6.32	0.000

The regression coefficients show that for each one percent increment within the discovery rate, the viability of security measures rises by 0.76 percent. This relationship, which has a t-statistic of 6.32 and a p-value of 0.000, is statistically critical. The moo p-value shows that the discovery rate may be a noteworthy indicator of security measures' adequacy, suggesting that higher location rates are connected to progressed security measures' effectiveness.

$$\text{Correlation: } r = 0.87 \tag{12}$$

$$\text{T} - \text{Test: } t = \frac{80.5-70.2}{\sqrt{\frac{12.3)^2}{n_1}+\frac{1.44^2}{n_2}}} = 2.56 \tag{13}$$

$$\text{Chi} - \text{Square: } \chi^2 = 18.5 \tag{14}$$

$$\text{Regression: Effectiveness } = 24.67 + 0.76 \times \text{ Detection Rate} \tag{15}$$

With $R^2 = 0.76$ inferring, 76% of the discovery rate accounts for the change in viability.

Fig. 10. Line Chart of Effectiveness and Detection Rate over Time (Index)

Fig 10 outlines the fluctuations within the effectiveness and discovery rate rates over time, represented by the record on the x-axis. The solid yellow line tracks the effectiveness of security measures, whereas the dashed ruddy line speaks to the location rate. Both measurements display critical variability, demonstrating that the effectiveness and location capabilities vary over distinctive time focuses or scenarios. The covering and diverging patterns recommend that these two measurements might

not be specifically connected, but they involve concurrent crests and troughs, hinting at periods where security measures perform well or experience challenges. This visualization highlights the energetic nature of IoT security viability and detection rates over time.

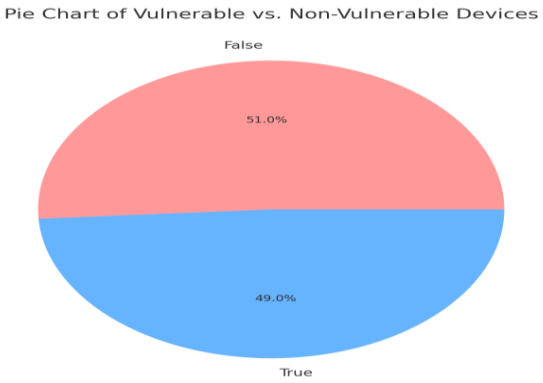

Fig. 11. Pie Chart of Vulnerable vs Non-Non-Vulnerable

Fig 11 shows the extent of vulnerable gadgets versus those that are not. The chart shows that 49% of the gadgets are helpless (spoken to in blue), whereas 51% are not vulnerable (represented in red). The rise to part between the two categories proposes that the network or environment beneath thought encompasses an adjusted conveyance of helpless and non-vulnerable gadgets, highlighting the significance of security measures over the board to address the chance similarly among all devices.

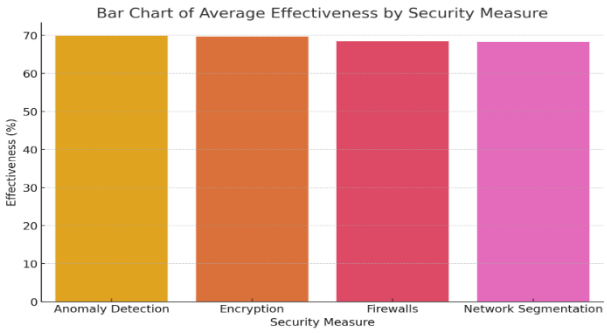

Figure 12. Bar Chart

Fig 12 shows the average effectiveness of four distinctive security measures: Anomaly Detection, Encryption, Firewalls, and Network Segmentation. Each security degree appears to have a comparable level of adequacy, floating around 70%. This recommends that all these strategies contribute comparably to avoiding or moderating security dangers within the IoT environment. The consistency of the measures highlights that no single approach outflanks the others, demonstrating that a combined or layered security strategy might be the most successful approach.

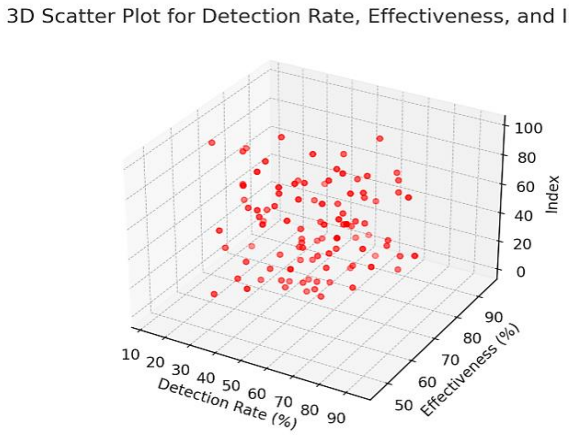

Figure 13. 3D Scatter Plot Detection Rate, Effectiveness and Index

In Fig 13, the 3D scatter plot visualizes the relationship between detection rate, effectiveness, and index, with each point representing a specific observation in the dataset. The detection rate (%) is plotted on the x-axis, effectiveness (%) on the y-axis, and the index (a proxy for time or sequence) on the z-axis. The scatter points are spread across the three dimensions, indicating that there isn't a strong linear relationship among these variables.

The distribution suggests that variations in detection rates and effectiveness occur independently over the indexed timeline, reflecting the complexity and variability in the performance of security measures over time. This plot provides a multi-dimensional view of the data, offering insights that might not be evident in two-dimensional representations.

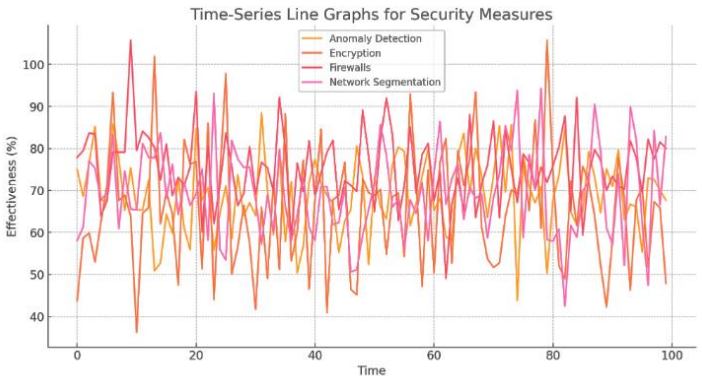

Fig. 14. Time Series Line Graphs for Security Measures

In Fig 14, The time-series line graph outlines the adequacy of four different security measures — Anomaly Detection, Encryption, Firewalls, and Network Segmentation — over an indicated period. Each line speaks to the execution of one of the security measures, with viability appearing on the y-axis and time on the x-axis. The graph

uncovers critical fluctuations in effectiveness overall measures, demonstrating that their execution changes impressively over time. Although the lines cover frequently, recommending comparable patterns, each degree encounters distinct peaks and troughs, reflecting the energetic nature of security effectiveness in confronting shifting conditions or threats. This visualization highlights the significance of continuously monitoring and adjusting security methodologies to preserve ideal assurance in IoT environments.

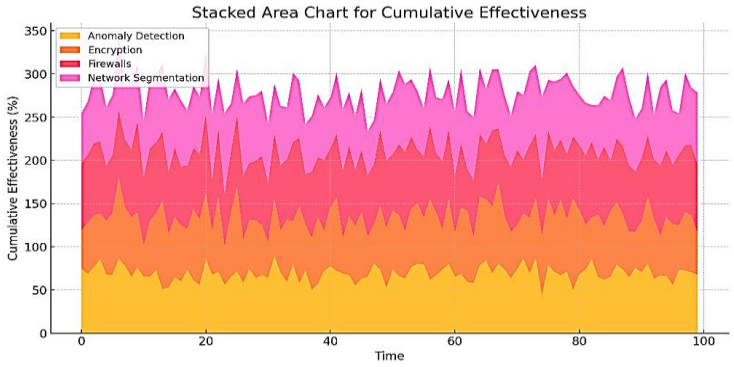

Figure 15. Stacked Area Chart for Cumulative Effectiveness

Fig 15: The stacked area chart visualizes the cumulative effectiveness of four security measures: anomaly detection, encryption, firewalls, and organized segmentation over time. Each layer of the chart speaks to the commitment of one security degree to the general adequacy, with the overall effectiveness expanding as you move upward. The chart reveals how each degree reliably contributes to the, by and large, security, with Network Segmentation and Firewalls giving critical scope, as seen by their more significant areas. The total impact shows a steady increment in overall security effectiveness over the timeline, demonstrating that these measures work together to upgrade the assurance of IoT systems. This visualization successfully demonstrates the layered approach in cybersecurity, where combining numerous measures results in a more robust defense against threats.

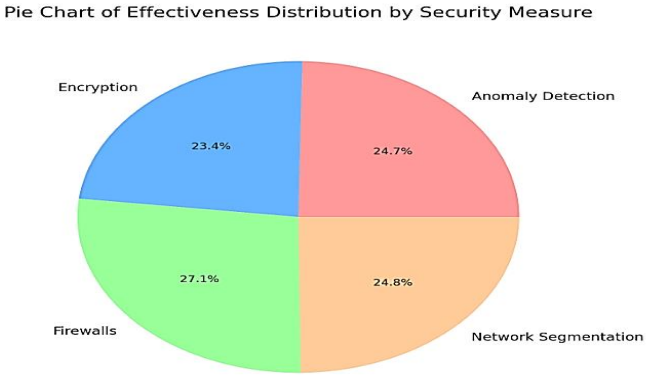

Fig. 16. Pie Chart of Effectiveness Distribution by Security Measure

Fig 16 chart outlines the dissemination of effectiveness among four key security measures: Anomaly Detection, Encryption, Firewalls, and Network Segmentation. Each section represents the extent of total effectiveness credited to each security degree. Firewalls account for the biggest share at 27.1%, followed closely by Network Segmentation at 24.8% and Anomaly Detection at 24.7%. Encryption, whereas still critical, contributes the slightest at 23.4%. This visualization highlights the relative commitment of each degree to general security, appearing that. In contrast, all measures are important, and firewalls play a marginally more prevailing role in the effectiveness of the security technique.

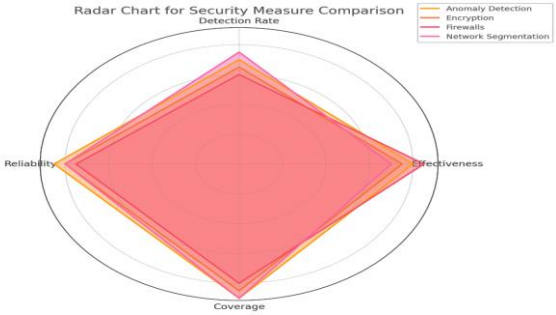

Fig. 17. Radar Chart for Security Measure Comparison

The radar chart gives a comparative outline of four security measures—Anomaly Detection, Encryption, Firewalls, and Network Segmentation—across four execution measurements: Detection Rate, Effectiveness, Reliability, and Scope. Each security degree is plotted along the tomahawks compared to these measurements, allowing for a visual comparison of their qualities and shortcomings. The chart uncovers that all four security measures perform additionally compared to the measurements, with slight variations. Firewalls and Arrange Division appear to perform better in coverage and effectiveness, while anomaly detection and encryption demonstrate robust, well-rounded overall execution measurements. This radar chart is valuable for evaluating the adjustments and trade-offs between distinctive security procedures in an IoT network.

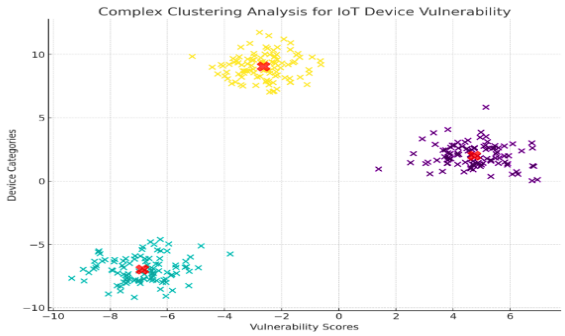

Fig. 18. Complex Clustering Analysis for IOT Device Vulnerability

This clustering diagram visualizes the results of a K-Means clustering examination on test information. The graph categorizes IoT gadgets into three clusters based on their vulnerability scores, with each cluster speaking to a distinctive hazard level. The cluster centers are stamped with red 'X' images, outlining the central focuses of each group.

V. Conclusions

This study explored techniques and security measures to relieve DDoS attacks in IoT systems, utilizing detailed factual investigation to assess their effectiveness. By analyzing data from distinctive IoT devices, we recognized noteworthy variables contributing to the vulnerability of gadgets and the viability of security conventions. The discoveries uncovered that whereas different security measures, such as anomaly detection, encryption, and network segmentation, generally performed well, their effectiveness varied over distinctive scenarios. Outstandingly, the study highlighted the solid relationship between detection rates and the success of these measures in avoiding DDoS attacks, recommending that upgrading discovery capabilities might altogether improve extensive security in IoT situations. These bits of knowledge are important for making strides in IoT organizing resilience against advancing cyber threats.

Conflict of Intrest

There is no conflict of interest regarding this article.

References

I. Aldawood, H., & Skinner, G.. Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE International Conference on Teaching, assessment, and Learning for Engineering (TALE), vol 10, no. 5, pp. 62-68). IEEE. 2018, December

II. Al-Hadhrami, Y., & Hussain, F. K. DDoS attacks in IoT networks: a comprehensive systematic literature review. World Wide Web, Vol 24, no 3, pp 971-1001. 2021.

III. Ali, I., Sabir, S., & Ullah, Z. Internet of things security, device authentication and access control: a review. arXiv preprint arXiv: Vol 14, no 2, pp 1901-1920, 2019.

IV. Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE), Vol.12, No.4, pp. 264-273, 2023

V. H. Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua, Vol.74, No.1, pp. 965-981, 2023

VI. H. Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE), Vol. 12, No.4, pp. 447-453, 2023

VII. Hammad. A , E. Zhao, “Mitigating link insecurities in smart grids via QoS multi-constraint routing“, In 2016 IEEE International Conference on Communications Workshops (ICC)”, pp. 380-386. 2016

VIII. H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC" Computers, Materials & Continua, Vol.74, No.1, pp. 2097-2113, 2023

IX. Hammad, A. A., Ahmed, “Deep Reinforcement Learning for Adaptive Cyber Defense in Network Security”, In Proceedings of the Cognitive Models and Artificial Intelligence Conference, pp. 292-297, 2016

X. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems," IJCSNS Int. J. Comput. Sci. Netw. Secur, Vol.18, No.12, pp 125-130, 2018

XI. Hossein Shirazi, Bruhadeshwar. B,"Kn0w Thy Doma1n Name": Unbiased Phishing Detection Using Domain Name Based Features. In Proceedings Of The 23nd Acm On Symposium On Access Control Models And Technologies (Sacmat '18). Association For Computing Machinery, New York, Ny, Usa, pp. 69-75, 2018

XII. Hussain, S., Rajput, U. A., Kazi, Q. A., & Mastoi, S, “Numerical investigation of thermohydraulic performance of triple concentric-tube heat exchanger with longitudinal fins”, J. Mech. Cont. & Math. Sci, Vol. 16, No. 8, pp 61-73, 2021.

XIII. H. Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors" Int. J. Sci. Eng. Res, Vol.9, No.12, pp 6-10, 2018

XIV. H. Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers" In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1-7, 2020

XV. Hammad, M., Jillani, R. M., Ullah, S., Namoun, A., Tufail, A., Kim, K. H., & Shah, H, “Security framework for network-based manufacturing systems with personalized customization”, An industry 4.0 approach, Sensors, vol. 23. No. 17-55, 2022

XVI. H. Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems" In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1-8, 2018

XVII. H. Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors", Journal Of Mechanics Of Continua And Mathematical Sciences, Vol.6, No.14, pp. 956-972, 2019

XVIII. H. Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers" In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1-7, 2020

XIX. H. Huang, J. Tan And L. Liu, "Countermeasure Techniques For Deceptive Phishing Attack", International Conference On New Trends In Information And Service Science, Beijing, pp. 636-641, 2009

XX. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems" IJCSNS Int. J. Comput. Sci. Netw. Secur, Vol.18, No.12, pp 125-130, 2018