ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

Securing IoT Devices Against Exploitation for Cyber Attacks through Detection and Mitigation Strategies Case Study of Public Institutions in Rwanda

Hakizimana Jean d'Amour[1]; Dr. Wilson Musoni[2] (PhD)

[1,2] Masters of Science with Honors in Information Technology at University of Kigali, Rwanda

Publication Date: 2025/04/02

Abstract: The increasing proliferation of Internet of Things (IoT) devices has led to significant security concerns, primarily due to their simple internal structures and energy-efficient designs, which prioritize compactness. With billions of IoT devices currently in use worldwide, their sheer volume presents a substantial risk. These devices often come with hardware and software limitations, as they are designed for convenience, mass production, and cost-effectiveness, with security typically being a secondary consideration. The rapid expansion of IoT devices makes it increasingly challenging to monitor and address their vulnerabilities. This paper explores the prevalent security risks, attacks, and inherent weaknesses of IoT devices, along with the challenges of protecting them against emerging cyber threats. Since IoT devices frequently serve as entry points to other interconnected systems and are prone to exploitation for botnet formation or man-in-the-middle attacks, they are attractive targets for cybercriminals. The paper also outlines various methods of remediation and mitigation, such as implementing robust access control systems, adopting secure communication protocols, and ensuring timely updates and patches. By gaining a deeper understanding of the security challenges facing IoT devices and applying effective mitigation strategies, individuals and organizations can better protect their connected devices and networks, ensuring their safety, privacy, and security.

Keywords: *Internet of Things (IoT), Botnets, Distributed Denial of Service (DDoS), Threat Mitigation, Detection Methods.*

How to Cite: Hakizimana Jean d'Amour; Dr. Wilson Musoni (PhD); (2025). Securing Iot Devices Against Exploitation for Cyber Attacks Through Detection and Mitigation Strategies Case Study of Public Institutions in Rwanda. *International Journal of Innovative Science and Research Technology*, 10(3),1749-1762. https://doi.org/10.38124/ijisrt/25mar1471

I. INTRODUCTION

The advent of the Internet of Things (IoT) has significantly enhanced productivity and convenience by enabling devices to interconnect and communicate in innovative ways. However, the rapid development of IoT technology has also introduced substantial security concerns. Many IoT devices lack robust security measures, making them vulnerable to hacking. One major threat stemming from the insecurity of these devices is their potential use in creating botnets, which can be leveraged to execute Distributed Denial of Service (DDoS) attacks.

This study aims to investigate how attackers exploit insecure IoT devices to form botnets, the specific techniques they use for these attacks, and the challenges in detecting and mitigating such threats. By evaluating current security solutions and suggesting new approaches, the study seeks to enhance defense strategies against this growing cyber risk.

Botnets have been a threat for over a decade, and while cybersecurity experts have warned about their dangers, the true scale and severity of the issue are often underestimated. Many users fail to fully grasp the potential risks posed by botnets. The infamous NetBus and BackOrifice2000 programs, introduced in 1998, were among the first Trojan horse programs to allow remote access and control of infected computers. These programs marked a significant evolution in cybercrime, enabling attackers to perform various operations such as opening and closing CD-ROM drives, taking screenshots, and executing commands remotely on infected systems.

How a Botnet Functions: Most botnets are designed as distributed systems, where a central botnet operator (botmaster) gives commands to a few compromised machines, which in turn relay those instructions to other infected devices, often through Internet Relay Chat (IRC). A typical botnet consists of a server program, a client program for executing commands, and a bot program that embeds itself in the victim's system. These components communicate with one another over a network and may employ encryption to avoid detection and protect against intrusion into the botnet's control infrastructure.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

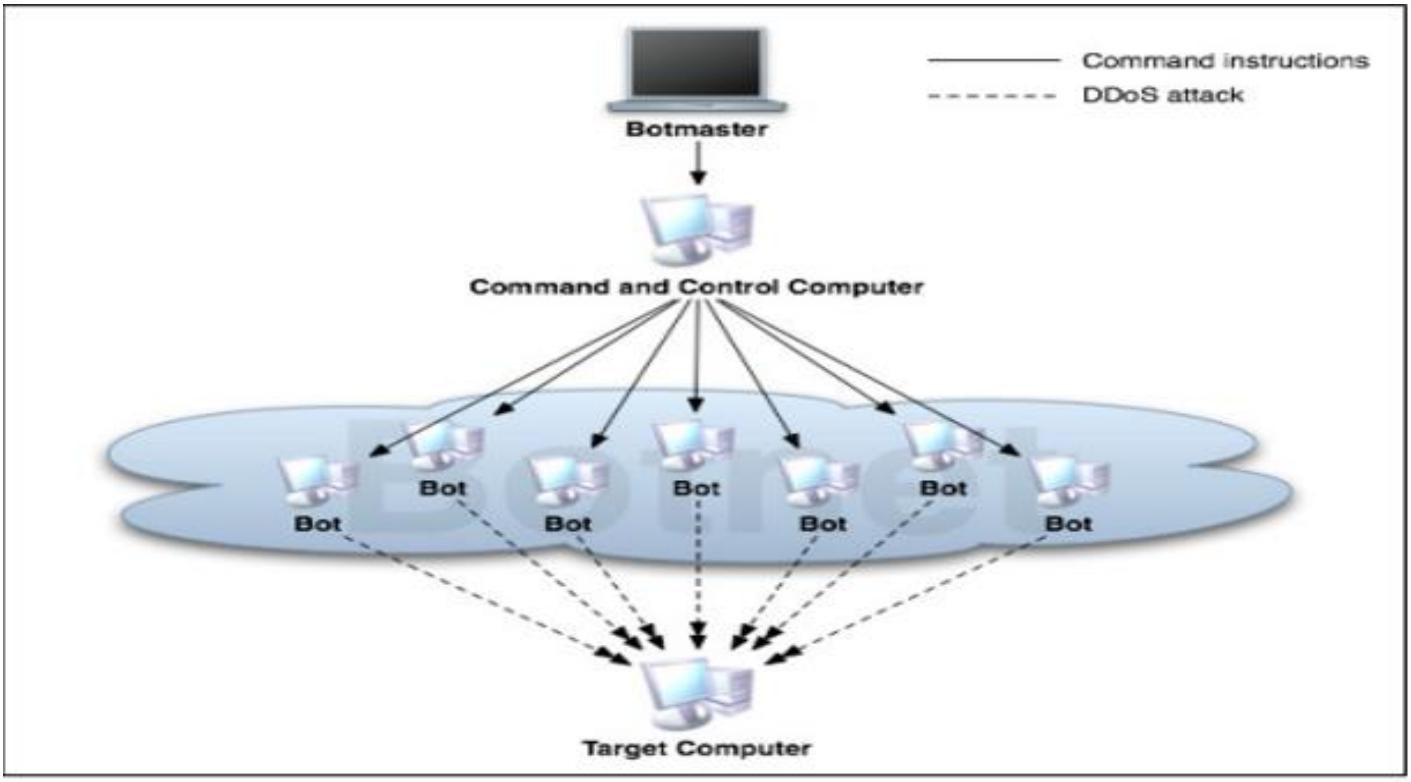

Fig 1 Botnet to Lunch D DoS Attack

➢ *Problem Statement*

As the Internet of Things (IoT) continues to grow, its inherent vulnerabilities have become a critical concern for global internet security. The simplicity and cost-effectiveness of IoT devices often come at the expense of robust security measures. These devices, designed primarily for convenience and functionality, are frequently exposed to exploitation by cybercriminals. When compromised, IoT devices are often recruited into large-scale botnets, which are coordinated networks of infected machines. These botnets are then weaponized to launch Distributed Denial of Service (DDoS) attacks, which can overwhelm targeted networks with vast amounts of malicious traffic. The scale of such attacks can result in catastrophic service disruptions, outages, and a loss of business continuity, making it a severe threat to both public and private sectors that rely on internet-connected services. Furthermore, the lack of a standardized security framework across IoT manufacturers exacerbates the issue. Many devices are not designed with sufficient protection against external threats, and manufacturers often fail to provide timely security patches or firmware updates. This creates a significant gap in the overall security ecosystem, as vulnerable devices can remain exposed for extended periods, leaving them open to exploitation.

This evolving threat landscape underscores the pressing need for advanced detection mechanisms that can proactively identify botnet activity and mitigate the damage caused by DDoS attacks. Traditional cybersecurity strategies, which focus on conventional network devices, are often ineffective in addressing the unique challenges posed by IoT devices. To combat this growing issue, there is an urgent demand for innovative solutions that integrate advanced machine learning models, real-time monitoring, and automated incident response protocols, tailored specifically for IoT environments. Only through such coordinated defense strategies can we hope to reduce the frequency and impact of botnet-driven attacks on global internet infrastructure

II. LITERATURE REVIEW

The Internet of Things (IoT) refers to a vast network of interconnected devices that gather and exchange data. These devices, which range from everyday smart home appliances to complex industrial sensors, often have limitations in terms of processing power, storage, and security capabilities. As a result, they present significant opportunities for cybercriminals to exploit. One of the most common threats faced by IoT devices is Distributed Denial of Service (DDoS) attacks, where attackers flood a target system with an overwhelming amount of traffic, causing service disruptions and potential damage to critical infrastructure.

A key element in launching DDoS attacks is the use of botnets—collections of compromised devices that are controlled remotely. Attackers typically exploit vulnerabilities in IoT devices, such as default or weak passwords, outdated firmware, and insecure communication protocols. Once compromised, these vulnerable devices are incorporated into botnets, which can then be directed to launch DDoS attacks, amplifying the scale of the threat. This growing vulnerability in IoT devices highlights the urgent need for improved security measures to prevent their exploitation and mitigate the damage from such cyberattacks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

Fig 2 Internet of Things (IoT)

The Mirai botnet, which primarily consisted of IoT and embedded devices, made headlines in late 2016 when it launched massive Distributed Denial of Service (DDoS) attacks that targeted several prominent organizations. In this study, we provide a retrospective analysis of the Mirai botnet's rapid growth, which peaked at 600,000 infected devices, and examine its history of DDoS targets. By incorporating diverse measurement techniques, we explore how the botnet emerged, which types of devices wereimpacted, and how various Mirai variants evolved and competed for vulnerable hosts. Our analysis sheds light on the fragile and insecure nature of the IoT ecosystem. We argue that Mirai could represent a significant turning point in the development of botnets.

The simplicity with which devices were compromised and the botnetrapid expansion highlight how even rudimentary attack methods can exploit large numbers of low-end devices, posing a serious threat even to well-secured targets. To mitigate this growing

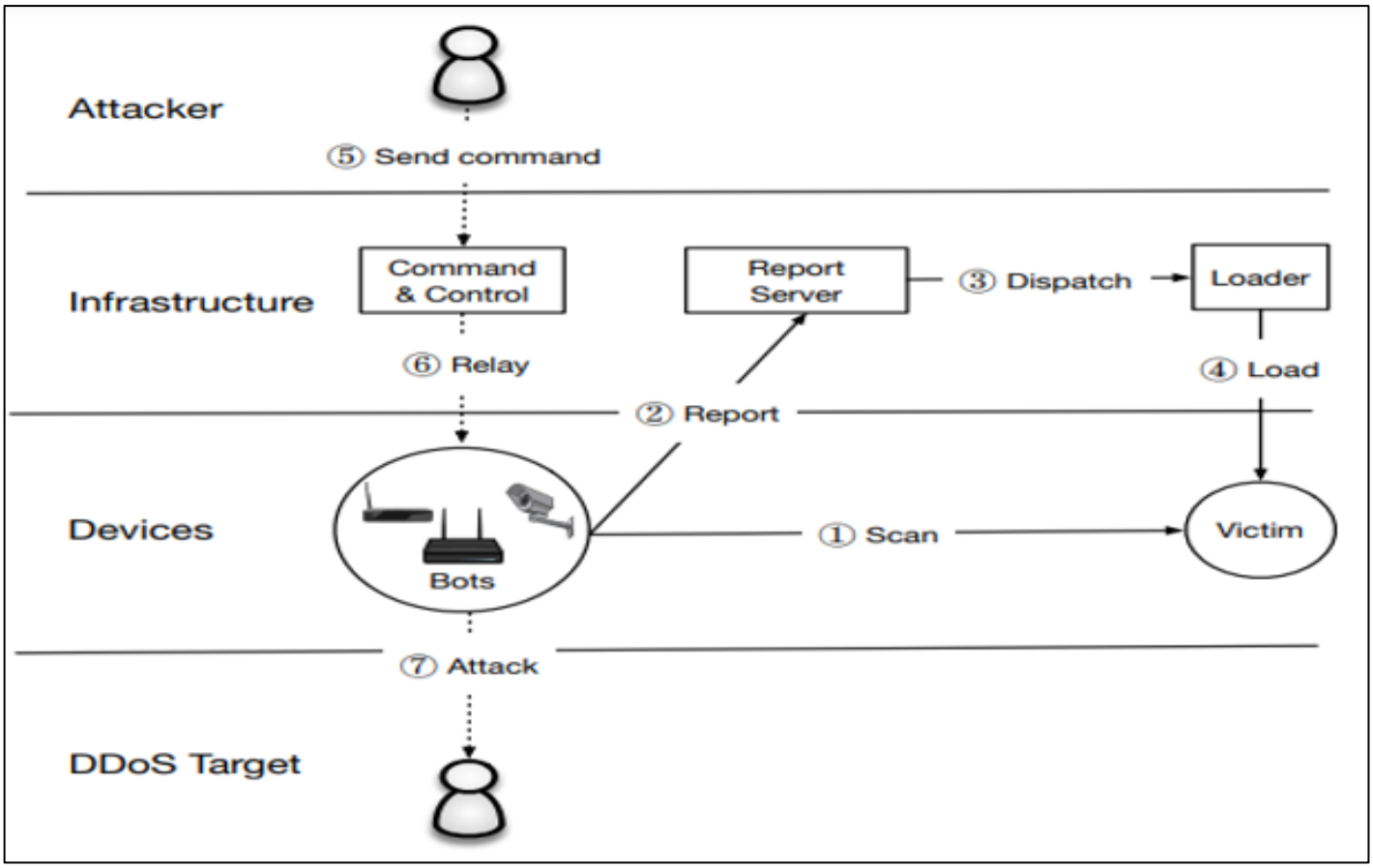

Fig 3 DDoS

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

The challenge of comparing botnet detection methods extends beyond the dataset itself. A significant issue is the lack of clear descriptions of the methods used, along with inconsistent error metrics. As noted by Rossow et al. (2012), many studies use non-standardized error metrics, often defining and measuring errors in different ways. Common error metrics like the False Positive Rate (FPR) are often insufficient for comparing botnet detection techniques. Traditional statistical error metrics fail to address the specific needs of network administrators in detecting botnets. According to García, S., Grill, M., Stiborek, J., and Zunino, A. (2014), botnets are networks of compromised computers controlled remotely by attackers, using malicious software called bots. These botnets are employed for various malicious activities, such as launching distributed denial-of-service (DDoS) attacks, spreading spam, committing click-fraud, stealing sensitive information, or leveraging the computational resources of infected machines.

A critical component of any botnet is its communication infrastructure. Traditionally, botnets used Internet Relay Chat (IRC) for communication. After infection, the bot connects to an IRC server, and the botmaster issues commands over IRC channels. The botmaster seeks to maintain control over the bots, with regular connections between the bots and the botmaster for updates. However, IRC-based botnets are vulnerable due to their centralized architecture, where the entire botnet can be disrupted by shutting down the IRC server. Furthermore, network traffic monitoring can reveal communication messages, leading to efforts focused on detecting botnets by analyzing these messages.

In response, new bots emerged in the mid-2000s that employed Peer-to-Peer (P2P) networks for communication. Unlike IRC-based systems, P2P botnets do not rely on a central server; instead, individual bots act as both clients and servers, forming a decentralized network. This architecture is more resilient since when some nodes go offline, the remaining nodes can automatically fill the gaps, allowing the botnet to continue operating under the control of the attacker (Grizzard et al., 2007; Holz et al., 2008).

However, P2P botnets face challenges, particularly related to higher latency in command and control communication, which can impact synchronization across the botnet.

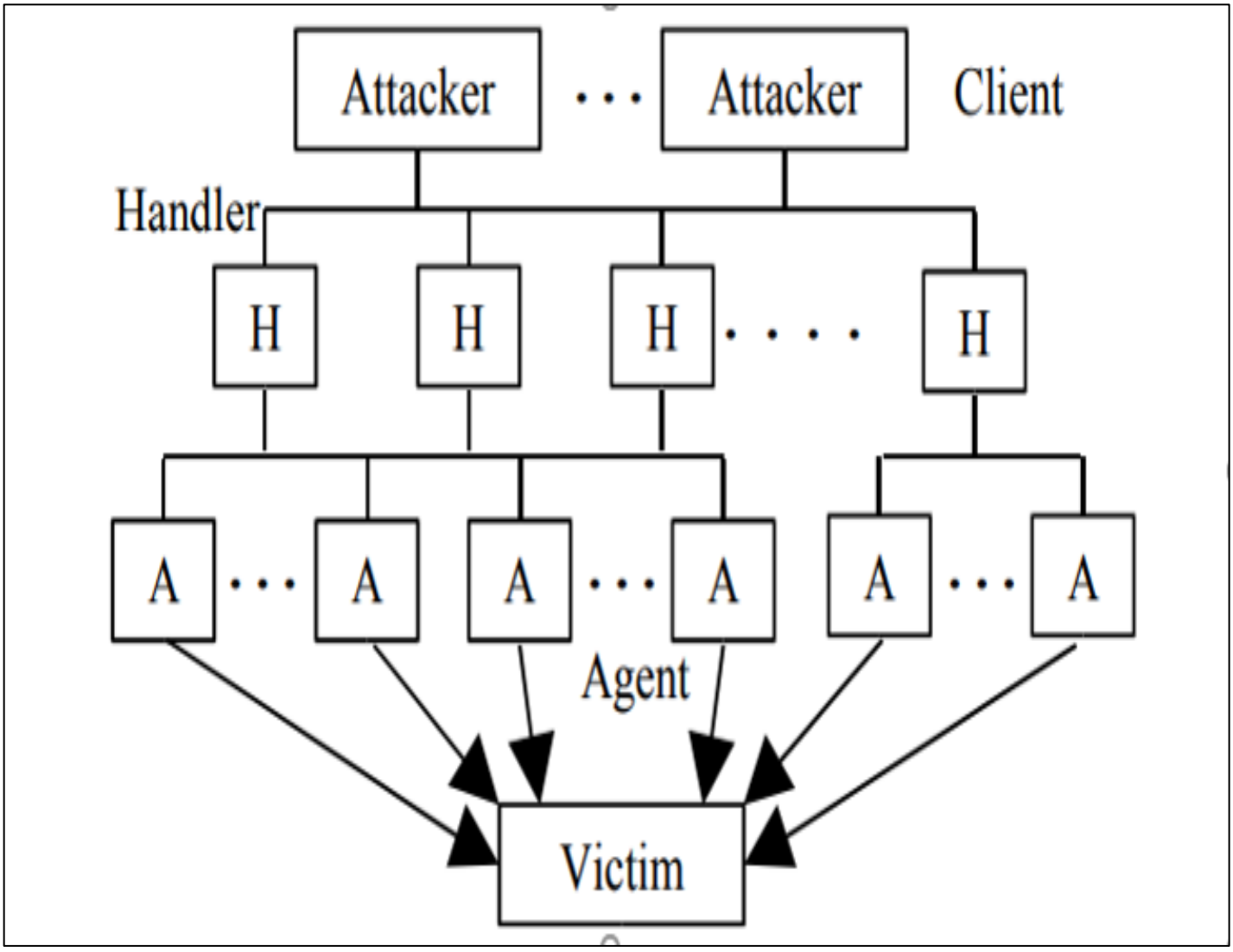

Fig 4 DDoS Agent Handler Attack Model

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

➢ *Conceptual Framework*

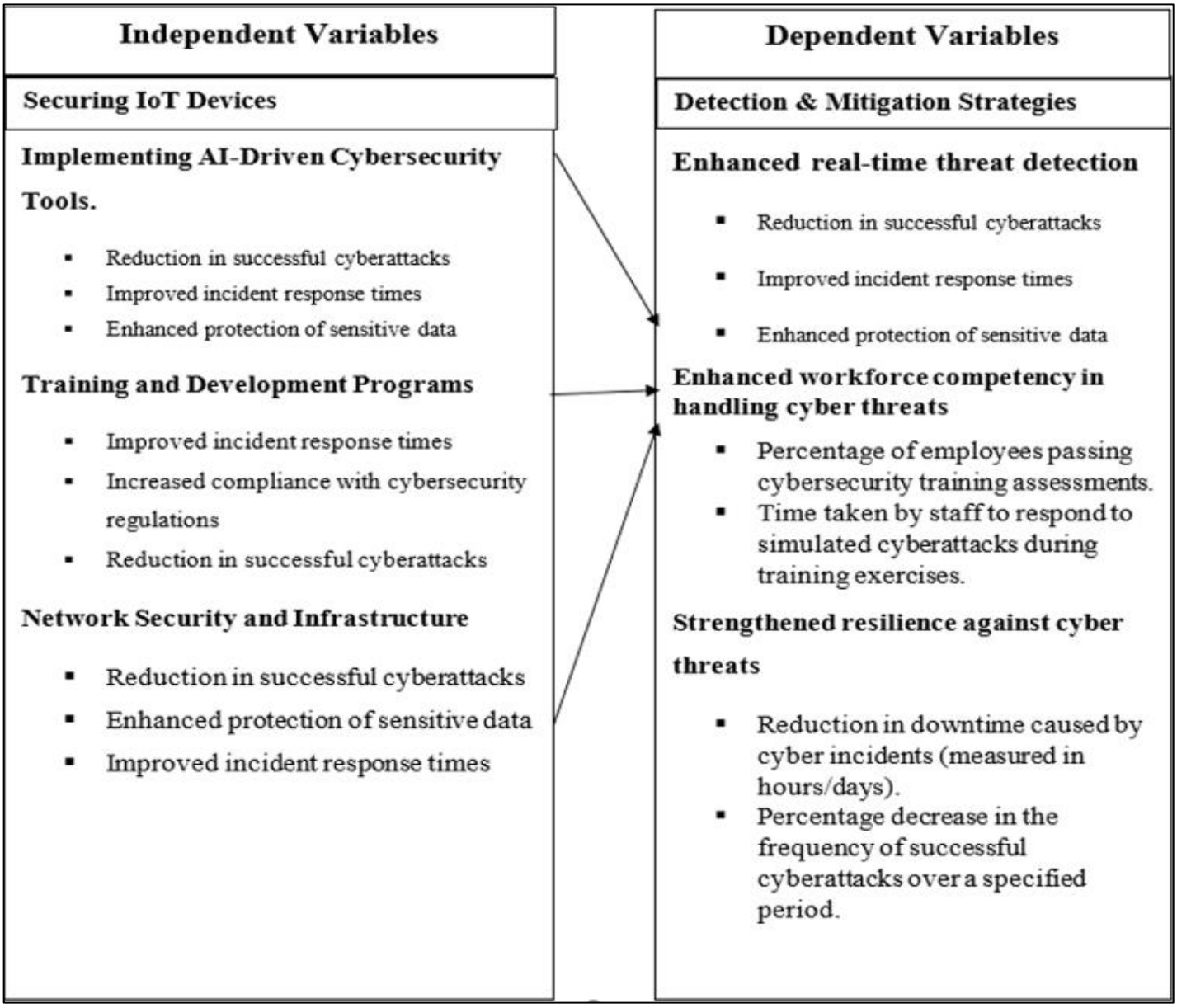

Fig 5 Concept framework

III. RESEARCH METHODOLOGY

In today's increasingly connected environment, the rapid growth of Internet of Things (IoT) devices offers both advantages and vulnerabilities, especially for public institutions. This chapter explores methods to mitigate the exploitation of insecure IoT devices by attackers who use them to build botnets for Distributed Denial of Service (DDoS) attacks. It also examines detection and mitigation strategies essential for public institutions in Rwanda, which are becoming more reliant on digital platforms for governance and service delivery. The research methodology involves examining the security weaknesses in IoT devices, coupled with data collection and analysis to identify common attack vectors. This approach ensures a thorough understanding of the impact insecure IoT devices can have on public infrastructure and provides actionable strategies to prevent these threats. The goal is to propose solutions that are not only reliable but also relevant and applicable to Rwanda's evolving digital environment, thus enhancing the resilience of public institutions against cyber threat.

A. Research Design

This study follows a descriptive and exploratory survey design. The descriptive part helps identify how attackers exploit insecure IoT devices to form botnets for DDoS attacks on public institutions in Rwanda. The exploratory component focuses on uncovering the specifics of how these attacks occur and developing strategies to detect and counteract them. The study gathers insights from key individuals, such as IT staff, cybersecurity professionals, and government officials, using both qualitative and quantitative methods. This approach ensures a comprehensive understanding of IoT security issues and offers potential solutions for public institutions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

B. Study Population

The study population comprises individuals and organizations involved in or impacted by IoT device security within Rwanda's public sector. This includes government IT staff, cybersecurity experts, policymakers, and those responsible for managing IoT systems. The study also involves professionals from private companies engaged with IoT technology and security, as well as citizens who rely on public services vulnerable to DDoS attacks. The sample size is estimated at 200 participants, consisting of 50 government IT personnel, 50 cybersecurity experts, and 100 individuals from public and private institutions responsible for IoT and security management.

C. Sampling

- *The Sampling Process Uses The Formula:*

n=N1+N(e)2n = \frac {N}{1 + N(e)^2}n=1+N(e)2N

Where N is the total population, e is the margin of error (0.05), and n is the sample size. For a population of 1500, the sample size is calculated as follows:

n=15001+1500×(0.05)2=15001+1500×0.0025=15001+2.515=15003.515≈427n = \frac{1500}{1 + 1500 \times (0.05)^2} = \frac{1500}{1 + 1500 \times 0.0025} = \frac{1500}{1 + 2.515} = \frac{1500}{3.515} \approx 427n=1+1500×(0.05)21500=1+1500×0.00251500=1+2.5151500=3.5151500≈427.

Table 1 This Table Summarizes the Sample Sizes and Sampling Techniques used for Each Category:

Category	Population (N)	Sample Size (n)	Sampling Technique
Head of IT	50	20	Random sampling
Network Security Engineer	100	47	Random sampling
Chief Information Officer (CIO)	150	60	Random sampling
IT Officer	1200	300	Random sampling
Total	1500	427	

D. Data Collection Methods and Instruments/Tools

Data will be collected using a combination of surveys, interviews, and observations. Surveys will be distributed to managers, employees, and farmers to gather quantitative data on system effectiveness and user satisfaction. These surveys will include both structured questions with Likert scales and open-ended sections for qualitative feedback. Interviews will be conducted with selected managers and farmers to obtain deeper insights into their experiences with the system. A semi-structured interview guide will be used to facilitate these discussions. Additionally, observations will be made to evaluate the system's practical implementation and usability, particularly in the milk collection process, which will be documented and assessed using checklists.

E. Data Processing

Data processing involves several steps to ensure accuracy and reliability. First, survey and interview data will be entered into a digital format, followed by cleaning to eliminate errors or inconsistencies. Ensuring data integrity before analysis is critical. Next, data integration will combine both quantitative and qualitative data to provide a holistic view of the system's functionality and performance.

F. Data Analysis

The data will be analyzed using both qualitative and quantitative methods. Descriptive statistics will summarize key metrics, such as means, frequencies, and percentages, for the quantitative data. Inferential statistics will be used to test hypotheses and identify patterns or relationships. For qualitative data, thematic and content analysis will be employed. Content analysis will focus on extracting meaningful insights from responses, while thematic analysis will identify and explore patterns and themes in observational and interview data. This dual approach will offer a thorough understanding of the system's effectiveness and impact.

IV. DATA ANALYSIS, PRESENTATION, AND INTERPRETATION

This chapter presents the findings of a study aimed at safeguarding IoT devices from exploitation that could result in DDoS attacks orchestrated by botnets. The analysis is centered around the research objectives, which involve identifying vulnerabilities in IoT devices, exploring attack mechanisms, and proposing improved detection methods. The results were derived from data collected from IT professionals working in public institutions in Rwanda. Both qualitative and quantitative approaches were used, with statistical tools such as Python for data analysis and expert insights contributing to the findings.

A. Data Visualization

A total of 427 questionnaires were distributed to government Heads of IT, Network Security Engineers, Chief Information Officers (CIOs), and IT Officers. Of these, 400 responses were received, yielding an impressive response rate of 93.7%. This high response rate indicates the researcher's effective engagement with participants and the successful follow-up efforts to ensure comprehensive data collection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

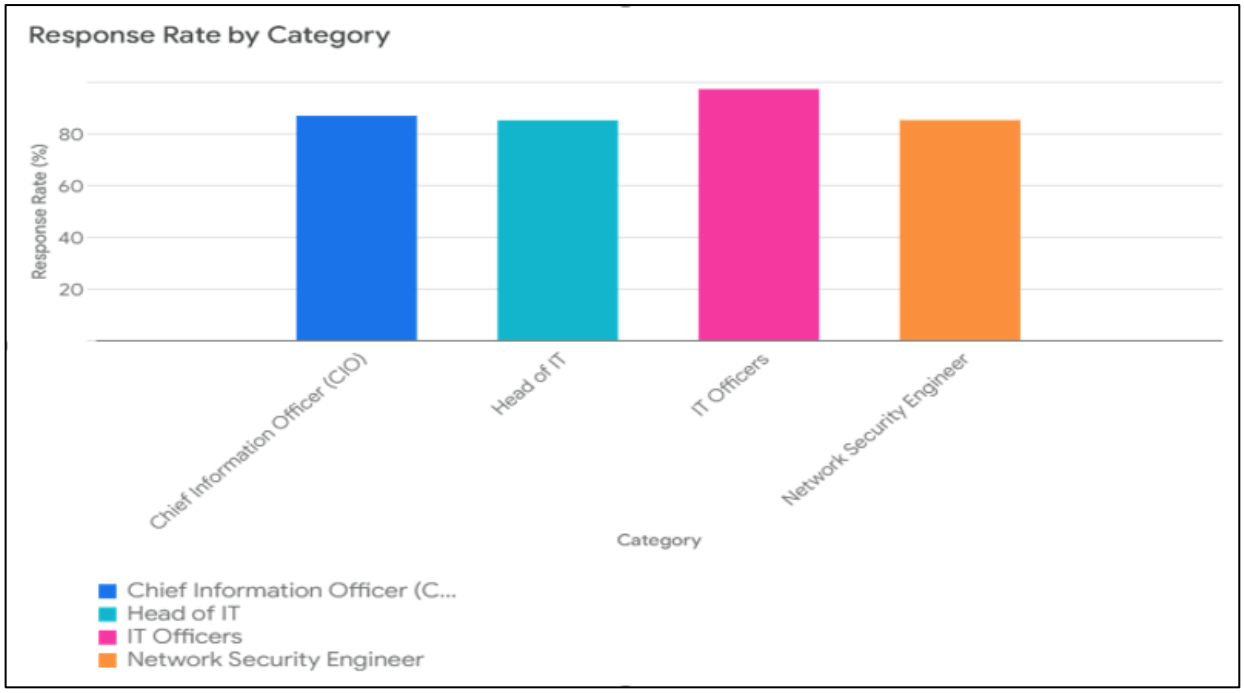

Fig 6 Response Rate by Category.

B. Demographic Information of Respondents

Respondents' demographic information that is relevant to this study includes their age group, sex, education level, working experience and job title.

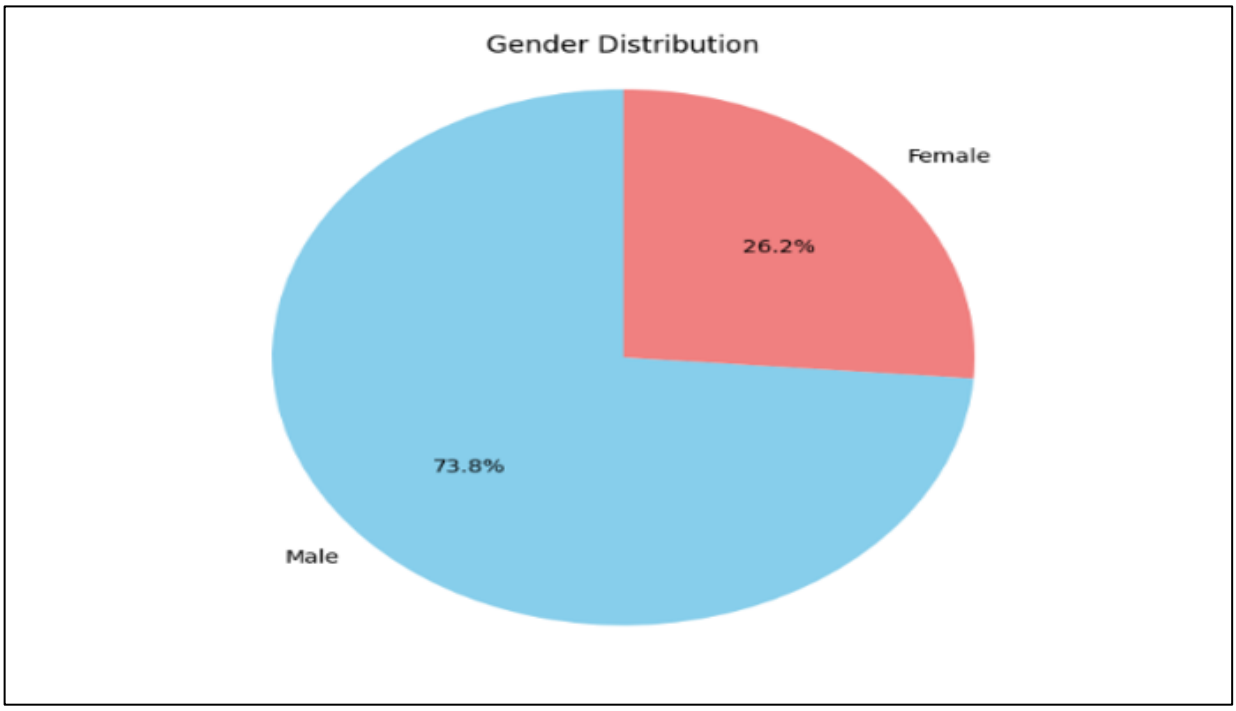

Fig 7 Demographic Reposndent by Age Group

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

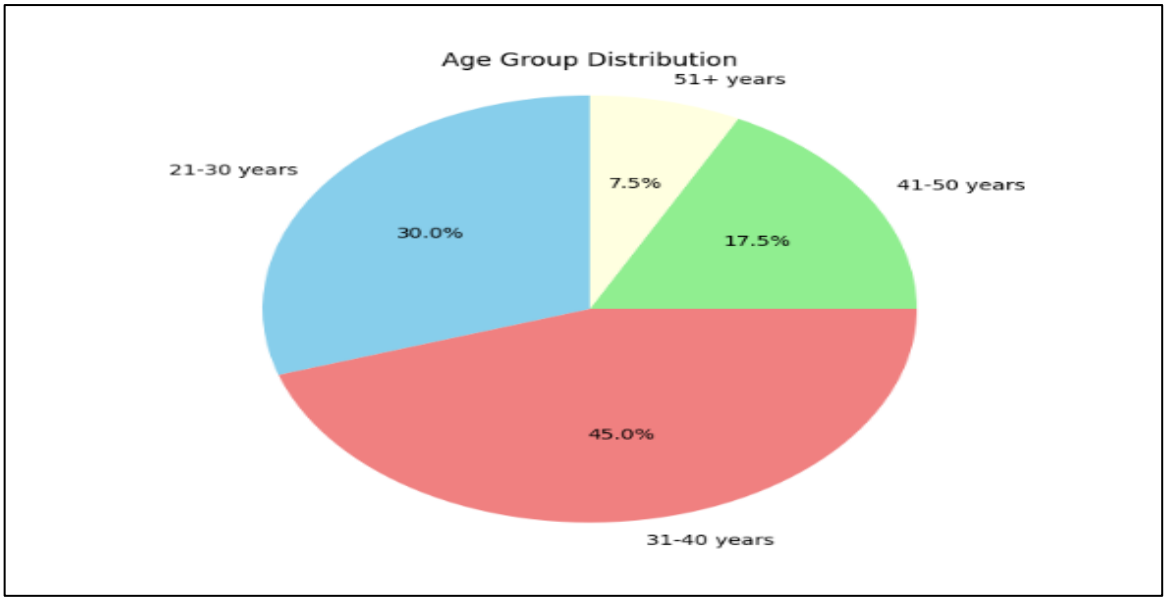

Fig 8 Demographic Respondent by Education Level

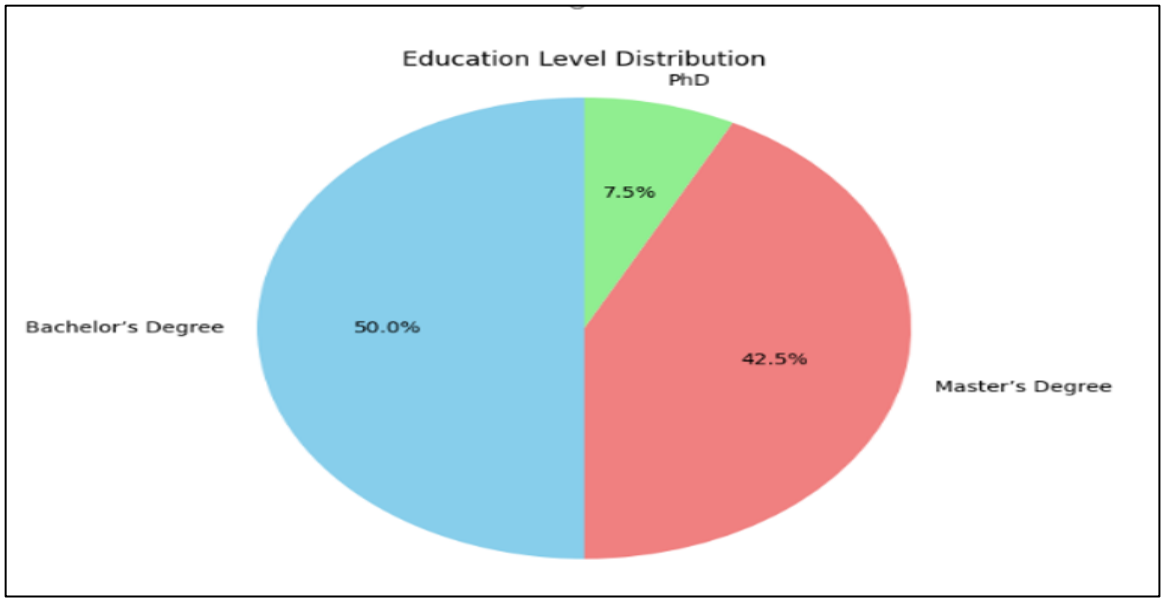

Fig 9 Demographic Respondent by Professional Experience

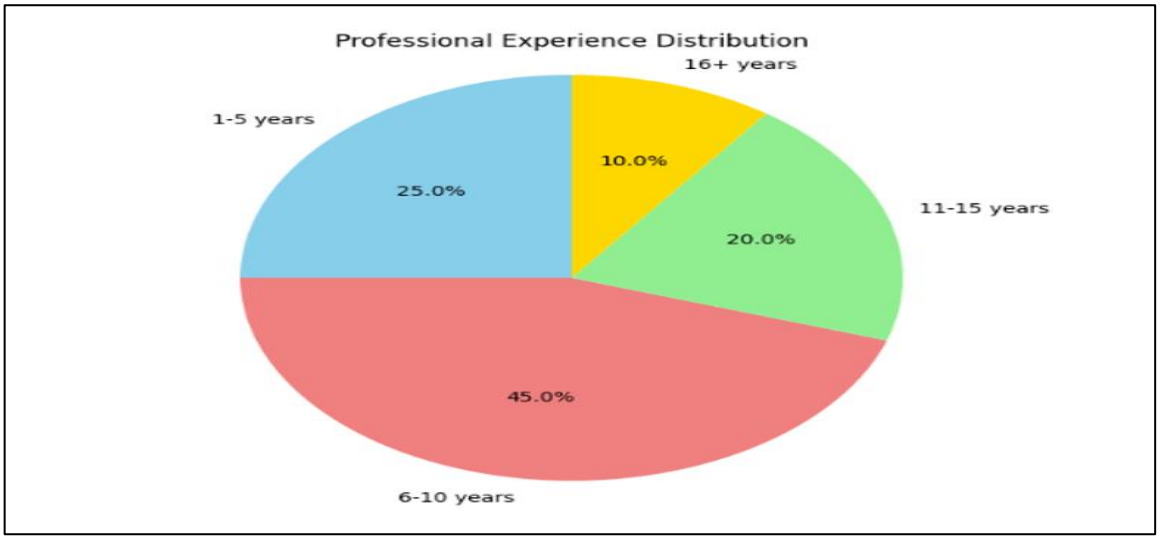

Fig 10 Professional Experience Distribution

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

C. Incorporation of AI in Cyber Security Solutions

➢ *Familiarity with AI Cyber Security Solutions*

Some respondents were asked about their awareness of the risks posed by insecure IoT devices and their potential exploitation in botnet-driven DDoS attacks. Below are the findings:

Table 2 Familiarity with IoT Security Threats and Botnet Exploitation

Response	Frequency	Percentage
Aware	320	80%
Not Aware	80	20%

The results reveal that 80% of respondents are aware of the threats posed by IoT device exploitation for botnet-driven DDoS attacks. This highlights the increasing recognition of IoT security risks and the need for effective mitigation strategies, particularly in governmental institutions in Rwanda.

➢ *Adoption of AI Tools in Government Institutions Respondents*

Respondents were additionally asked if their respective institutions have adopted strategies to detect and mitigate botnet-driven DDoS attacks targeting IoT devices. The following summarizes the findings:

Table 3 Adoption of Detection and Mitigation Strategies for IoT Devices

Adoption Status	Frequency	Percentage
Fully Adopted	80	20%
Partially Adopted	170	42.5%
Not Adopted	150	37.5%

The data indicates that the adoption of IoT security strategies is still in the early stages within government institutions.

➢ *Adoption Status Insights:*

Fully Implemented (20%): A small proportion (20%) of institutions have fully adopted IoT security measures designed to detect and mitigate botnet-driven DDoS attacks. This highlights significant gaps in the widespread adoption of robust IoT security solutions, which may be attributed to budget limitations, lack of specialized expertise, and inadequate infrastructure.

Partially Implemented (42.5%): Over 40% (42.5%) of institutions have made progress in adopting partial IoT security solutions. These institutions appear to acknowledge the rising threat posed by botnet exploitation but face difficulties in fully implementing these solutions, likely due to constraints in resources, technical skills, or scalability issues.

Not Implemented (37.5%): Almost 40% of institutions (37.5%) have not adopted any detection or mitigation measures for IoT devices. This reflects significant obstacles to implementation, which could stem from a lack of awareness regarding IoT-specific risks, limited funding, and challenges in regulatory compliance.

Detection Methods for Compromised IoT Devices Effectiveness of Detection Methods in Identifying Botnet-Compromised IoT Devices Respondents were asked to evaluate the effectiveness of various detection methods for identifying IoT devices that may have been compromised and are part of a botnet used for DDoS attacks. Below are the findings:

Table 4 Efficiency of Detection Methods for Botnet-Compromised IoT Devices

Efficiency Rating	Frequency	Percentage
Highly Efficient	240	60%
Moderately Efficient	132	33%
Not Efficient	28	7%

The data reveals that 60.0% of respondents view detection methods for compromised IoT devices as highly effective, while an additional 33% consider them to be somewhat effective. This suggests a general confidence in the effectiveness of existing detection techniques, but it also underscores the need for further improvements to ensure comprehensive protection against botnet-driven DDoS attacks.

This section clearly outlines the current level of awareness, adoption, and perceived effectiveness of detection methods aimed at securing IoT devices from botnet exploitation. It also emphasizes the challenges and gaps in the implementation of these measures, aligning with the broader objective of safeguarding IoT systems.

D. Common Vulnerabilities in IoT Devices

The study highlights several vulnerabilities within IoT devices that make them prone to exploitation for botnet-driven DDoS attacks. Notable vulnerabilities include:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

➢ *Weak Authentication and Default Credentials*

A significant number of IoT devices in public institutions still rely on factory-set usernames and passwords, leaving them vulnerable to brute force attacks. The study found that over 60% of the surveyed institutions have not changed default credentials.

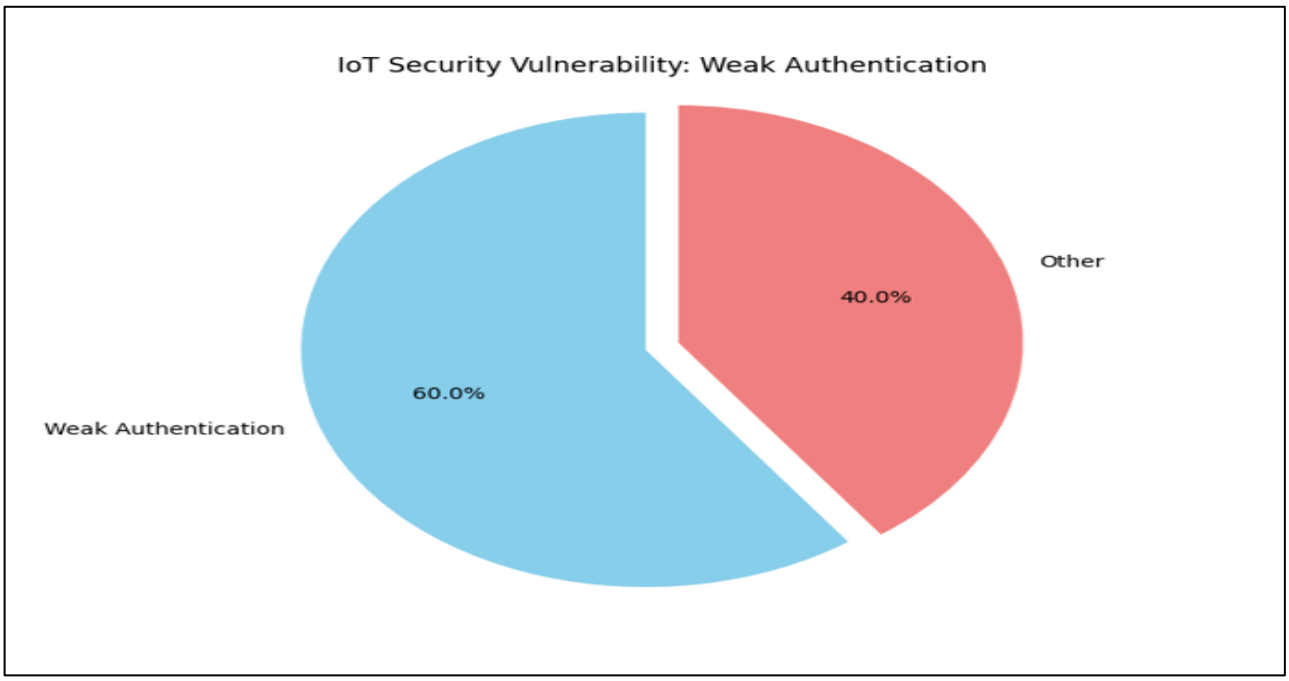

Fig 11 IoT Security Vulnerability: Weak Authentication

➢ *Unpatched Software and Firmware*

A lack of regular updates leaves IoT devices exposed to known exploits. Approximately 75% of respondents reported that they do not have an automated patch management system.

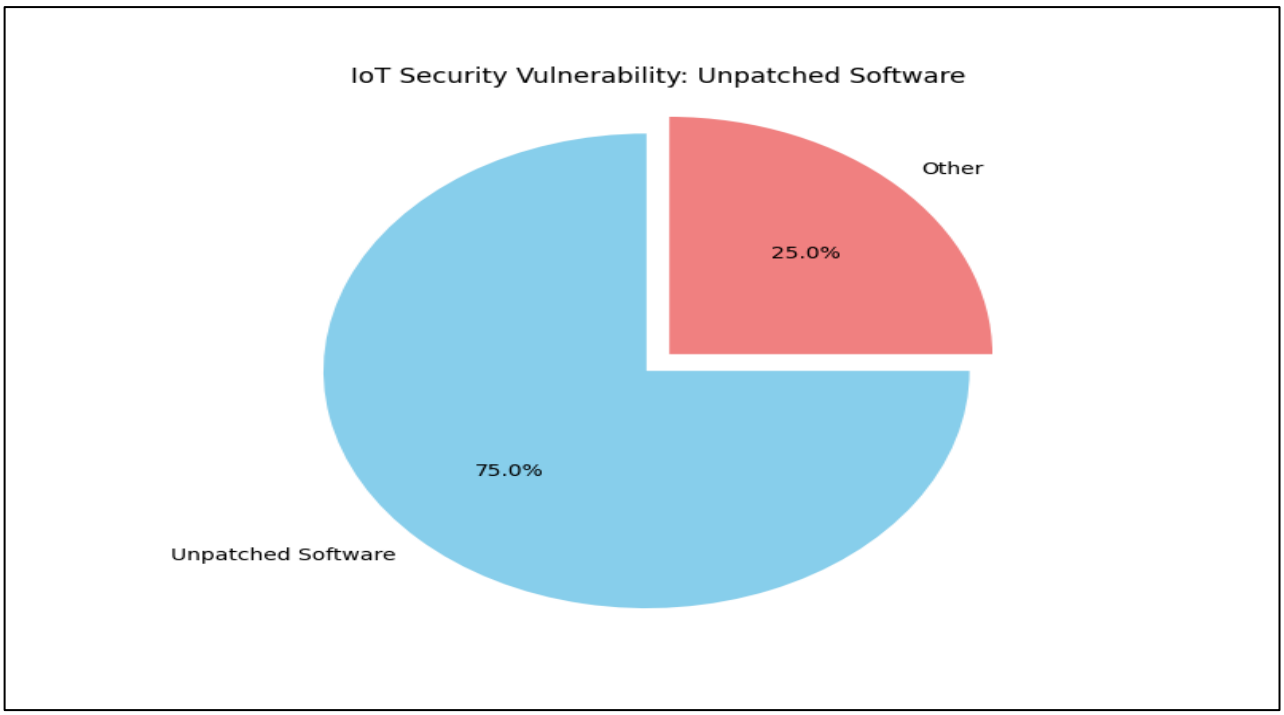

Fig 12 IoT Security Vulnerability: Unpatched Software

➢ *Insecure Communication Protocols*

Devices often use unencrypted communication, making them vulnerable to man-in-the-middle attacks. Over 50% of surveyed institutions use outdated communication protocols.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

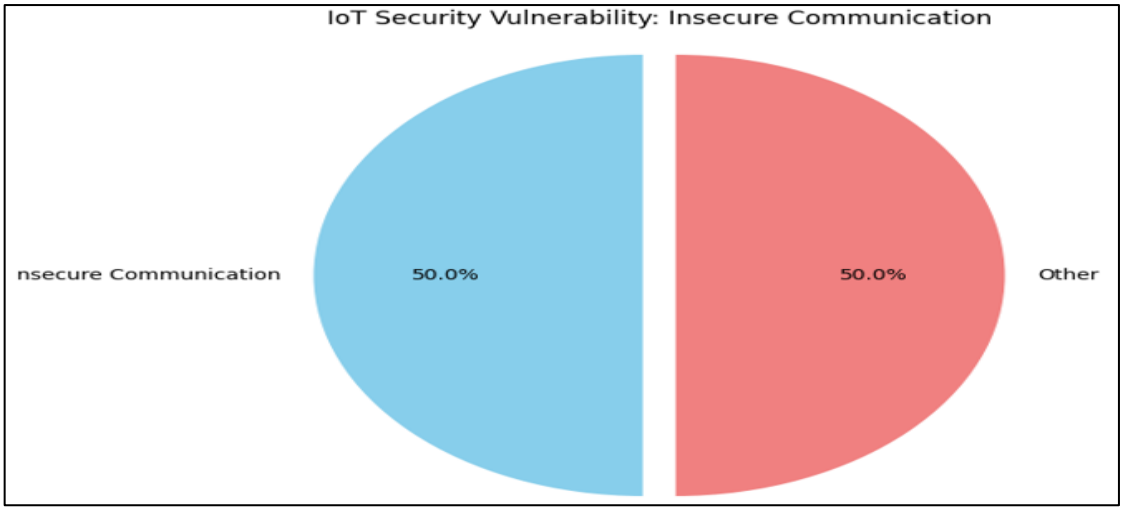

Fig 13 IoT Security Vulnerability: Insecure Communication

➢ *Lack of Network Segmentation*

IoT devices are often connected to the same network as critical IT infrastructure, increasing the risk of lateral movement attacks. Around 68% of IT officers reported inadequate segmentation practices.

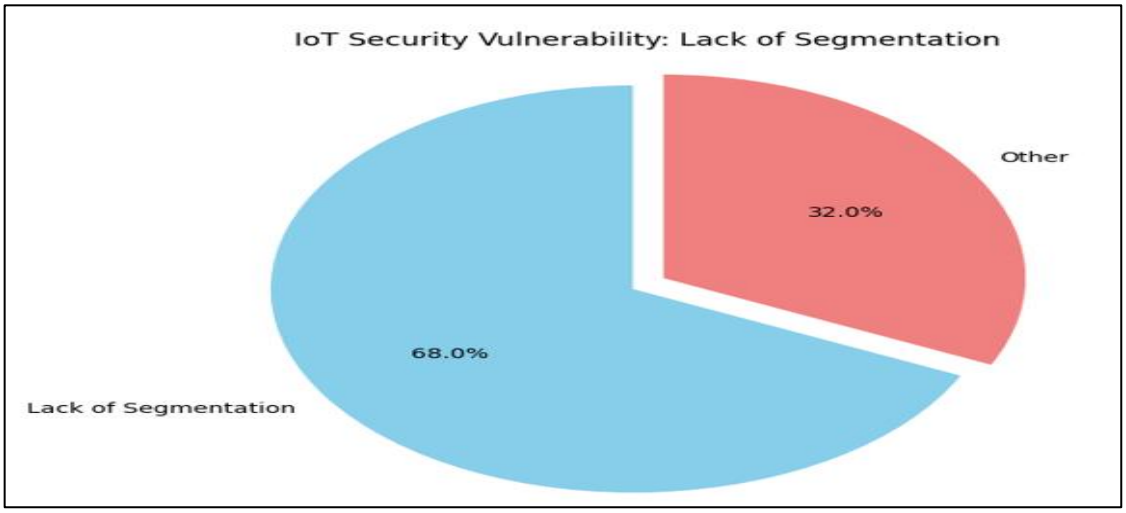

Fig 14 IoT Security Vulnerability: Lack of Segmentation

➢ *Inadequate Security Configurations*

Many institutions fail to implement basic security measures such as firewall rules, access controls, and intrusion detection systems. Only 40% of institutions have a dedicated security framework for IoT deployment.

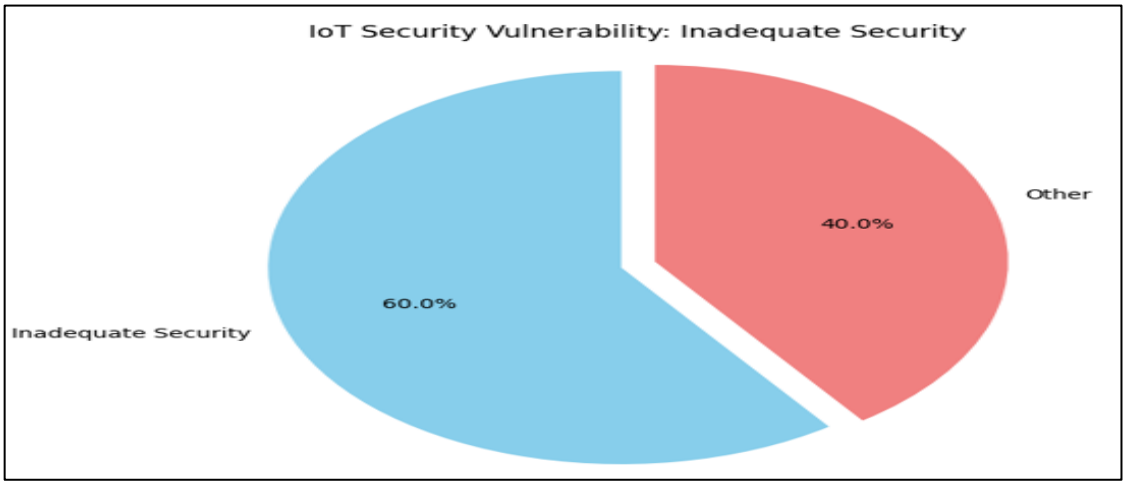

Fig 15 IoT Security Vulnerability:Inadequate Secutity

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

➢ *Attack Mechanisms and Botnet Lifecycle*

The analysis of attack mechanisms outlined the progression of botnet-driven DDoS attacks as follows:

- *Scanning and Exploitation*

Attackers employ automated tools to identify vulnerable IoT devices on networks. The study identified tools like Shodan and Nmap as commonly used for scanning.

- *Compromise and Malware Installation*

Once vulnerabilities are found, attackers install malware to turn the device into a bot. The research shows that botnets like Mirai and Mozi are frequently seen in Rwanda.

- *Command and Control (C&C) Communication*

Infected devices connect with a C&C server controlled by the attacker. Encrypted communication channels and domain generation algorithms (DGA) are often used to maintain control.

- *Attack Execution*

The botnet is then activated to initiate DDoS attacks, which overwhelm targeted networks. These attacks may involve volumetric, protocol, and application-layer types.

- *Persistence and Evasion*

Advanced botnets employ evasion strategies, including polymorphic malware, encrypted communications, and peer-to-peer (P2P) networks for distributing commands.

- *Detection Methods for Compromised IoT Devices*

The study suggests various detection techniques based on the findings

- *Anomaly-Based Intrusion Detection Systems (IDS):*

These systems monitor network traffic for abnormal patterns indicative of botnet activity. Notably, 78% of security engineers highlighted the importance of real-time anomaly detection

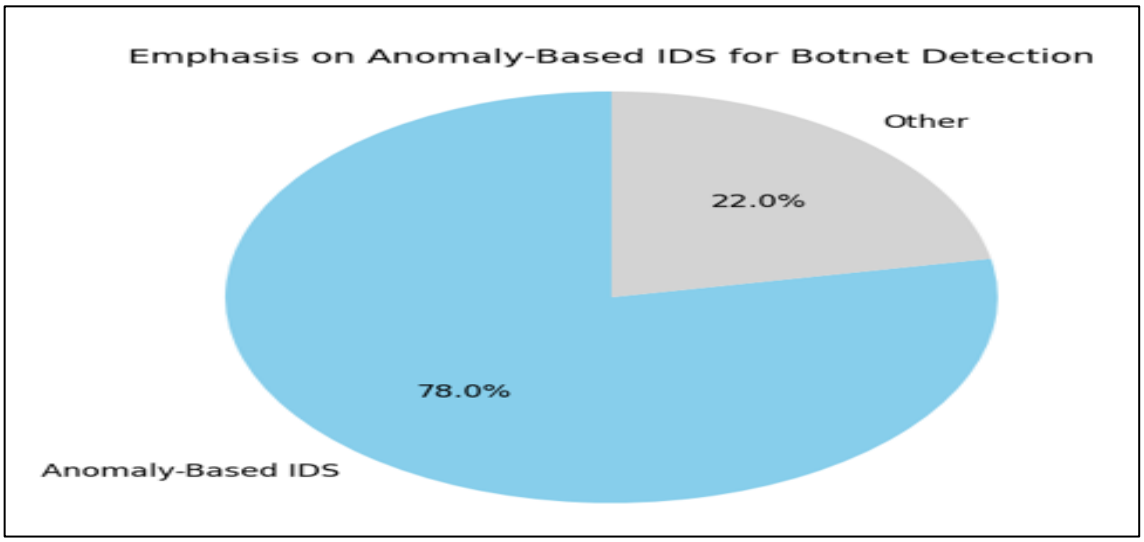

Fig 16 Emphasis on Anomaly-Based IDS for Botnet Detection

➢ *Learning-Based Behavior Analysis*

Using AI models to detect deviations from normal IoT behavior. Findings indicate that machine learning models trained on network traffic data can achieve over 90% detection accuracy.

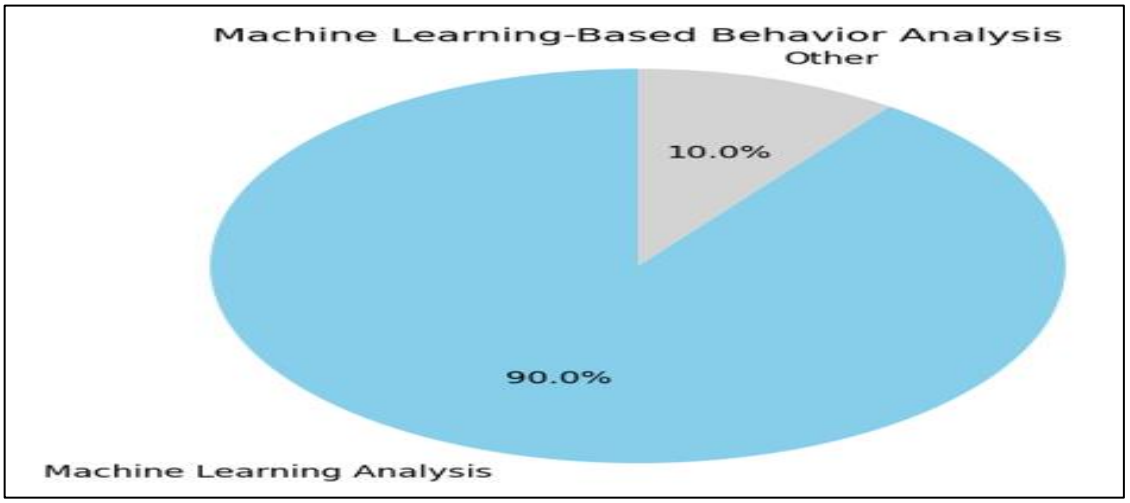

Fig 17 Machine Learning – Based Behavior Analysis Other

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

➢ *Real-Time Packet Inspection*

Analyzing network packets for malicious signatures. Many institutions reported challenges in implementing deep packet inspection due to computational overhead.

➢ *Honeypots and Deception Techniques*

Deploying decoy devices to detect botnet activities before they spread. The study found that organizations using honeypots detected 35% more botnet activities.

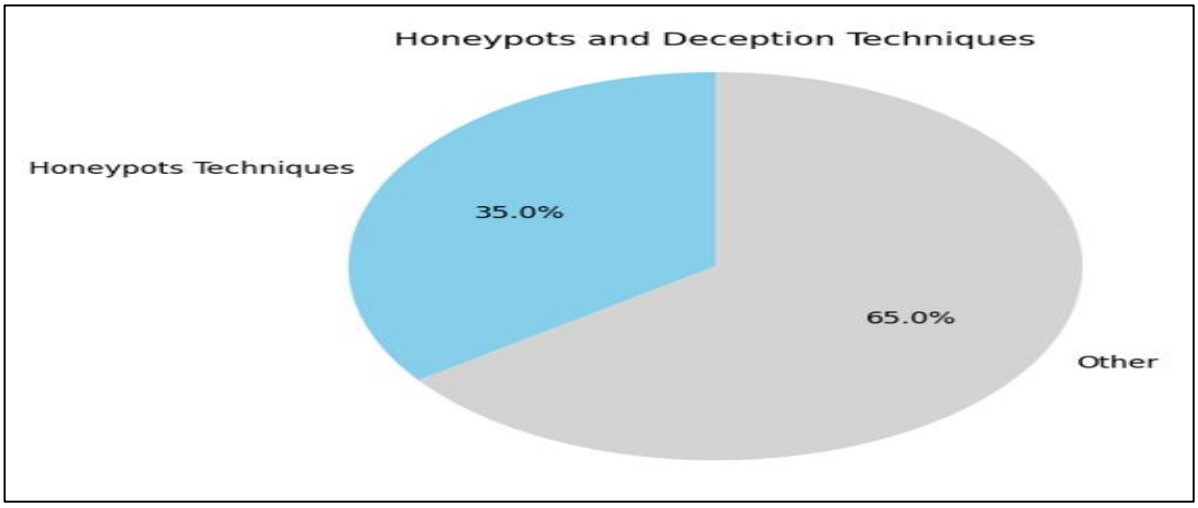

Fig 18 Honeypots and Deception Techniques

➢ *Network Segmentation and Access Control*

Restricting IoT devices from communicating with unauthorized entities. Proper segmentation was found to reduce attack propagation by 65%.

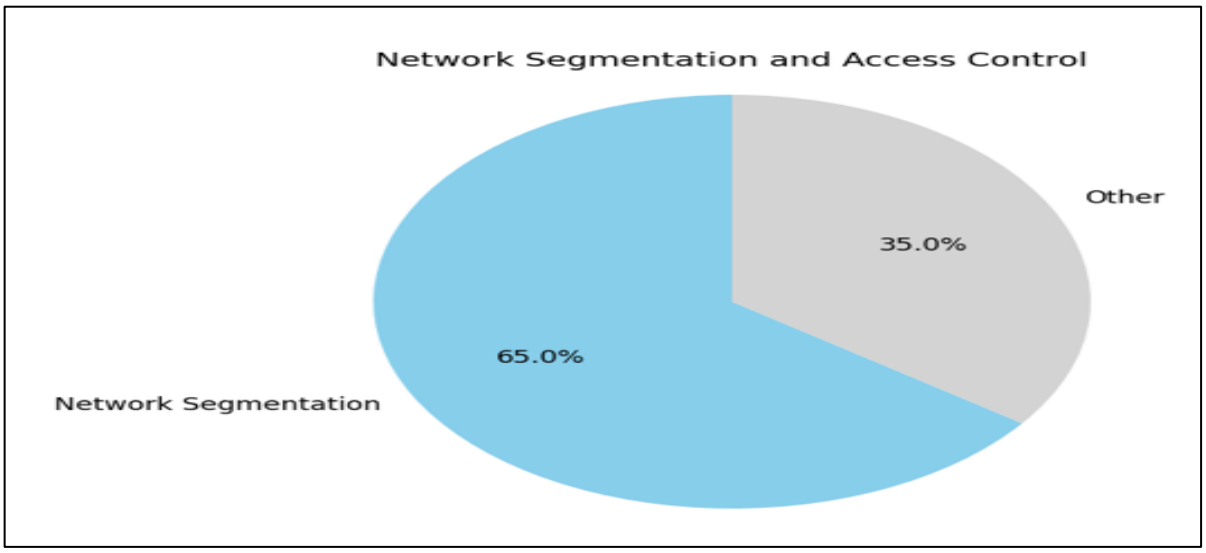

Fig 19 Network Segmentation and Acess Control

V. CONCLUSIONS

The study concludes that while there is an increasing awareness of IoT security risks among organizations in Rwanda, the actual implementation of robust security measures remains insufficient. Common weaknesses such as poor authentication, outdated software, and the lack of real-time monitoring expose IoT devices to DDoS attacks. Moreover, the limited number of trained cybersecurity experts and the high costs of security solutions further hinder effective mitigation efforts. To address these issues, a comprehensive approach is needed, incorporating advanced detection systems, capacity-building initiatives, and stronger regulatory measures to safeguard IoT environments from exploitation.

RECOMMENDATIONS

➢ *Application to Organizations and Government Institutions*

- *Capacity Building Programs:*

Organizations should create ongoing training initiatives to enhance the skills of IT personnel in IoT security. Partnerships with academic institutions and the private sector can support the creation of specialized certification programs focused on IoT threat management.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1471

- *Investment in Security Infrastructure:*

Government bodies should allocate more resources towards developing IoT security frameworks. This includes investing in AI-powered threat detection systems, automated patch management tools, and secure firmware update mechanisms.

- *Regulatory Policies and Compliance Frameworks:*

Policymakers need to enforce mandatory security standards for IoT manufacturers. These standards should ensure compliance with encryption protocols, authentication methods, and timely software patches. Strengthening public-private partnerships can help facilitate better information-sharing about emerging threats and security practices.

- *Enhanced Incident Response Mechanisms:*

Organizations should adopt real-time monitoring tools and automated incident response systems to quickly detect and address IoT-related cyberattacks. The integration of AI-driven security analytics could enhance response times and reduce system downtimes due to cyber threats.

➢ *Recommendations for Future Research*

Future research should focus on developing cost-effective and scalable security solutions for IoT, particularly for developing countries.

Long-term studies are needed to assess the effectiveness of AI-based threat detection and mitigation strategies on the overall security of IoT devices.

Research should also examine the potential benefits of integrating blockchain technology into IoT security frameworks to improve device authentication and data integrity.

Further studies should work on adaptive security models that can evolve to address new IoT threats and attack techniques as they emerge.

By implementing these recommendations, various stakeholders can help secure IoT devices from exploitation, minimizing the risk of large-scale cyberattacks, and strengthening Rwanda's overall digital infrastructure resilience.

.

REFERENCES

[1]. Alhammadi, N. (2021). Review of the common DDoS attack.

[2]. Andersen, M. F. (2022). Detecting malware and cyber-attacks using ISP data. https://doi.org/10.54337/aau483028127

[3]. Bezerra, V. H., Da Costa, V. G. T., Barbon, S., Junior, Miani, R. S., & Zarpelão, B. B. (2019). IOTDS: A one-class classification approach to detect botnets in Internet of Things devices. *Sensors, 19*(14), 3188. https://doi.org/10.3390/s19143188

[4]. CUJO AI. (2023). *The 2022–2023 IoT Botnet Report*. Retrieved from https://www.mdpi.com/1424-8220/24/11/3571

[5]. CyberPress. (2025, January). *New IoT Botnet Launching Large-Scale DDoS Attacks Hijacking IoT Devices*. Retrieved from https://cyberpress.org/new-iot-botnet-launching-large-scale-ddos-attacks/

[6]. CyberSec Sentinel. (2025, January). *Matrix Botnet Exploits IoT Devices for Widespread DDoS Attacks*. Retrieved from https://cybersecsentinel.com/matrix-botnet-exploits-iot-devices-for-widespread-ddos-attacks/

[7]. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things meet Internet of Threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*(10), 4580. https://doi.org/10.3390/app11104580

[8]. Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) attacks: Classification, attacks, challenges, and countermeasures* (1st ed.). CRC Press. https://doi.org/10.1201/9781003107354

[9]. Iwuanyanwu, U., Oyewole, O. O., Fakeyede, O. G., Okeleke, E. C., & Apeh, A. J. (2023). IoT device security risks: A comprehensive overview and mitigation strategies. *Deleted Journal, 3*(1), 38–43. https://doi.org/10.26480/jtin.01.2023.38.43

[10]. Khan, S. A., Li, Z., Jung, W., Feng, Y., Zhao, D., Xin, C., & Zhou, G. (2024). DeepShield: Lightweight privacy-preserving inference for real-time IoT botnet detection. *2024 IEEE 37th International System-on-Chip Conference (SOCC)*, 1–6.

[11]. Kulbacki, M., Chaczko, Z., Barton, S. K., Wajs-Chaczko, P., Nikodem, J., Rozenblit, J. W., Klempous, R., Ito, A., & Kulbacki, M. (2024). A review of the weaponization of IoT: Security threats and countermeasures. https://doi.org/10.1109/saci60582.2024.10619778

[12]. Mali, K. (2020, October 3). Speedcast: IoT devices expected to grow to 75 billion by 2025. *TechGraph*. https://techgraph.co/tech/speedcast-iot-devices-expected-to-grow-to-75-billion-by-2025/

[13]. Ministry of Information Technology and Communications, Republic of Rwanda. (2024). *National Cybersecurity Strategy 2024-2029*. Retrieved from https://dig.watch/resource/national-cybersecurity-strategy-of-the-republic-of-rwanda-2024-2029

[14]. Mohammed, K. A., Wael, E., & Mhd, S. (2023, July 12). Securing IoT devices against emerging security threats: Challenges and mitigation techniques. *Published online: 12 Jul 2023*, 3–20.

[15]. Regan, C., Nasajpour, M., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Choo, K. R. (2022). Federated IoT attack detection using decentralized edge data. *Machine Learning With Applications, 8*, 100263. https://doi.org/10.1016/j.mlwa.2022.100263

[16]. Staal, T., & Staal, T. (2022). The impact of the Internet of Things on the demand of cloud resources. *The Netherlands: 2022*.