Parametric Threat Analysis of IOT Related Cyberattacks

S. Deepa[1], Lakshmi Kalyani[2], V.K. Sharma[3], Vinod Kumar Chouhan[4], Savita Utreja[5]

[1] Team Lead, [2] Scientist F, [3] Scientist G, [4] Scientist E, [5] Scientist G
[1]Education & Training Division,
[1]Centre for Development of Advanced Computing, NOIDA, India
[1]deepasathya12@gmail.com, [2]lakshmikalyani@cdac.in, [3]vksharma@cdac.in, [4]vinodk@gov.in, [5]sutreja@meity.gov.in

Abstract - The world is more connected than ever and all the credit goes to the fast growth and deployment of the Internet of Things (IOT) nearly across all sectors of significance like smart home/ city, banking, industrial automation and healthcare. The rapid growth of technology has also invited a wide range of attacks on these devices endangering user safety and data privacy. There are numerous analyses on the threats to IOT devices. We have tried to classify the technical severity of some common threats encountered by the IOT devices in recent years, based on Common Vulnerability Scoring System (CVSS) parameters and the results are presented.

Index Terms - Internet of Things (IoT), IoT Vulnerabilities, CVSS, Ransomware, Botnet, Cyberattack.

I. INTRODUCTION

The IoT devices have redefined our lives in ways we would not have imagined a decade before. There are a wide range of these devices in the market and the number of connected devices increase exponentially every year. Fig. 1 shows the exponential growth of the IoT devices over time. Needless to say, they also easily fall prey to the cyberattacks, exploiting the vendors mindset to prioritize simplification over security. There are a lot of works and review papers which analyze in detail the vulnerabilities of IoT, layer wise and suggest best possible solutions [1-9]. But there is rarely a report on real life threats, put together [10,11]. There is work on single specific threat like Mirai [12-14], Silex Malware [15]. We have tried to fill in this gap by considering real attacks that have happened in the past year and analyze their severity using CVSS metrics [16].

Based on the literature survey done, we first discuss the common vulnerabilities in the IOT domain, followed by a discussion of common threats faced by the IoT devices and the most attack-prone devices. We have listed the major cyberattacks that happened related to the IoT field with a brief description of the attack. The literature survey is from credible sources like peer-reviewed journals, white papers, and threat reports of cybersecurity platforms.

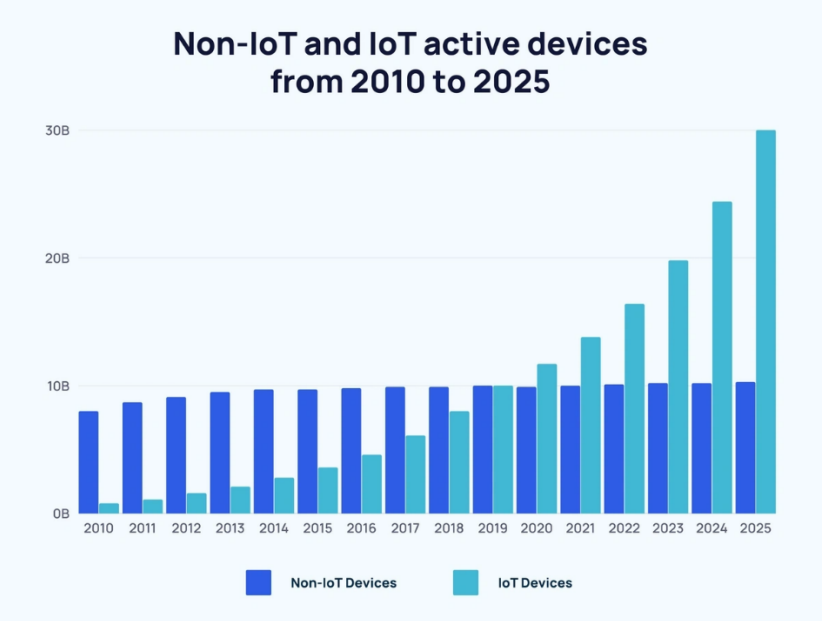

Fig.1: Graph showing the increase in the number of IoT devices [17]

1.1 Common Vulnerabilities in IoT Domain

IoT devices' limited security and processing power makes them liable to relatively simple yet devastating attacks. The Open Web Application Security Project (OWASP), is an open access non-profit forum which maintains a regularly-updated list of the most pressing web-related security concerns, and is accepted globally. According to OWASP's the latest identified 2025 list [18], the top 10 vulnerabilities based on real-world incidents, that can compromise the security of IoT devices are:

- Weak, Guessable, or Hardcoded Passwords
- Insecure Network Services
- Insecure Ecosystem Interfaces
- Lack of Secure Update Mechanism
- Using Insecure or Outdated Components
- Lack of a Proper Privacy Protection
- Insecure Data Transfer and Storage
- Absence of Device Management
- Insecure Default Settings
- Lack of Physical Hardening

These insights draw attention to the need for robust, proactive IoT security measures to address the asymmetrical risks posed by adversaries, thus safeguarding the IoT ecosystems effectively.

1.2 Common Threats in IoT Domain

The Data Security Council of India's (DSCI) Cyber Threat, in its 2025 report [19], has pointed out that imminent attacks on IoT devices, AI-powered adaptive malware and enhanced social engineering attacks will infiltrate all aspects of life, especially critical infrastructure, mobile and personal data. Some of most commonly encountered threats related to IOT domain are Botnet attack, Ransomware/ Malware attack, Distributed Denial of Service (DDoS) attack, Supply chain attack, Eavesdropping attack, Man-in-the-middle attack, Jamming, Spoofing, Data Tampering, Credential Stuffing attack, etc. Of these, the world is witnessing a multifold increase in the number of ransomware attacks and DDoS attacks every year. According to Cybercrime statistics projection, Ransomware attacks will strike every 2 seconds by 2031 [20]. Fig. 2 gives an insight on the most commonly attacked IoT devices.

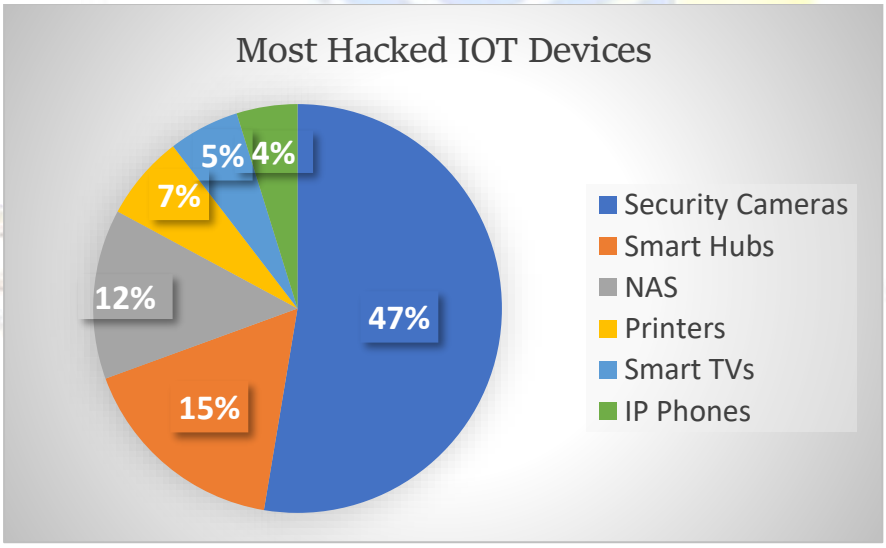

Fig.2: Most attacked IoT Devices [21]

1.3 . The important IoT related cyberattacks of 2024-2025

According to reliable statistics, the total global malware volume rose 30% in the first half of 2024. Encrypted threats were up about 92% compared to the previous year. Attacks on smart home products have increased by **124%** in 2024 [22]. The 2025 Annual Cyber Threat Report of the research firm is filed with stats on the latest vulnerabilities threatening IoT devices. The yearly reports of other well-known security firms too

reflect the same trend. Even though the reports claim a sharp increase in smart home products, there are no reports on specific incidents and the trend as a whole is only reported. Healthcare IoT devices are other attractive targets, with attacks on medical devices increasing multi fold, year over year. Table. 1, presents a list of IOT related cyberattacks that have featured and analysed in at least 3-4 cybersecurity forums. Out of these, we have analysed three incidents with the scoring metrics that we have used. Fig. 3 gives the timeline of the attacks mentioned in Table. 1.

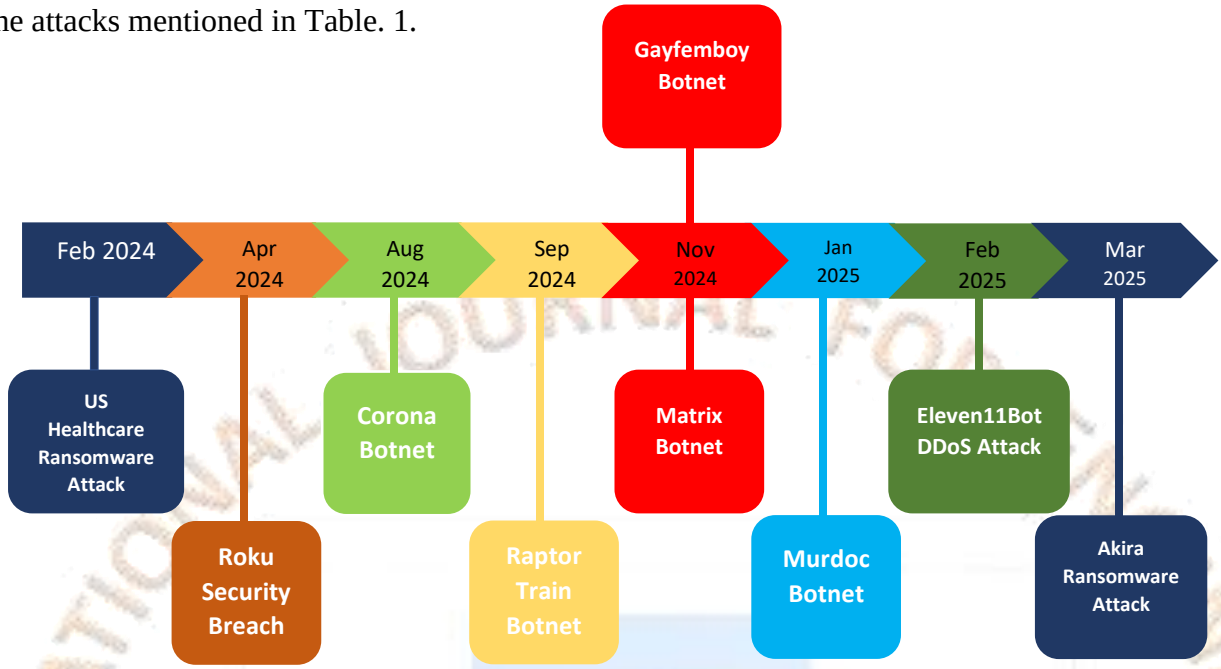

Fig.3 Timeline of the IoT related Cyberattacks

Table.1: IoT related Use cases and their brief description

S.No	Period	Threat	Description
1	**Feb 2024**	**US Healthcare IOT Ransomware Attack [23]**	ALPHV/BlackCat gained access via Microsoft's remote desktop protocol as well as brute-force attacks against Active Directory (AD); stole up to **6TB of sensitive data of about 190 million people;** non-verified ransom payment of $22 million
2	**April 2024**	**ROKU security Breach [24]**	About **576,000 Roku accounts** were compromised with hackers making unauthorized purchases on some accounts; Login credentials were stolen through "credential stuffing. Roku is a maker of smart tv and streaming devices.
3	**Aug 2024**	**AVTECH IP Cameras Exploited to spread Malware [25]**	The Corona Mirai-based malware botnet spread through a 5-year-old remote code execution (RCE) zero-day CVE-2024-7029 (CVSS v4 score: 8.7/10), in **AVTECH AVM1203 IP cameras,** targeting cameras still in service despite them having reached EoL five years ago. Despite reaching EOL, these devices are still used worldwide, by transportation authorities and other critical infrastructure entities.
4	**Sep 2024**	**Raptor Train Botnet [26]**	The Raptor Train IoT botnet operated by the **Flax Typhoon**, is one of the largest IoT botnets ever uncovered, affecting over **260,000 devices** globally, including routers, IP cameras, and NAS targeting military, government, education, and telecommunications.
5	**Nov 2024**	**Matrix Botnet Attack [27]**	Matrix using m**alwares** Mirai, PYbot, Pynet, DiscordGo, Homo Network carried out DDoS targetting IoT devices such as **IP cameras, routers, and DVRs** affecting telecom equipment; enterprise

			servers; Nearly **35 million devices** affected. **Threat Score:** High (8.5/10).
6	**Jan 2025**	**Mirai Variant Murdoc Botnet Exploits AVTECH IP Cameras and Huawei Routers [28]**	Murdoc Botnet using Mirai and Bashlite, had targeted Avtech and Huawei devices for roughly six months. According to Qualys, at least 1,300 IPs have been active as part of the campaign & the botnet's operators use more than **100 servers for command-and-control** (C&C).
7	**Feb 2025**	**Elevenbot DDoS Attack [29]**	Nearly 86000 devices turned into bots for DDOS attack. Targeted online gaming platforms. Eleven11bot is not a standalone botnet but a Mirai variant leveraging a novel exploit against HiSilicon-based IoT devices, particularly those running the TVT-NVMS9000 video management software. One of the largest botnet attacks.
8	**Mar 2025**	**Akira Ransomware attack exploited webcam to bypass EDR [30]**	After their initial attempts to deploy ransomware were thwarted by the organization's EDR system, the attackers pivoted to exploit an unsecured webcam connected to the network. By leveraging this device, they successfully launched encryption attacks, effectively circumventing the EDR protections in place. **300+ victims worldwide**.
9	**2025**	**Gayfembot Persistant DDoS Attack [31]**	Gayfembot is an improvised and persistant using UPX polymorphic packing to target Industrial cellular IoT **ASUS routers,** using N-day vulnerabilities; **Four-Faith routers**, by breaching CVE-2024-12856. **Nearly 15000+ devices added to botnets everday.**

There are ways to analyze the severity of a discovered vulnerability, to decide on the urgency to find a fix to the problem. We have attempted to find the criticality of the reported IoT related cyberattack cases. In the following section we have briefly discussed some available techniques.

II. A BRIEF ABOUT VULNERABILITY SCORING SYSTEMS

The notable techniques to assess the cyber related vulnerabilities are:

- The Common Vulnerability Scoring System (CVSS)
- Exploit Prediction Scoring System (EPSS)
- Vulnerability Priority Rating (VPR) and
- Stakeholder Specific Vulnerability Categorization (SSVC).

2.1. The Common Vulnerability Scoring System (CVSS)

The CVSS [16] serves as a standard to assess severity of the vulnerabilities to indicate which should be given priority to find a fix. It is an open framework owned and managed by FIRST.Org, Inc. FIRST is a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The Severity rating by CVSS classifies the vulnerabilities as follows:

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Table:2 Severity Ratings and corresponding CVSS

Some disadvantages of CVSS are that it provides "One-size-fits-all" solution; About 60% of all CVEs are rated 'high' or 'critical' by CVSS, which makes it difficult to decide on vulnerabilities that need an urgent fix. It typically takes 45 days for National Vulnerability Database (NVD) to publish CVSS scores following the vulnerability publication. Even though some have apprehensions on the inconsistencies of the scoring method by different entities [32-34], it still remains a widely used standard globally. Taking cue from the metrics used to find the severity of the vulnerabilities, we have tried to analyse the criticality of real-world attacks.

2.2 Exploit Prediction Scoring System (EPSS)

EPSS [35] gives an assessment of the probability that a software vulnerability will be exploited in the wild. This is based on Machine Learning classifiers and proprietary IDS alert data from Kenna Security. This makes it less transparent.

2.3 Vulnerability Priority Rating (VPR)

VPR [36] prioritizes vulnerability remediation by Tenable. VPR also uses ML models. The raw data is provided from Threat intelligence platforms, NVD, Exploit kit and frameworks. The score generated from the threat models is combined with the CVSS score and VPR is generated. VPR gives preference to vulnerabilities with publicly available exploit codes.

2.4 Stakeholder Specific Vulnerability Categorization (SSVC)

While all the above methods use CVSS in some form or the other, SSVC [37] is an alternative assessment method to CVSS. SSVC avoids numerical representations. According to SSVC, temporal and environmental considerations should be primary and not optional as in CVSS. The target audience for SSVC are incident responders like Suppliers, Deployers and Co-ordinators of patches. SSVC includes decision trees for Suppliers and Deployers, and categorizes the vulnerabilities into four response types viz. defer, scheduled, out-of-cycle, and immediate. There are different decision trees for the suppliers, deployers and co-ordinators and the outcomes are colour coded for easy identification.

Even though there are other techniques, CVSS still remains relevant and acts as a standard, as it has tried to overcome its shortcomings to some extent in its fourth version. The other techniques, however, are just viewed as ones that can supplement and support CVSS. Hence, we have tried to use CVSS V 4.0 metrics to find the severity of some IoT related cyberattacks in recent times. The method followed is detailed in the following section.

III. METHODOLOGY

The world has faced many cybersecurity threats in the year 2024 and in the first six months of 2025 (till this article was conceived). To narrow down the number of cases, we have considered only IOT device related cyber security attacks that had large scale impact. The methodology followed is schematically represented in Fig. 4. Out of the many threats, we have taken three threats as examples and shown scoring for them. The way each case is examined is given in 3.1. To analyze the severity of every case we have used CVSS metrics as given in Sec. 3.2.

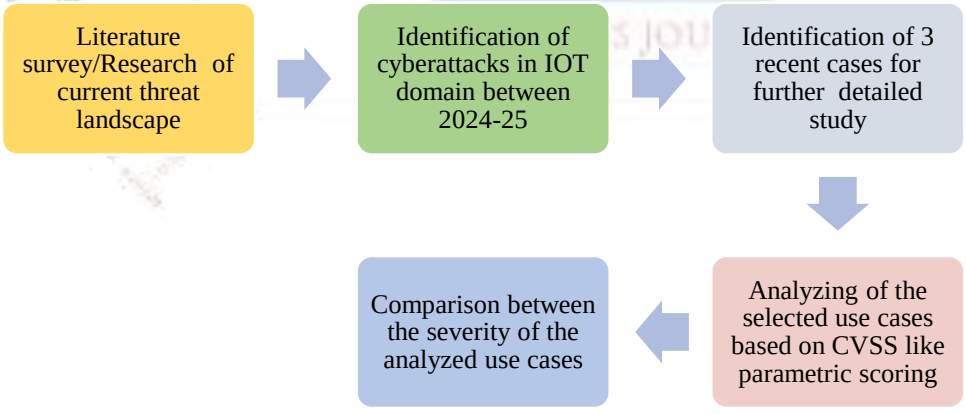

Fig. 4: Schematic representation of the Workflow

3.1 Incident or Challenge

a) **Description of the Incident**
b) **Importance of Addressing the Issue**
c) **Primary Role of IoT in the Attack**
d) **Key Vulnerabilities and Exploitation Methods**
e) **Consequences of the Attack or Issue**

3.2 Parameters to be considered for scoring:

The parameters to be examined have been derived from the metrics used for Common Vulnerability Scoring System (CVSS) version 4, which in turn plays a major role in CVE numbering. The parameters are Attack Vector (AV), Attack Complexity (AC), Attack Requirements (AT), Privileges Required (PR), User Interaction (UI), Vulnerable System Confidentiality Impact (VC), Vulnerable System Integrity Impact (VI), Vulnerable System Availability Impact (VA), Subsequent System Confidentiality Impact (SC), Subsequent System Integrity Impact (SI), Subsequent System Availability Impact (SA) and Exploit Maturity (E). The explanation to these metrics is available in detail in [16]. Also, the calculator readily available in first.org website has been used to calculate the severity score.

IV. ANALYSES OF SOME USE CASES AND DISCUSSION

Three cases have been selected from the list given in Table.1., to demonstrate the parameter-based analysis, as given in the template. They will provide clarity to the methodology suggested in this article.

4.1 Case 1: New Eleven11bot botnet infects 86,000 devices for DDoS attacks

a. Brief Description

Eleven11Bot, a new botnet threat actively spreading across the internet has managed to compromise over 86,000 devices, turning them into bots for launching DDoS attacks against targeted networks and services.

b. Importance of Addressing the Issue

Unchecked propagation of botnets like Eleven11Bot presents severe risks to internet infrastructure, business continuity, and user privacy. Addressing this threat is vital for protecting digital ecosystems, especially with the increasing dependency on cloud-based and IoT services.

c. Primary Role of IoT in the Attack

Eleven11Bot leveraged the insecure nature of many IoT devices to build a large-scale botnet. These devices often lack robust security configurations, making them easy targets for malware to exploit and enlist into a botnet army. Once infected, the devices are remotely controlled by the attacker to conduct DDoS attacks.

d. Key Vulnerabilities and Exploitation Methods

- Exploits known vulnerabilities in devices such as routers and DVRs.
- Uses **default or weak credentials** for brute-force access.
- Targets systems with **open ports and unpatched firmware**.

e. Consequences of the Attack or Issue

- High-volume DDoS attacks leading to service disruption.
- Unauthorized use of network resources.
- Potential for cascading attacks and lateral movement across systems.
- Infected devices can be used for future malware propagation.
- Potential integration into larger botnet networks for cybercrime-as-a-service.

Table 3: Parameter Based Analysis of Case:1

Metric	Value	Justification
Attack Vector (AV)	Network(N)	IoT devices are compromised remotely over the internet.
Attack Complexity (AC)	Low(L)	No complex conditions—attacker can target weak/default credentials or exposed ports.
Attack Requirement (AR)	Present(P)	Requires devices to have open ports/default config.
Privileges Required (PR)	None(N)	Attackers gain access using default/root-level without legitimate privileges.
User Interaction (UI)	None(N)	Devices are compromised autonomously; no human action required.
Vulnerable System – Confidentiality Impact (VC)	None(N)	No data theft from the IoT devices—they become bots, not vantage points for data.
Vulnerable System – Integrity Impact (VI)	High(H)	Device behaviour is modified to join the botnet.
Vulnerable System – Availability Impact (VA)	High(H)	Availability is heavily impacted—devices flood external targets.
Subsequent System – Confidentiality Impact (SC)	None(N)	No data exfiltration from other systems.
Subsequent System – Integrity Impact (SI)	None(N)	Not used to modify external systems.
Subsequent System – Availability Impact (SA)	High(H)	External service availability is disrupted via DDoS.
Exploit Maturity(E)	Attacked(A)	it **works reliably**, but it's not considered "fully automated and widespread" yet.

Score: 9 / Critical

4.2 Case 2: Ransomware gang encrypted network from a webcam to bypass EDR

a. Description of the Incident or Challenge

In March 2025, cybersecurity firm S-RM reported a novel attack vector employed by the Akira ransomware gang. After their initial attempts to deploy ransomware were thwarted by the organization's EDR system, the attackers pivoted to exploit an unsecured webcam connected to the network. By leveraging this device, they successfully launched encryption attacks, effectively circumventing the EDR protections in place. The Akira ransomware group initially gained access to the victim's network through an exposed remote access solution, likely using stolen credentials or brute-force methods. They deployed Any Desk for persistence and attempted to spread ransomware via Remote Desktop Protocol (RDP). However, their efforts were blocked by the organization's EDR system. In response, they scanned the network for vulnerable devices and identified an unsecured webcam, which they exploited to bypass the EDR and execute their ransomware payload.

b. Importance of Addressing the Issue

This incident underscores the critical need to reassess and fortify the security of all network-connected devices, not just traditional endpoints. As attackers continue to innovate, exploiting overlooked vulnerabilities in IoT

devices, organizations must adopt comprehensive security strategies that encompass every facet of their digital infrastructure.

c. Significance to IoT

In this incident, the IoT device—a poorly secured webcam—played a critical role by serving as an entry point for the Akira ransomware gang after their initial attempts were blocked by the organization's EDR system. By exploiting the webcam, which lacked proper security controls, the attackers were able to bypass traditional defenses, move laterally within the network, and successfully encrypt critical systems. This highlights how unsecured IoT devices can undermine enterprise security and be leveraged for sophisticated cyberattacks.

d. Key Vulnerabilities and Exploitation Methods

- **Exposed Remote Access Tools**: The attackers exploited an unsecured remote access solution, highlighting the risks associated with improperly secured remote management tools.
- **Unsecured IoT Devices**: The lack of security measures on the webcam allowed the attackers to use it as a conduit to bypass EDR protections.
- **Lateral Movement via RDP**: The attackers utilized RDP to move laterally within the network, seeking systems to deploy their ransomware.

e. Consequences of the Attack or Issue

By circumventing the EDR system through the webcam, the attackers successfully encrypted systems within the network. This not only disrupted operations but also posed significant data loss risks and potential financial and reputational damages due to the ransomware attack.

Table 4: Parameter Based Analysis of Case:2

Metric	Value	Justification
Attack Vector (AV)	Network(N)	IoT devices are compromised remotely over the internet.
Attack Complexity (AC)	Low(L)	No complex conditions—attacker can target weak/default credentials or exposed ports.
Attack Requirement (AR)	Present(P)	Requires devices to have open ports/default config.
Privileges Required (PR)	None(N)	Attackers gain access using default/root-level without legitimate privileges.
User Interaction (UI)	None(N)	Devices are compromised autonomously; no human action required.
Vulnerable System – Confidentiality Impact (VC)	None(N)	No data theft from the IoT devices—they become bots, not vantage points for data.
Vulnerable System – Integrity Impact (VI)	High(H)	Device behaviour is modified.
Vulnerable System – Availability Impact (VA)	High(H)	Availability is heavily impacted.
Subsequent System – Confidentiality Impact (SC)	High(H)	Data encrypted on other connected systems.
Subsequent System – Integrity Impact (SI)	High(H)	Because of possible data theft, integrity affected.
Subsequent System – Availability Impact (SA)	High(H)	Data availability compromised.
Exploit Maturity(E)	Attacked(A)	It **works reliably**, but it’s not considered "fully automated and widespread" yet.

Score: 9.2 / Critical

4.3 Case 3: Gayfembot Botnet Attack

a. Brief Description

Gayfemboy botnet has evolved into a formidable cyber threat with advanced exploitation capabilities. Originally identified as a derivative of the Mirai botnet, it began as a series of malware samples packed with UPX(bypass to signature based internet security eg: Anti-virus). Over time, its developers continuously refined its architecture, experimenting with techniques like UPX polymorphic packing, modifying registration packets, and incorporating 0-day exploits.

b. Importance of Addressing the Issue

This type is dynamic and improvises with time. The attacker can modify the router's configuration files, discover other devices in the network, and further enhance the attack. It is found to be aggressive and retaliatory.

c. Primary Role of IoT in the Attack

The compromised bots added to the botnet in the form of routers exhibiting known vulnerabilities were then utilized for persistent DDoS attacks.

d. **Key vulnerabilities and exploitation methods:**

Industrial cellular IoT Routers; ASUS routers, using N-day vulnerabilities; Four-Faith routers, by breaching CVE-2024-12856.

Exploitation Method:

Target Scanning: The attacker scans the internet for Four-Faith routers with default credentials (like admin/admin) exposed to the internet.

Authentication Bypass & Exploit HTTP Post: The attacker sends a crafted request to /apply.cgi endpoint with payload: adj_time_year=1;sh shellcode.sh; (CGI: Common Gateway Interface)

Command Injection: This command gets injected into the router's OS shell (Linux-based), allowing remote code execution.

Reverse Shell: The router now initiates a connection to the attacker's server, giving full control to the attacker.

Joins Botnet: The compromised router becomes part of the botnet army and can now launch DDoS or spread malware.

Persistence: Scripts are placed in start-up routines to survive reboots and ensure long-term access

e. Consequences of the attack

Nearly 15000+ routers were added to the botnet every day, targeting China, United States, Russia, Turkey, Iran, Germany, United Kingdom, and Singapore; Telecoms and Govt organizations targeted.

Table 5: Parameter Based Analysis of Case:3

Metric	Metric	Justification
Attack Vector (AV)	Network(N)	Attack occurred over the internet via /apply.cgi
Attack Complexity (AC)	Low(L)	No authentication or complex chaining required.
Attack Requirement (AR)	None(N)	No external conditions were necessary to exploit the vulnerability — it was straightforward, automated, and scalable (over 15,000 devices).
Privileges Required (PR)	None(N)	No credentials needed to launch exploit.
User Interaction (UI)	None(N)	No user action was required.
Vulnerable System – Confidentiality Impact (VC)	Low(L)	No sensitive data stolen from router, but visibility into basic config possible.
Vulnerable System – Integrity Impact (VI)	Low(L)	Configuration or firmware altered (e.g., injected botnet code).
Vulnerable System – Availability Impact (VA)	High(H)	Router taken over, service interrupted or added to DDoS pool.

Subsequent System – Confidentiality Impact (SC)	None(N)	Botnet did not exfiltrate data from downstream systems.
Subsequent System – Integrity Impact (SI)	None(N)	No downstream data alteration by router observed.
Subsequent System – Availability Impact (SA)	High (H)	Possible downstream disruption in case of DDoS amplification.
Exploit Maturity(E)	Attacked	it **works reliably**, but it's not considered "fully automated and widespread" yet.

Score: 9.2/Critical

4.4 Inferences from the study

We have considered a DDoS attack, a persistent DDoS attack and a ransomware case for detailed analysis. The statistics of the last year shows that the DDoS attacks and Ransomware attacks are the most prominent in the IoT arena. Of the nine cases listed, 6 are DDoS attacks, 2 are Ransomware attacks and 1 is a Credential Stuffing case. Ransomware attacks are a menace in IIOT, but there is no extensive report on them. Table 6 gives the inferences in a crisp form.

Table 6: Scores and preventive measures of the cases considered

S.No.	Use Case	Score/ Severity	Suggestive preventive measures
1	**Eleven11bot DDoS Attack**	9 / Critical	Conduct network-wide surveys to identify commonly targeted IoT devices (like routers, DVRs, IP cameras) with open ports, default credentials, or unpatched firmware; **Update Firmware; Change Default Credentials;** Segment vulnerable devices into isolated VLANs with **outbound internet access restrictions;** Turn off remote access features and close unused ports, such as Telnet and SSH, to reduce potential attack vectors; **Monitor Network Traffic f**or unusual patterns that may indicate a compromised device.
2	**Akira Ransomware Attack**	9.2 / Critical	Enforce real-time micro-segmentation where each IoT device has a policy-defined communication boundary; Conduct periodic security assessments of all connected devices; Implement strict access controls and monitor for unauthorized access attempts; Ensure Anomaly detection; Enable timestamped logs stored remotely
3	**Gayfemboy Persistent DDOS Attack**	9.2/ Critical	Regularly update routers and IoT device firmware to the latest version; Immediately change default usernames and passwords on devices. Every device should have unique and strong passwords; Use complex passwords and enable two-factor

			authentication (2FA) wherever possible; Disable HTTP, Telnet, FTP, or other unnecessary services on routers; Organizations must have a proper incident response plan in case devices are compromised; Push for global standards on IoT device security.

V. CONCLUSION

In this article, we have made an attempt to present the threatening attacks over the past year in the field of IoT. The existing vulnerability rating techniques have been briefed and the CVSS metrics template has been used for analysis. Three cases have been chosen as examples to analyze their criticality. Each case has been analyzed in detail and results are presented. This will serve as an awareness to the various types of threats faced in the IOT domain and help to identify the most common and impactful threats to the domain. Also, based on these studies, best practices to avert these attacks have also been suggested.

VI. REFERENCES

[1] Tageldin, Laila. "Internet of Things Security: Threats, recent trends, and mitigation approaches." *Advances in Internet of Things*, 2025, pp. 1-15.

[2] Imtiaz, Nouman, Wahid, Abdul, Abideen, Syed Zain Ul, Kamal, Mian Muhammad, Sehito, Nabila, Khan, Salahuddin, Virdee, Bal Singh, Kouhalvandi, Lida and Alibakhshikenari, Mohammad, "A deep learning-based approach for the detection of various Internet of Things intrusion attacks through optical networks." *Photonics*, *MDPI*, 2025, pp. 1-39.

[3] Tehseen Mazhar, Sunawar khan, Tariq Shahzad, Muhammad Amir khan, Mamoon M. Saeed, Joseph Bamidele Awotunde & Habib Hamam, "Generative AI, IoT, and blockchain in healthcare: application, issues, and solutions." *Discover Internet of Things*, 5:5, 2025.

[4] Tariq Emad Ali, Faten Imad Ali, Pavle Dakić & Alwahab Dhulfiqar Zoltan, "Trends, prospects, challenges, and security in the healthcare internet of things." *Computing* 107.1, 2025, 28.

[5] T. Magara, and Y. Zhou. "Internet of things (IoT) of smart homes: privacy and security." *Journal of Electrical and Computer Engineering* 2024.1, 2024, 7716956.

[6] A. H. Eyeleko, and T. Feng. "A critical overview of industrial internet of things security and privacy issues using a layer-based hacking scenario." *IEEE Internet of Things Journal* 10.24, 2023, pp. 21917-21941.

[7] G. Vardakis, G. Hatzivasilis, E. Koutsaki and N. Papadakis, "Review of Smart-Home Security Using the Internet of Things." *Electronics* 13.16, 2024, 3343.

[8] H. Sebestyen, D. E. Popescu, R.D. Zmaranda. "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories." *Computers* 14.2, 2025, 61.

[9] N.N. Thilakarathne, M.S.A. Bakar, P. E. Abas, H. Yassin, "Internet of things enabled smart agriculture: Current status, latest advancements, challenges and countermeasures." *Heliyon* 11.3, 2025.

[10 B. Paul, A. Sarker, S.H. Abhi, S.K. Das, M.F. Ali, M.M. Islam, M.R. Islam, S.I. Moyeen, M.F.R. Badal, M.H. Ahamed, and S.K. Sarker, "Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies." *Heliyon* 10.19, 2024.

[11] O.I. Falowo, and J. B. Abdo. "2019–2023 in review: Projecting DDoS threats with ARIMA and ETS forecasting techniques." *IEEE Access* 12, 2024, pp. 26759-26772.

[12] J. Margolis, T.T. Oh, S. Jadhav, Y.H. Kim and J.N. Kim, "An in-depth analysis of the mirai botnet." *2017 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2017.

[13] X. Zhang, O. Upton, N.L. Beebe and K.K.R. Choo, "Iot botnet forensics: A comprehensive digital forensic case study on mirai botnet servers." *Forensic Science International: Digital Investigation* 32, 2020, 300926.

[14] A. Affinito, S. Zinno, G. Stanco, A. Botta, G. Ventre, "The evolution of Mirai botnet scans over a six-year period." *Journal of Information Security and Applications* 79, 2023, 103629.

[15] B.I. Mukhtar, M.S. Elsayed, A.D. Jurcut, M.A. Azer, "IoT vulnerabilities and attacks: SILEX malware case study." *Symmetry* 15.11, 2023, 1978.

[16] CVSS v4.0 Specification Document

[17] 60+ Amazing IoT Statistics (2024-2030)

[18] OWASP IoT Top 10 Vulnerabilities (2025Updated) | Wattlecorp Cybersecurity Labs

[19] **https://www.seqrite.com/india-cyber-threat-report-2025/**

[20] https:/cybersecurityventures.com/Ransomware- Will- Strike- Every -2 -Seconds- By- 2031

[21] https://devopedia.org/iot-security

[22] 2025 SonicWall Cyber Threat Report: The Need For Speed and Strong Allies to Overcome the Cybersecurity Battlefield

[23] 190 Million Individuals Affected by Change Healthcare Data Breach - The HIPAA Guide

[24] Roku security breach: 576,000 accounts affected by cyberattack, company says | CNN Business

[25] Malware exploits 5-year-old zero-day to infect end-of-life IP cameras

[26] Raptor Train Chinese Botnet Compromises 200K+ Devices | Cyber News

[27] Matrix Botnet Exploits IoT Devices for Widespread DDoS Attacks

[28] Murdoc Botnet Ensnaring Avtech, Huawei Devices - SecurityWeek

[29] https://www.bleepingcomputer.com/news/security/new-eleven11bot-botnet-infects-86-000-devices-for-ddos-attacks/

[30]https://www.cyberdaily.au/security/11811-watch-this-unsecured-webcam-used-in-recent-ransomware-attack
[31] https://iottechnews.com/news/gayfemboy-breaks-mirai-botnet-trend-persistent-threat/
[32] M. Aggarwal, "A study of CVSS v4. 0: A CVE scoring system." *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, Vol. 6. IEEE, 2023.
[33] L. Miranda, L. Senos, D. Menasché, G. Srivastava, A. Kocheturov, E. Lovat, A. Ramchandran, and T. Limmer, "A Product-Oriented Assessment of Vulnerability Severity Through NVD CVSS Scores." *2025 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2025.
[34] J. Wunder, A. Kurtz, C. Eichenmüller, F. Gassmann, Z. Benenson, "Shedding light on CVSS scoring inconsistencies: A user-centric study on evaluating widespread security vulnerabilities." *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024.
[35] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, M. Roytman, "Exploit prediction scoring system (EPSS)." *Digital Threats: Research and Practice* 2.3 (2021): 1-17.
[36] https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss
[37] J.M. Spring, E. Hatleback, A. Householder, A. Manion, D. Shick, "Prioritizing vulnerability response: A stakeholder-specific vulnerability categorization (version 2.0)", *Technical Report. Carnegie-Mellon University, Pittsburgh PA*, 2021.

INTERNATIONAL JOURNAL FOR ENGINEERING TECHNIX RESEARCH
TIJER
OPEN ACCESS JOURNAL