



Module Code & Module Title

CC7178NI Cyber Security Management

50% Individual Coursework

“Cyber-attacks from black hat hackers on IoT devices”

Year

2025 Spring Sem 1

Student Name: Abhiyan Shrestha

London Met ID: **24059497**

College ID: **np01ms7s250025**

Assignment Due Date: **April 29, 2025**

Assignment Submission Date: **May 4, 2025**

Word Count: **4399**

I confirm that I understand my coursework needs to be submitted online via My Second Teacher under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Turnitin Report

Cyber attacks from black hat hackers on IoT devices by Abhiyan Shrestha Final Version Turnitin.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid::3618:91511826

Submission Date

Apr 16, 2025, 3:47 PM GMT+5:45

Download Date

Apr 16, 2025, 3:49 PM GMT+5:45

File Name

Cyber attacks from black hat hackers on IoT devices by Abhiyan Shrestha Final Version Turnitin.docx

File Size

22.3 KB

26 Pages


3,475 Words

19,056 Characters



Page 1 of 29 - Cover Page

Submission ID trn:oid::3618:91511826



Page 2 of 29 - Integrity Overview

Submission ID trn:oid::3618:91511826

0% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

0

Not Cited or Quoted 0%

Matches with neither in-text citation nor quotation marks

1

Missing Quotations 0%

Matches that are still very similar to source material

0

Missing Citation 0%

Matches that have quotation marks, but no in-text citation

0

Cited and Quoted 0%

Matches with in-text citation present, but no quotation marks

Top Sources

0%

Internet sources

0%

Publications

0%


Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.



Page 3 of 29 - Integrity Overview

Submission ID trn:oid::3618:91511826

Match Groups

0

Not Cited or Quoted 0%

Matches with neither in-text citation nor quotation marks

1

Missing Quotations 0%

Matches that are still very similar to source material

0

Missing Citation 0%

Matches that have quotation marks, but no in-text citation

0

Cited and Quoted 0%

Matches with in-text citation present, but no quotation marks

Top Sources

0%

Internet sources

0%

Publications

0%

Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1

Submitted works

Southern New Hampshire University - Continuing Education on 2022-10-22

<1%

3

Abstraction

The rapid expansion of Internet of Things (IoT) devices, with the promise of increased automation and data-driven productivity in sectors like healthcare and manufacturing, has simultaneously boosted cybersecurity threats from malicious actors, referred to as "black hat hackers." This report analyzes the vulnerabilities present in most IoT devices due to weak security practices, default passwords, lack of standardization, and inadequate update systems. These weaknesses open extremely deep points of entry for cyberattacks, ranging from loss of data and business disruption to potential physical damage, as exemplified in real-world instances with compromised robot cleaners and car control systems.

The literature review emphasizes the increasing risk of such attacks, employing robust countermeasures like deep encryption, regular firmware updates, and AI-driven intrusion detection systems. Emerging trends like honeypot building and machine learning usage are good directions for anticipatory defense. Important case studies, such as Zoho ManageEngine vulnerability exploitation and the Stuxnet cyber weapon against Iran's nuclear program, starkly delineate the potential for high impact, from data exfiltration to physical destruction. The report concludes by highlighting the urgent need for a paradigm shift in IoT security, suggesting the adoption of robust security features by design, industry-wide standardization, timely and open software updates, and enhanced user awareness to safeguard connected systems and critical infrastructure from continued cyber threats.

Table of Contents

• Abstraction.....	4
• Introduction.....	6
○ Problem Definition	
▪ Inadequate Security Features	
▪ Default Credentials	
▪ Lack of Standardization	
▪ Limited Update Mechanisms	
○ Current Scenario	
▪ Cyber Threats and Attack Vectors in IoT Devices	
▪ Case Studies Highlighting IoT Vulnerabilities	
▪ Countermeasures and Risk Mitigation Strategies	
▪ Emerging Trends and Future Directions	
▪ Conclusion	
• Literature Review.....	15
• Critical Analysis.....	23
○ Case Study 1: Impact and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization.	
▪ Background	
▪ Issue Identification	
▪ Mitigation	
▪ Summary	
○ Case Study 2: An Unprecedented Look at Stuxnet, the World's First Digital Weapon.	
▪ Background	
▪ Issue Identification	
▪ Mitigation	
▪ Summary	
• Conclusion.....	28
• References.....	.29

Introduction

Internet of Things (Alexander S. Gillis, 2023) means a connection of many network of devices that is physical which ranges from appliances for household to machinery for industrial purposes with its parts like software, sensors and many other technologies that enables for connections to exchange the data in the internet. Moreover, (IBM, n.d.) the interconnections that gives facility to connect between the systems and devices that is leading and making an enhancement in automation, efficient and driven by data decision which is helping in the various sectors. Lets suppose heathcare Internet of Things devices that is a wearable tracker for fitness which can monitor an health metrics of patient in a real time. Moreover, sensors for agriculture soil conditions checking that can help in more proper strategies in irrigation process for people. The use of Internet of Things devices made an big revolution in industries by giving and providing the unimaginable controls of level and insight into operations.

Now the fast growth and expansion of Internet of Things device technology also increased an risk of significant challenges for cybersecurity. Hackers that is called Black hat hackers (Nancholas, 2024) is a individual that exploit systems of computer (SANGFOR, n.d.) and use of networks for malicious intention which is an big threat for the Internet of Things devices. Hackers that is called (KASPERSKY, n.d.) white hat hackers is a individual that works in an ethical hacking environment legally for identifying and solving the problem of security vulnerabilities where as black hat hackers attack the systems for motives like sensitive data stealing, services disruption, or can even do any other kind of harms. Internet of Things devices have limited power for processing and security features that is minimal that is causing the attacks for cyber crimes.

Especially, Internet of Things (IDB, 2025) integrations in the infrastructures that is critical like systems for transportations, energy grids and even healthcare sectors can cause an potential damage or impacts of cyber crime or attacks. The devices that is once compromised can be a big loop hole for hackers which can help the black hat hackers for accessing a big networks, data breaches can happen, disruptions of operations and can even make an physical damage. Let's set an example like suppose an black hat hackers gains controls on interconnected devices of medical sectors equipment they can do things like device manipulations of its functions, even risk for the patient health and safety. Moreover, the access of unauthorized person to the industrial Internet of Things devices can lead to the results in changing of manufacturing process and can even close or shutdown the services that is essential.

Moreover, there is (Alexander S. Gillis, 2023) a lot of different types of IoT devices which is causing an complicated path for security measures. A lot of Internet of Things devices (IBM, n.d.) is designed with main focus in effective cost cutting and (Nancholas, 2024) functionality without focusing on security systems that is robust. Even the use of password that is default (SANGFOR, n.d.) and no regular updates on software which is an open ground for the cyber attacks. Internet of Things devices is growing rapidly as security issues (KASPERSKY, n.d.) and challenges is becoming more dangerous and critical for protecting our data that is sensitive and maintaining the integrity of the interconnected systems.

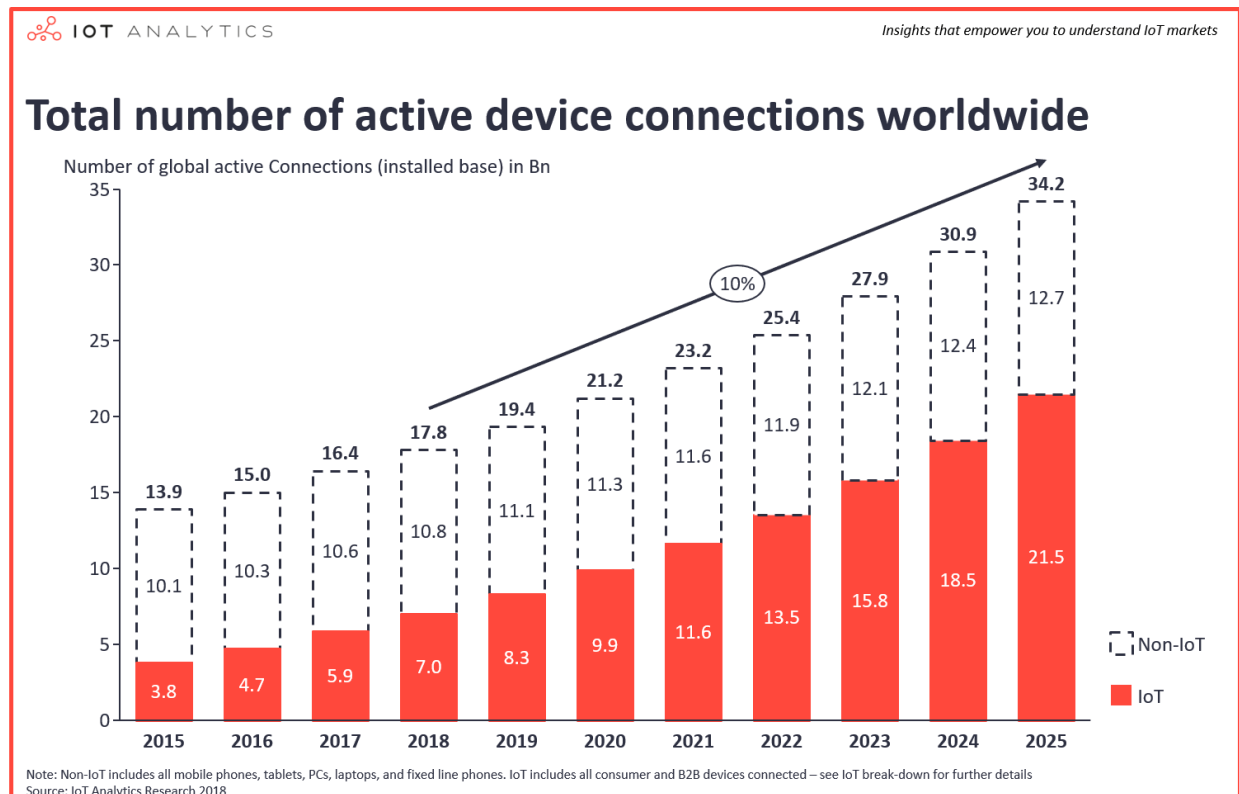


Fig: Total Number of Active IoT devices And Non IoT devices (Lueth, 2018)

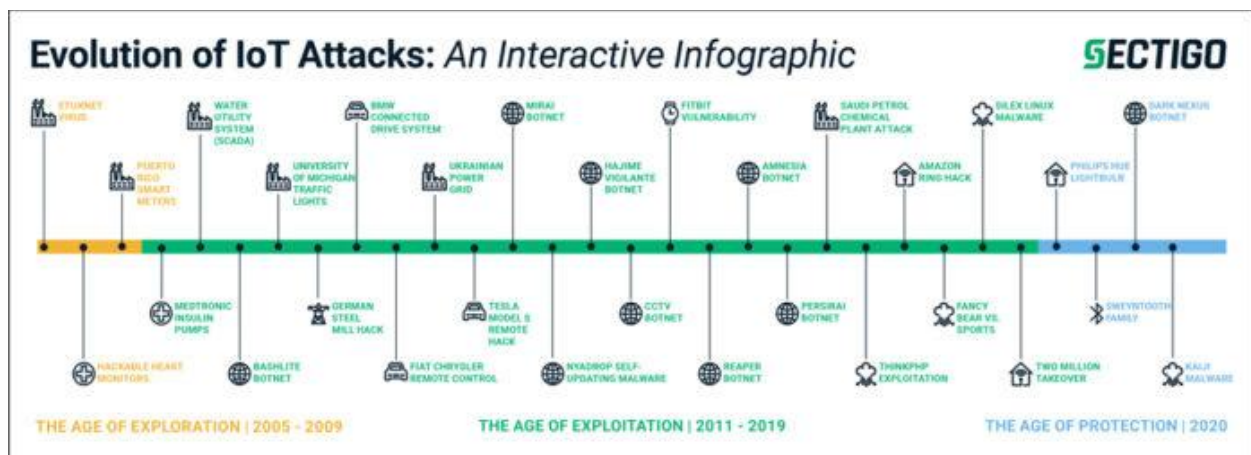


Fig: Evolution of IoT Devices Attacks (SECURITY, 2020)



Fig: Top Ten Security Targets on IoT devices (Buntz, 2016)

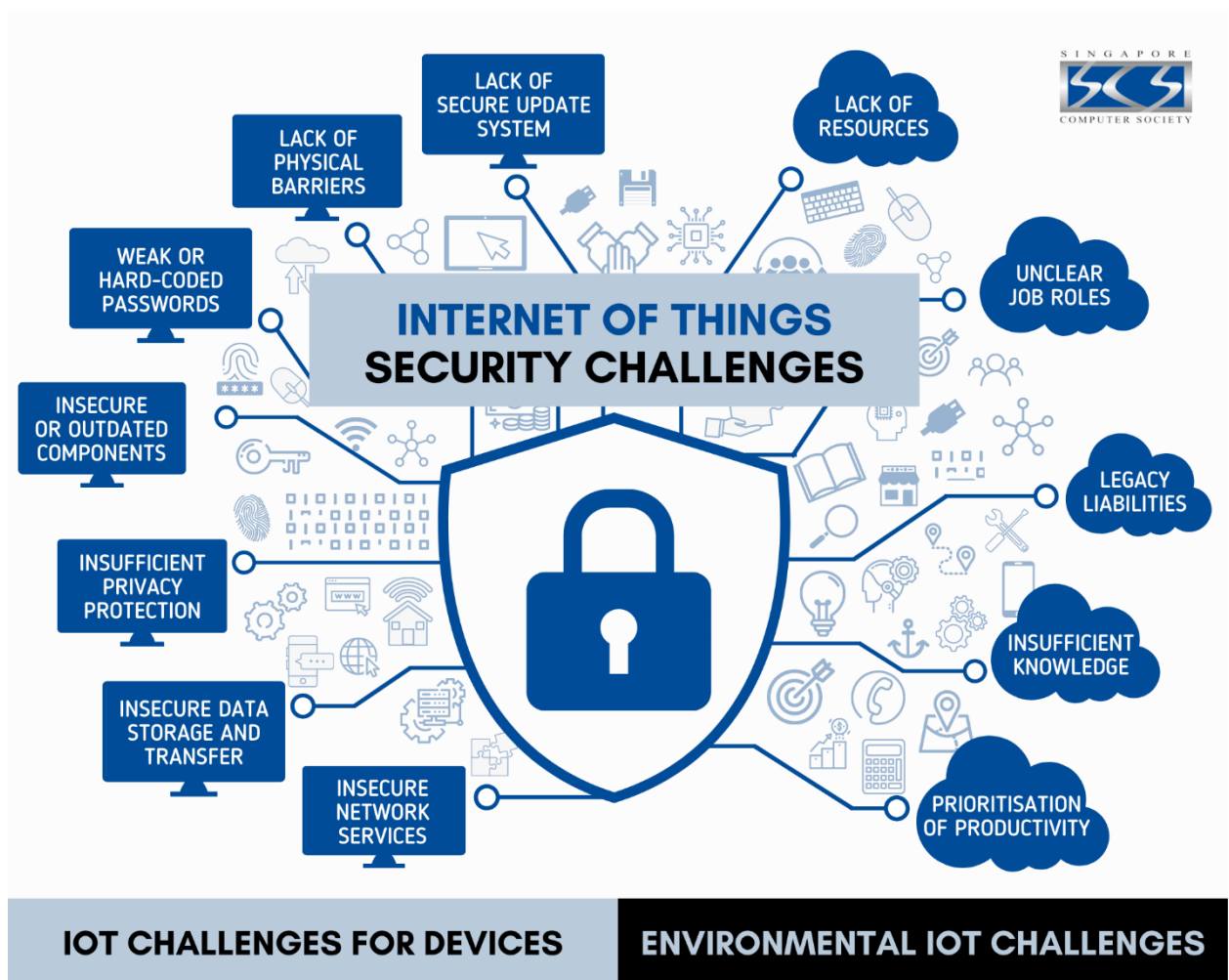


Fig: IoT devices Security Challenges (SOCIETY, 2021)

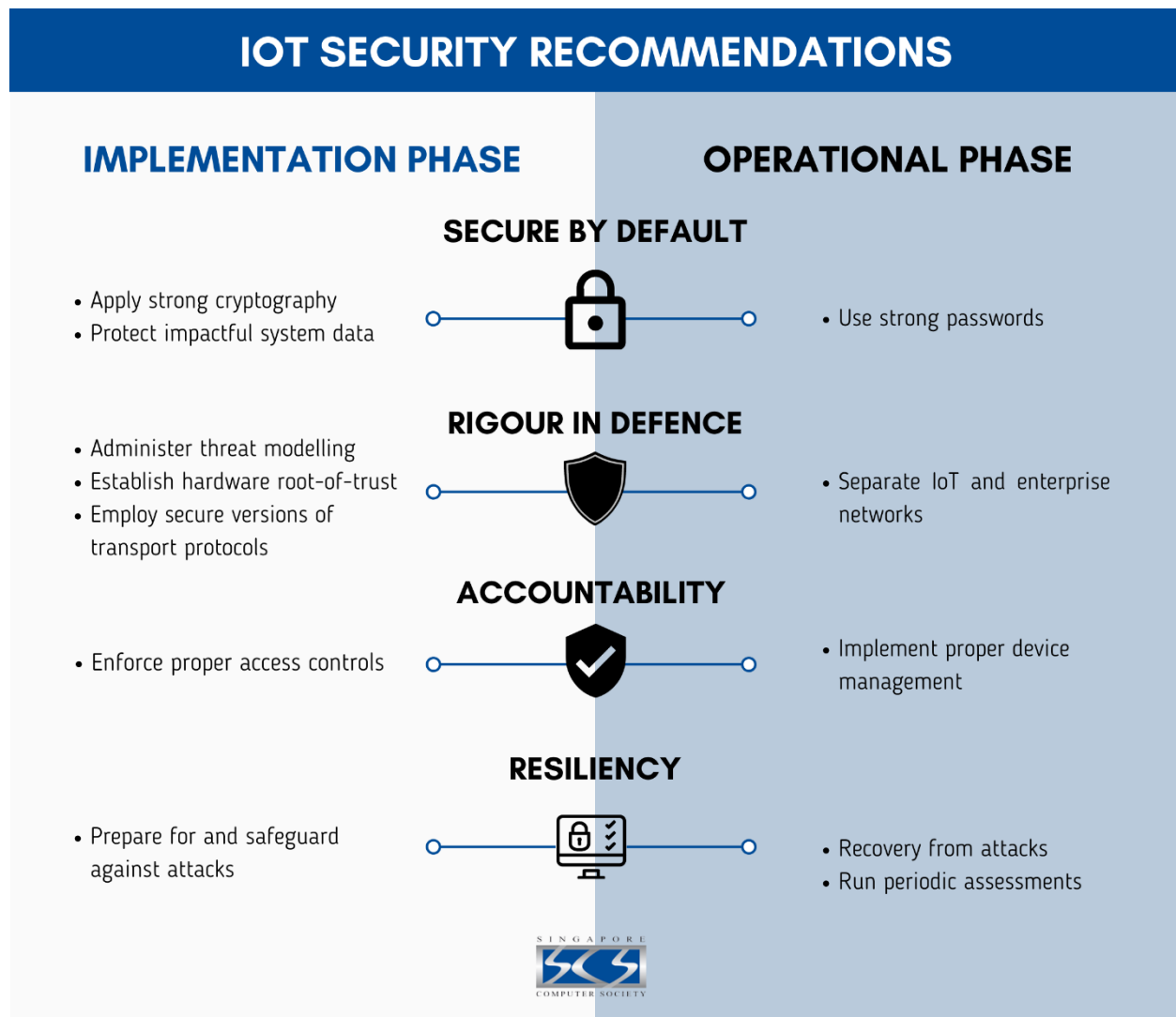


Fig: IoT devices Security Recommendations (SOCIETY, 2021)

a. Problem Definition

Issues that is core lies in the weak point or vulnerability of Internet of Things devices by cyber attacks which is caused by black hat hackers. Internet of Things devices always run with very less measures of security which is attracting hackers for doing malicious things and trying to gain access that is unauthorized in any ways either data or networks. These kind of the problems is rising by the following factors:

- **Inadequate Security Features:** Nowadays many Internet of Things devices lack the basic security measures like authentication that is secure and encryptions that is strong which leaves an big loop hole in the vulnerability and can be exploited by hackers.
- **Default Credentials:** Manufactures are using an usernames and passwords that is default which is also left default by the users that gives an point of entry for black hat hackers.
- **Lack of Standardization:** Even there is big absence of no standards for security protocol to follow for the Internet of Things devices which is causing an protections inconsistent that can make it more hard to secure the networks properly.
- **Limited Update Mechanisms:** One of the main problem faced by peoples or users is there is no support for regular updates on software and firmware knowing the weak point of the devices and leaving it weak for long time.

b. Current Scenario

Internet of Things devices security is facing an rise of cyber attacks which is also called DDoS attacks that is from black hat hackers for exploiting the weak point as seen in the Mirai botnets. Producers of the Internet of Things manufactures are trying to improve their security and policies but a lot of development in IoT devices has made an complex for security standardization process. Working as group can only fix this kind of issues.



Fig: DDoS Attack Evolutions (Andrew Shoemaker, 2024)



Fig: IoT Devices Cyber Attacks Average (KRATIKAL, 2021)

Literature Review

IoT devices (Praveen Pawar, 2018) made life of the peoples easy and even transformed many sectors like smart homes, industrial operations and even healthcare. Moreover, speedy expansion of the IoT devices has caused an challenges on cybersecurity which are exploited by the black hat hackers using there weak point or vulnerabilities for malicious purposes. The literature review shows research on recent threats that is being targeted by black hat hackers on Internet of Things devices and technique used by the hackers and its counter measures for mitigating the potential risks.

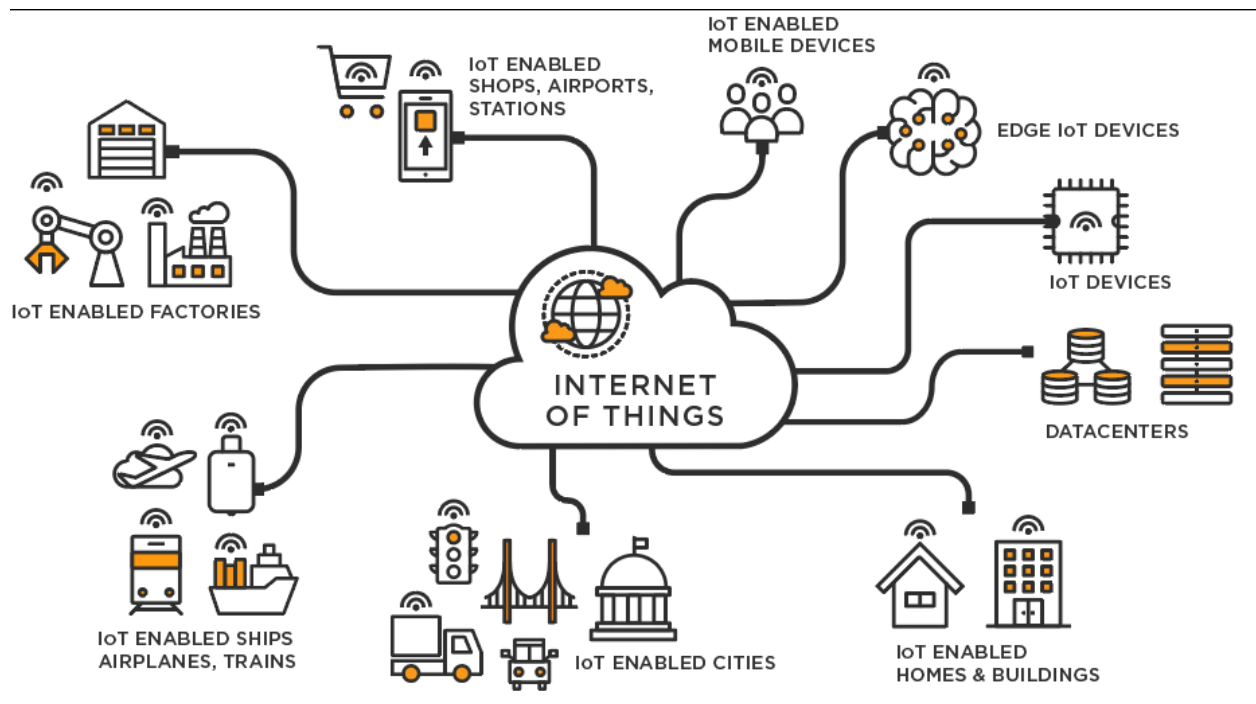


Fig: How IoT devices Makes Life Easier (Sehgal, 2022)

a) Cyber Threats and Attack Vectors in IoT Devices

Internet of Things devices (Konstantinos Tsiknas, 2021) are always operating with less features of security which makes the attackers get attracted with it and hackers attack and exploit them. (Usha Devi Gandhi, 2018) also introduced HloTPOT, a honeypot designed to monitor IoT devices and analyze contemporary threats. This study highlights Telnet attacks that the hackers exploit weak and default usernames and passwords credentials for gaining the unauthorized access. Moreover, this research also focuses on the how the attacks attack for developing the defense mechanisms that is effective and works perfectly.

Especially, sectors like industrial areas (Konstantinos Tsiknas, 2021) also use the Internet of Things devices which makes the work of the industries operation smooth but can cause an cybersecurity challenges. Even an journal (Praveen Pawar, 2018) was published with the name of “Journal of Cyber Security Technology” gives an best study survey of threats that is related to Industrial Internet of Things which is making attacks category into groups like denial of service, man in the middle and malware attacks. Research who wrote the journal told why it is important to bring an authentication system that is robust and even a intrusion detection systems for protecting the operations of the industrial works flow smoothly.

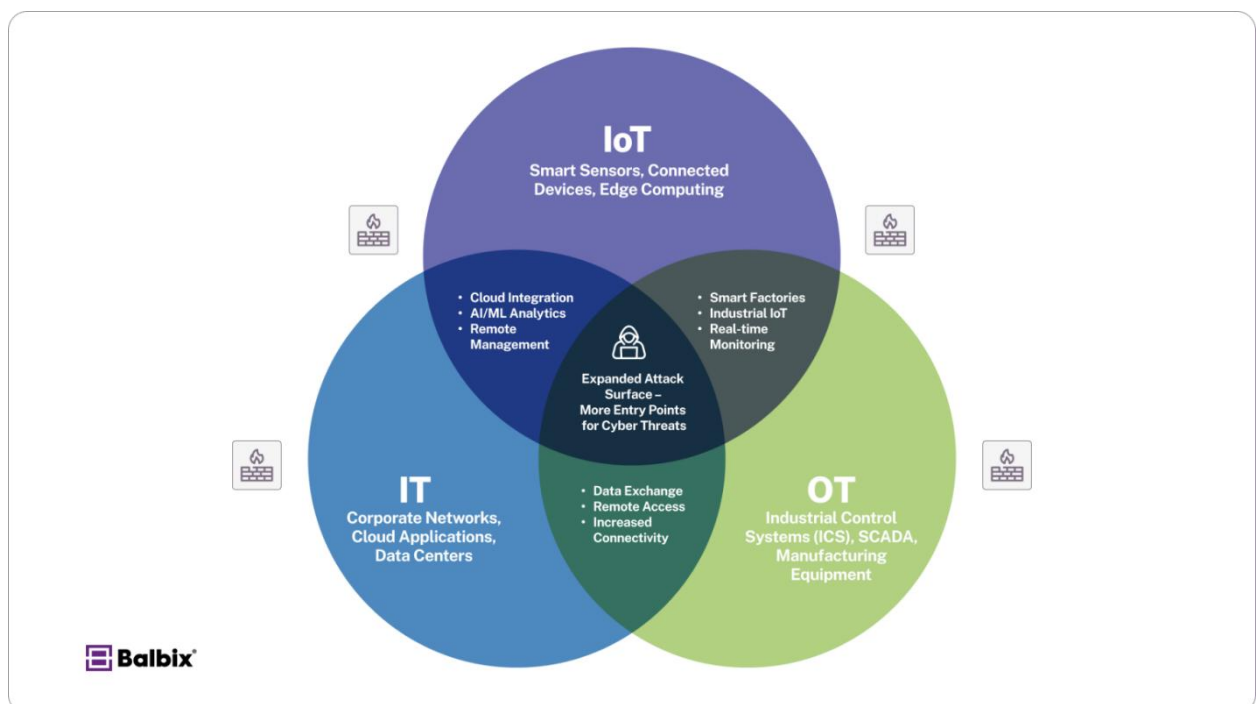


Fig: IoT Cyber Threats (Balbix, 2025)

b) Case Studies Highlighting IoT Vulnerabilities

Risk that is associated with IoT devices (Mohammed Aziz Al Kabir, 2023) in real world scenario. Article written in The Verge reported that on hackers are taking controls over an robot vacuum, for trying to chase away the pets and offensive attack at the owners. This kind of security breach are highlights the ways how hackers can compromise the Internet of Things devices and causes the harm to the users.

Especially, showing the detailed security flaws (Manos Antonakakis, et al., n.d.) in the Kia's web portal that allowed the hackers for gaining an remote access to control the features in vehicles like door unlocking and can even start the engine of the vehicles. These kind of vulnerabilities done by black hat hackers exposed in millions number from getting theft and even an unauthorized access plus demanding an need of the robust systems security measures for an connected vehicles.

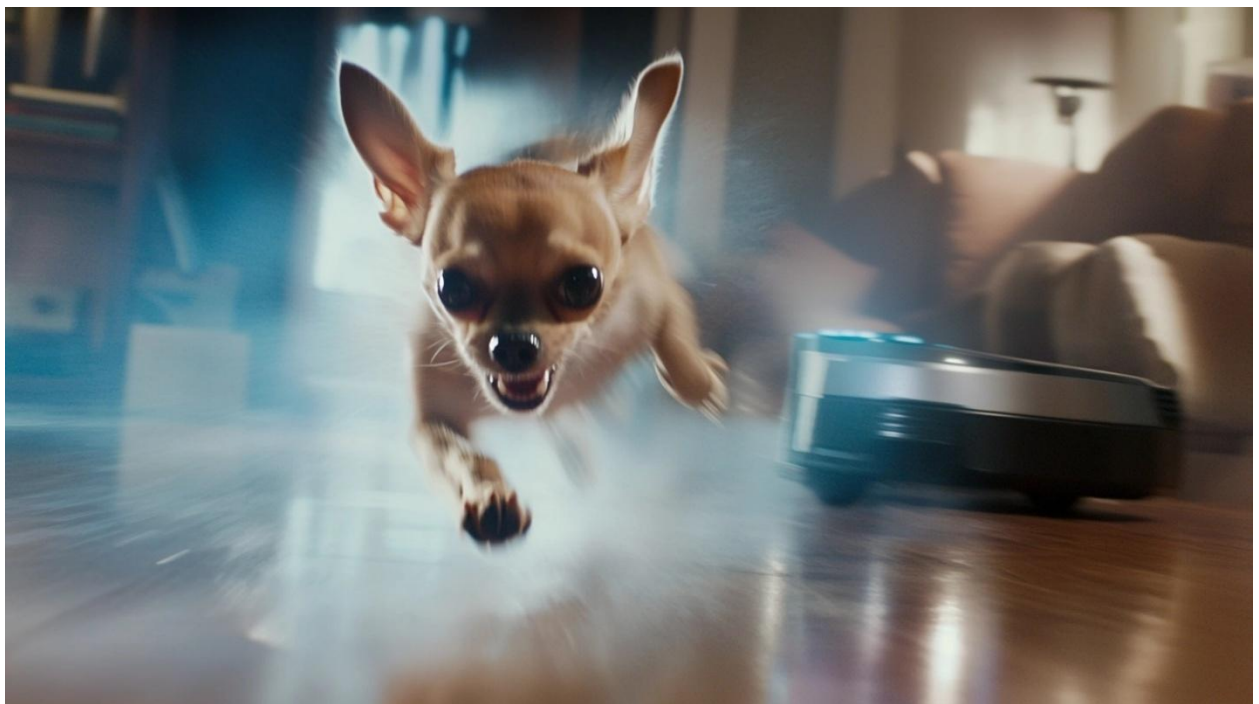


Fig: Robot Vacuum Attacking Pets (KasperskyOs, 2025)

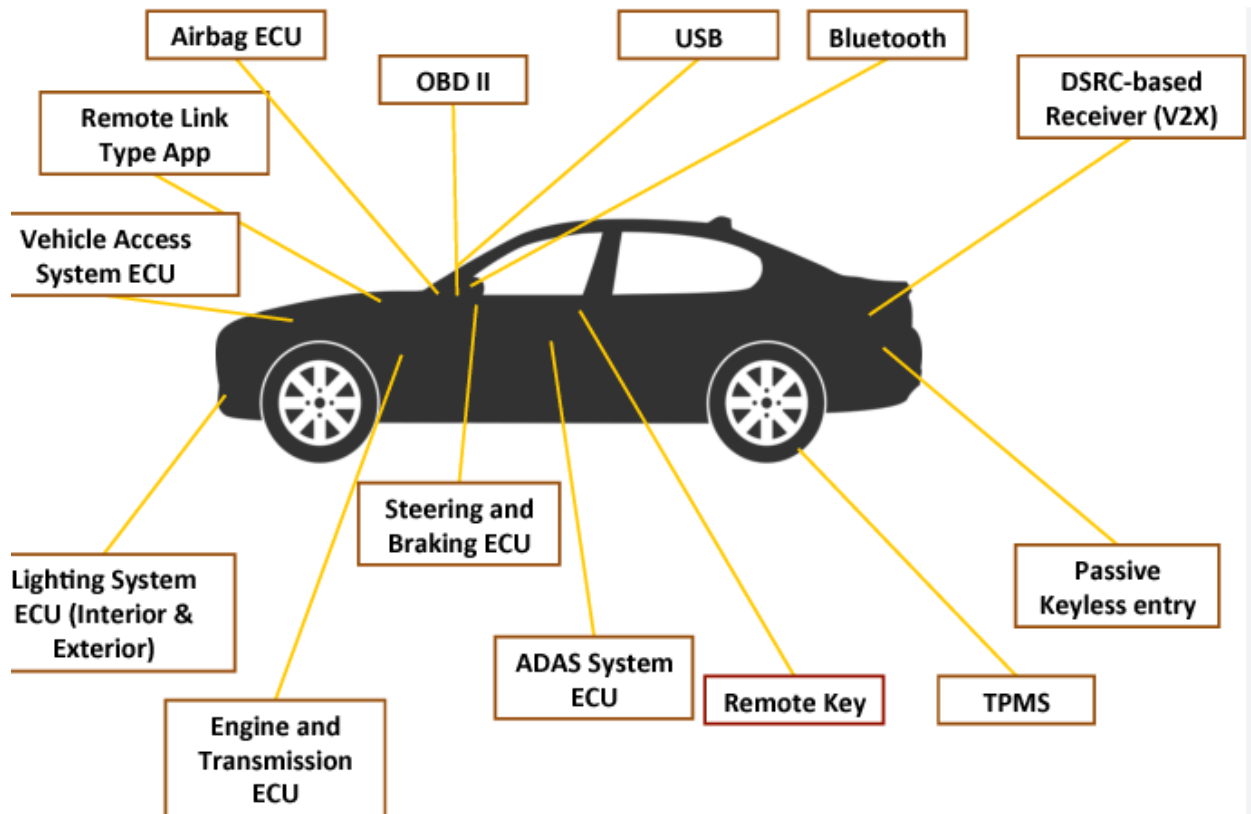


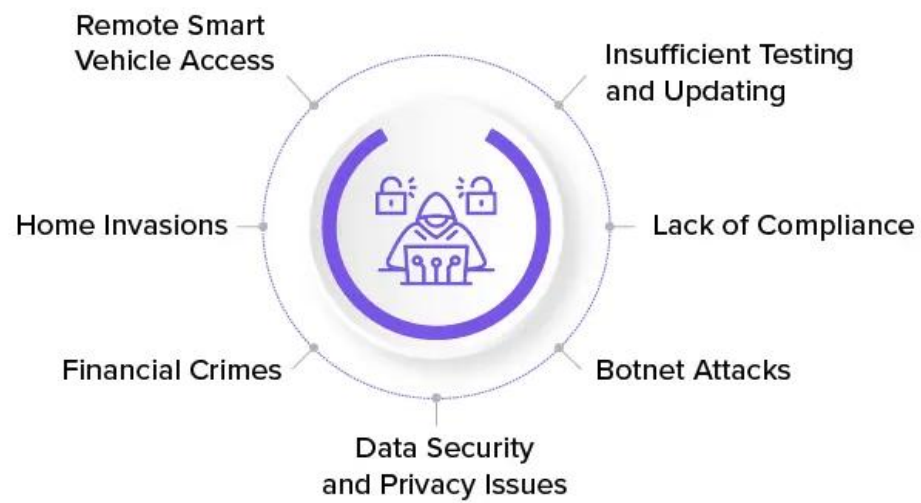
Fig: Car Vulnerabilities Using IoT devices (Bankole, 2023)

c) Countermeasures and Risk Mitigation Strategies

Moreover, challenges in cybersecurity that is being increased by Internet of Things devices. Research (Esra Altulaihan, 2022) that is published in Electronics reviewed an different types of cybersecurity threats for Internet of Things devices and even made an mitigation measures for countering it like using and implementing robust system using strong encryption, firmware updates (Ashutosh Bandekar, 2018) that is done regularly and using machine learning with detection systems for intrusion and prevention. The researchers also said about the importance of awareness in users and educating in risk mitigations.

Especially, sectors like healthcare (Usha Devi Gandhi, 2018) using the interconnected devices which is called an IoT devices brings an big security related concerns. Even an researchers from IEEE conference (Mirza Akhi Khatun, 2023) told about the use of the machine learning ideas and techniques for enhancing the security related to Health sectors Internet of Things ecosystems. These kind of research (Thapa, 2018)shows that how ML algorithms helps to detect unusual behaviors that is done during cyber attacks and improves the safety of the Healthcare Internet of Things ecosystems.

IoT Security Vulnerabilities and Challenges



appinventiv

Fig: IoT Security Vulnerabilities and Challenges (Sharma, 2024)

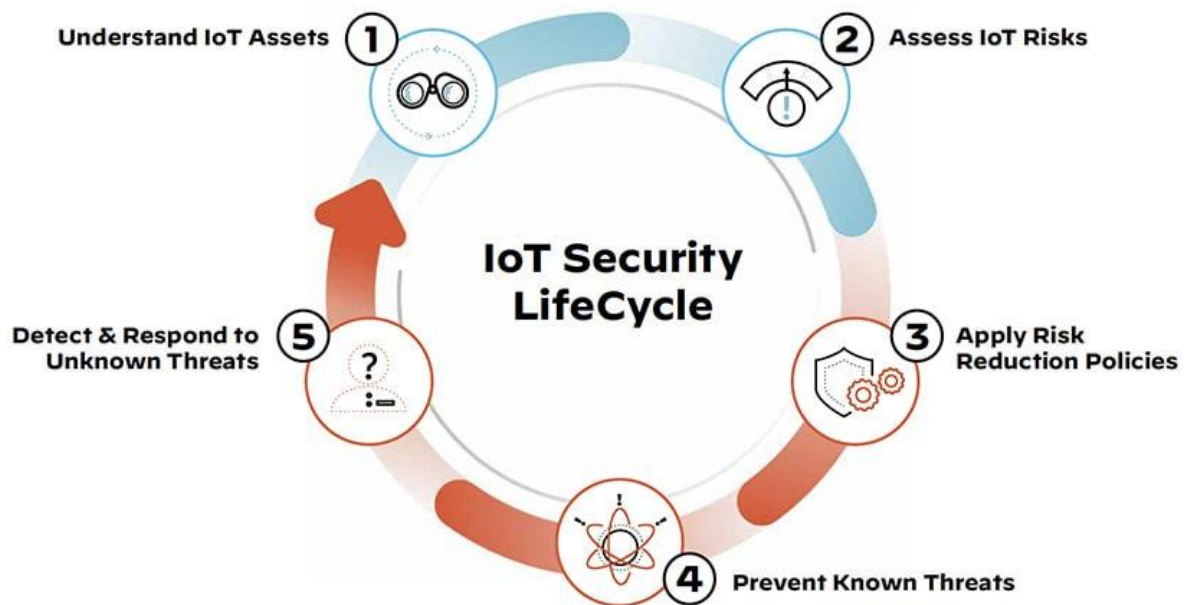


Fig: IoT Security Life Cycle (Networks, 2025)

d) Emerging Trends and Future Directions

Nature of threats related to cybersecurity (Esra Altulaihan, 2022) that is dynamic need an continuous adaption and unique innovation in mitigation of cybersecurity. The just recent growth (Usha Devi Gandhi, 2018) is showing and indicating a big interest in the honeypot development systems for Internet of Things ecosystems or environment. is also focusing in deploying an value of honeypots like HloTPOT for gathering intelligence about the behaviors of the attackers and development of the mechanism for defense in proactive manner.

Moreover, use of artificial intelligence and machine learning (Esra Altulaihan, 2022) in security mechanisms frameworks is gaining an popularity. Technologies (Mirza Akhi Khatun, 2023) like this helps to enhance the detection of threats capacity and helps to automate the security response for incident of cybersecurity. Using these types of things can help the security challenges be working in great condition and with no any type of cyber attacks caused by black hat hackers.

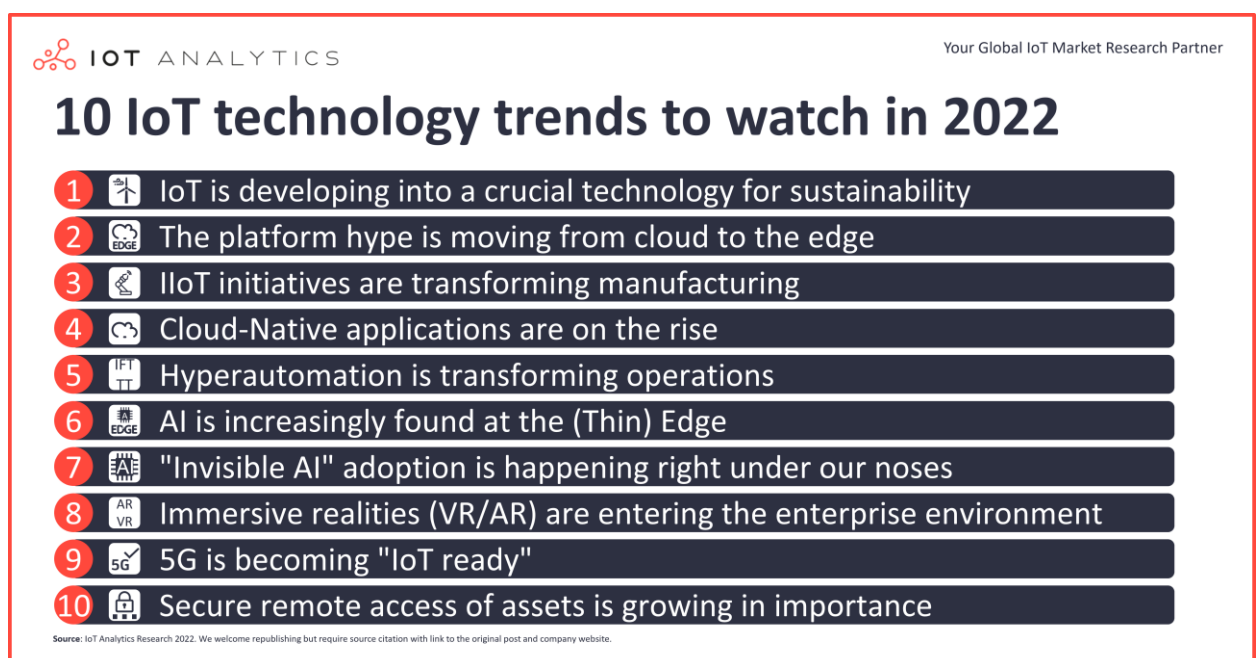


Fig: Top Ten IoT Devices Trends (Wilford, 2022)



Fig: Future of IoT Devices (Solulab, 2025)

e) Conclusion

Overall, the literature review shows the critical demand for a secure and robust cybersecurity mitigation and measures for protecting the Internet of Things devices from black hat hackers. Even though the progress for understanding of the vectors attack and countermeasures is rapidly improving still the attacks is causing the big trouble in the security part of the cyber world. Moreover, efforts should be always focused on security basic demand for security of robust systems protocols, even user awareness enhancing should be done and building an new Internet of Things devices that is made sure that it is safe and secure with robust security measures.

Critical Analysis

a) **Case Study 1:** Impact and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization. (CISA, 2022)

- **Background:** CISA (CISA, 2022) in October 22 and the FBI made an joint venture on cybersecurity advisory which highlighted the things that is being exploitation on multiple known public vulnerabilities at Zoho products ManageEngine. The vulnerabilities if attacked properly and is exploited successfully then this could lead to gain persistent access on victim networks. Especially, the APT group of peoples finds out weak point and vulnerabilities for many things like data exfiltration, latera movement and even reconnaissance. ManageEngine of Zoho (CISA, 2022) are being implemented by Information Technology software for management, which lead to the big target on organizations in many various sectors and areas. The easy way for attacking and exploiting flaws that coupled with extensive use and reach of ManageEngine Products (CISA, 2022) in enterprise area or environments that creates an big significant vectors for attacks.
- **Issue Identification:** The main issue (CISA, 2022) that was identified in the advisory is critical existence of vulnerabilities in few ManageEngine Zoho products. There weak points (CISA, 2022) were like authentication bypass flaws, arbitrary file upload vulnerabilities and even remote code execution opportunities. The important detailed vulnerabilities that were common are such as CVE-2022-35405 and even CVE-2022-28199. These kind of vulnerabilities allowed malicious actors to bypass security controls, even upload a malicious files and (CISA, 2022) unlimited execution of arbitrary of codes that caused an big effect on the systems. Especially, the unauthorized access (CISA, 2022) that can or could be used for conducting an more further activities that is malicious within networks that is compromised like ransomware deploying, sensitive data stealing and even an critical services disruptions. Nature of the persistent (CISA, 2022) also means that the actors that acts as a threat can maintain a smooth hold on the network for long periods of time which causes removing and detecting cybersecurity challenges more.
- **Mitigation:** Both CISA and FBI (CISA, 2022) are recommending an action immediately for mitigating the risk that is associated with these kind of vulnerabilities. Main mitigation ideas or strategies (CISA, 2022) that should be followed includes things like applying patches, hardening configurations, network segmentation, monitoring and detection, threat hunting and reviewing external exposures.

- **Summary:** CSA AA22-277A (CISA, 2022) served a warning that is critical regarding exploitation that is active with its weak point or vulnerabilities in ManageEngine of Zoho products (CISA, 2022) by black hat hackers or advance threat actors. The case study also shows if patching is done timely, security configurations is robust, and monitoring in active state for defending from these kind of threats. Moreover, if attackers impact successfully (CISA, 2022) and exploited the system then it can cause an data breach and even a loss of financial stability or even infrastructure disruptions in critical way. So, using these kind of recommendations (CISA, 2022) organizations also can reduce attack surface area for hackers for stopping it to get compromised. This case study (CISA, 2022) is highlighting the events of cyber threats that is being faced and even measures to protect it using the mitigation idea or practices in cybersecurity protection.

b) Case Study 2: An Unprecedented Look at Stuxnet, the World's First Digital Weapon.

- **Background:** Early 2010 (Zetter, 2014) noticed a deadly cyber weaponry and Stuxnet that is emerging as a example. It was a joint group work by US and Israel which was never conformed officially and It was targeted on Natanz nuclear facility in Iran. Moreover, facility had one IR-1 centrifuges that was very important for enrichment of uranium. This cyber attack (Zetter, 2014) objective was never for stealing the sensitive data but was to destruction of physical damage, a new way of cyber crime warfare. The article shows (Zetter, 2014) the details of the nature in the operation. Especially, the initial planning involved and new invention of the malware was found which was called Stuxnet that is very dangerous and focuses on control systems of Industrial sectors lets say Siemens programmable logic controllers (Zetter, 2014) and managed the centrifuges. This kind of moves that is from old generations or traditional IT Systems to operational technology has made a big difference in cyber threats problem.

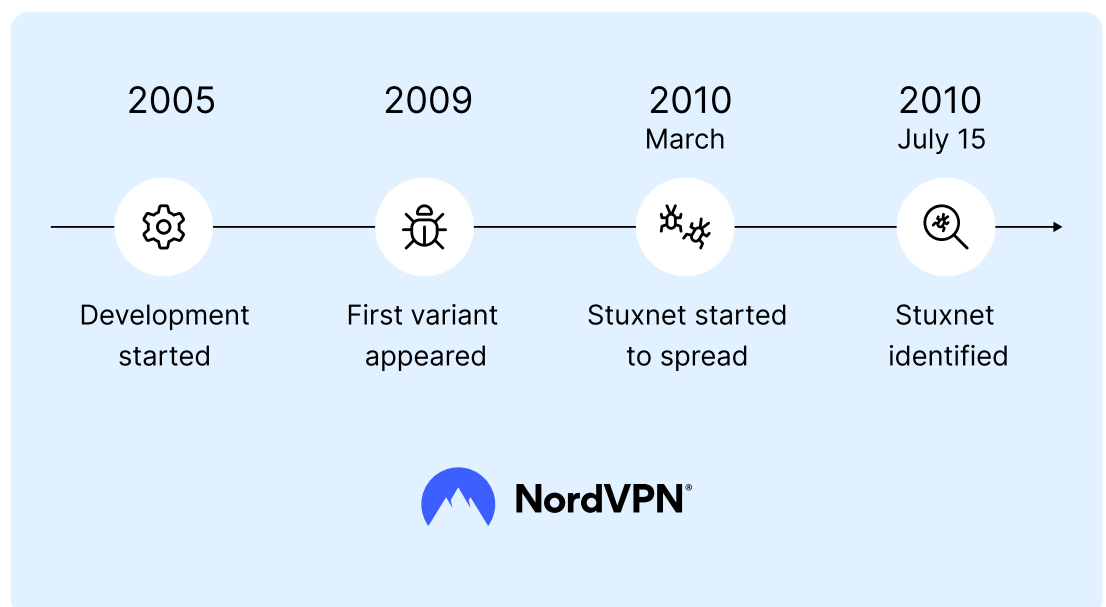


Fig: Timeline of Stuxnet Attack in Iran (NordVPN, n.d.)

- Issue Identification:** The main issue (Zetter, 2014) that was the covert disruption and damaging the nuclear program of Iran by cyber attacks means. Moreover, Stuxnet made an achievement (Zetter, 2014) by changing the centrifuges speed. It's behavior was that it was increase speed of rotation in drastically which caused heavy stress in the device and failure would occur. Moreover, (Zetter, 2014) it was again lowering the speed of the centrifuges. This malware (Zetter, 2014) was designed in such a way that the even intrusion detection system would not detect and could not send it to the control room which created a wrong sense of normal process but the centrifuges was destroyed systematically. The device (Zetter, 2014) that was used to spread a malware was a infected USB drives, which exploited a zero day vulnerability in windows os and Siemens software. This attack (Zetter, 2014) was so sophisticated in its nature that it had the ability to do the work in silently and even give chance to notice any kind of false sense to operator which made it had to detect and search it. Engineer of Iran called Bewilderment found out that the equipment was failing without any cause and we can see the how effective the attack of Stuxnet's deceptive tactics.

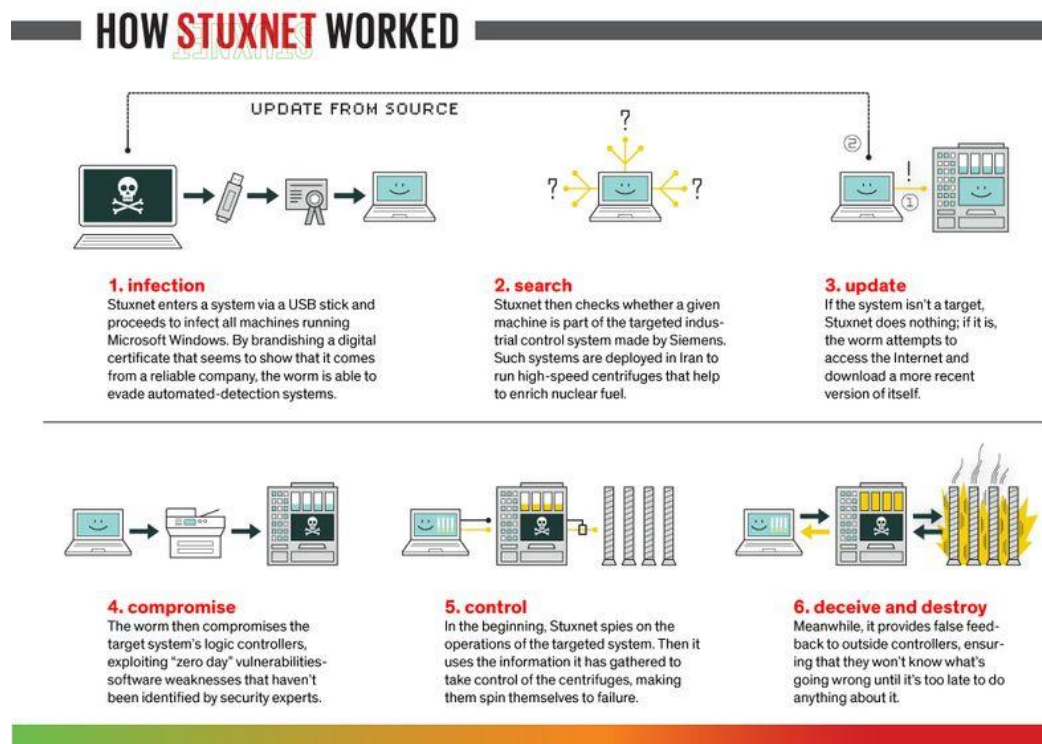


Fig: How Stuxnet worked (Spectrum, 2013)

- **Mitigation:** The problem solving idea that the Natanz facility immediately (Zetter, 2014) took involved search and identifying and main point deleting the Stuxnet worms and infection from the systems they are using. It was a very difficult and complex malware to be found because of how the malware (Zetter, 2014) was designed to do the work silently. Also Siemens updated the software (Zetter, 2014) and even the security patch for that vulnerability. Moreover the finding of Stuxnet made an wake up call on cybersecurity measures in community and organizations that is related to industrial worldwide. Especially, (Zetter, 2014) it also showed us the critical problem that needs to be addressed immediately for security enhancement like segmentation of networks, intrusion detection system that is robust and even a control on removable media is stricter. This kind of incident (Zetter, 2014) also helped the nation for awareness of how the attacks can be done and can be used against its owner by the method of cyber weapons attacks that can cause any kind of damage that is physical.
- **Summary:** Overall, Stuxnet shows us a (Zetter, 2014) moment of watershed in the history of cybersecurity. The wired article demonstrated the attacks that is potential to happen by hackers for stealing data and even a physical destruction on infrastructure that is critical. Moreover, this attack case showed and exposed weak point of the control systems used in industrial sectors or area and importance of securing it properly in proactive way from both information technology and operational technology. Stuxnet attacks (Zetter, 2014) incident impacted Iran program of nuclear but made an alert trigger for cyber threats globally that made an main focus on increasing ICS security, (Zetter, 2014) sharing threat intelligence and even the war of cyber crime in future. This kind of attack can be done by only using a advanced persistent threats.

Conclusion

Winding everything up, this report is painting a somber picture of the increasing cybersecurity attacks on the constantly expanding Internet of Things universe. The early hope of increased automation and efficiency based on data is more and more being dwarfed by the stark reality of abused vulnerabilities at the hands of black hat hackers. These weaknesses, due to improper security controls, default passwords, lack of standardization, and substandard update processes, yield fertile ground on which attackers enter and wreak destruction across different domains.

Literature review highlights the gravity of these threats, listing typical attack targets like DDoS attacks and weak credential breaches. Real-world case histories, such as the robot vacuum incursions and the Kia web portal breach, graphically illustrate the vulnerability to destruction that is on a continuum from individual disruption to large-scale unauthorized access. As protective practices like robust encryption, regular patches, and intrusion detection systems are being researched, the ever-changing nature of cyber threats necessitates continuous innovation and adaptability. The development of honeypot technologies and application of AI and machine learning bring promising lines of pursuance for anticipatory defense.

The sober examination of the CISA alert on Zoho ManageEngine vulnerabilities and the trailblazing Stuxnet attack provides additional urgency to the feeling. The ManageEngine case illustrates how outdated software can be leveraged for persistent access to enable data exfiltration and infrastructure disruption. Stuxnet, on the other hand, is a sobering reminder of cyber weapons intended to inflict physical harm, pushing cybercrime beyond traditional data theft.

Lastly, the report calls for an urgent paradigm shift in addressing IoT security. In the future, a multifaceted approach is required. This includes embedding robust security features into the architecture of IoT devices themselves, placing stringent standardization upon the industry, prioritizing and making transparent and regular software updates, and establishing a user-education and culture of awareness. The lessons learned from past attacks, coupled with objective consideration of new security technology, are what drive us to make our globalized world stronger in the face of ever-evolving black hat hacker threats. Our info security, our critical infrastructure, and even our body health come to rely more and more on our collective ability to address these weaknesses directly.

References

- Alexander S. Gillis, B. P. S. S., 2023. *TechTarget*. [Online]
Available at: <https://www.techtarget.com/iotagenda/definition/IoT-device>
- Andrew Shoemaker, G. M., 2024. *IMPERVA*. [Online]
Available at: <https://www.imperva.com/blog/wp-content/uploads/sites/9/2024/07/Figure-3-DDOS-Event.png.webp>
- Antariksh Sharma, P. V. M. K. S., 2023. Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning. 9 August.
- Ashutosh Bandekar, A. Y. J., 2018 . Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices. *Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices*, 26 August.
- Balbix, 2025. *Balbix*. [Online]
Available at: <https://www.balbix.com/app/uploads/IoT-Convergence-1536x864.png>
- Bankole, M. O., 2023. *Linkedin*. [Online]
Available at:
https://media.licdn.com/dms/image/v2/D4D12AQE0VNKSrZ74VQ/article-cover_image-shrink_720_1280/article-cover_image-shrink_720_1280/0/1693753037784?e=1748476800&v=beta&t=Uf2GW6udhYEDmRRxGTPKUTx0VGkEwu7Uu4p1vTHuHo8
- Buntz, B., 2016. *IOT WORLD TODAY*. [Online]
Available at: <https://eu-images.contentstack.com/v3/assets/blt31d6b0704ba96e9d/blt7153bc6ab66a9a22/63abe9f5090e5422c3936167/infographic-security.jpg?width=700&auto=webp&quality=80&disable=upscale>
- CISA, 2022. *CISA*. [Online]
Available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-277a>
- Esra Altulaihan, M. A. A. a. A., 2022. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions*, 16 Oct.
- IBM, n.d. *IBM*. [Online]
Available at: <https://www.ibm.com/think/topics/internet-of-things>
- IDB, 2025. *IDB*. [Online]
Available at: <https://www.idb.org/cybersecurity-and-the-internet-of-things/>
- KASPERSKY, n.d. *KASPERSKY*. [Online]
Available at: <https://www.kaspersky.com/resource-center/definitions/hacker-hat-types>

KasperskyOs, 2025. *KasperskyOs*. [Online]

Available at: <https://os.kaspersky.com/wp-content/uploads/sites/31/2025/01/pylesos-i-sobachka.png>

Konstantinos Tsiknas, D. T. ,. K. D. ,. C. S., 2021. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures*, 29 Jan.

KRATIKAL, 2021. *KRATIKAL*. [Online]

Available at: <https://kratikal.com/blog/wp-content/uploads/2021/09/Artboard-12A-copy-8@3x-100-scaled-1-2048x1058.jpg>

Lueth, K. L., 2018. *IOT ANALYTICS*. [Online]

Available at: <https://iot-analytics.com/wp/wp-content/uploads/2018/08/Number-of-global-device-connections-2015-2025-Number-of-IoT-Devices.png>

Manos Antonakakis, G. I. o. T. et al., n.d. *unix association*. [Online]

Available at: <https://www.unix.org/conference/unixsecurity17/technical-sessions/presentation/antonakakis>

Mirza Akhi Khatun, S. F. M. C. E. L. L. D., 2023. Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. *Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation*, 22 Dec.

Mohammed Aziz Al Kabir, W. E. S. S., 2023. Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques. *Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques*, 12 July, pp. 199-233.

Nancholas, B., 2024. *Keele Universty*. [Online]

Available at: <https://online.keele.ac.uk/the-internet-of-things-iot-and-its-impact-on-different-industries/>

Networks, p., 2025. *paloalto Networks*. [Online]

Available at:

https://www.paloaltonetworks.com/content/dam/pan/en_US/images/cyberpedia/what-is-iot-security-cyberpedia-image-3-868x488.jpg?imwidth=1366

NordVPN, n.d. *NordVPN*. [Online]

Available at:

<https://ic.nordcdn.com/v1/https://sb.nordcdn.com/m/231c25038240b424/original/blog-infographic-stuxnet-virus-svg.svg>

Praveen Pawar, A. T., 2018. Device-to-Device Communication Based IoT System: Benefits and Challenges. *Device-to-Device Communication Based IoT System: Benefits and Challenges*, 13 Jun, pp. 363-374.

SANGFOR, n.d. *SANGFOR*. [Online]

Available at: <https://www.sangfor.com/glossary/cybersecurity/what-is-black-hat->

[hacking#:~:text=This%20is%20where%20the%20term,purposes%20rather%20than%20helping%20organizations](#)

SECURITY, 2020. *SECURITY*. [Online]

Available at: <https://www.securitymagazine.com/ext/resources/loT-Infographic-Teaser-Image-FINAL-JPEGsmall.jpg?1590675045>

Sehgal, D., 2022. *Linkedin*. [Online]

Available at: <https://www.linkedin.com/pulse/iot-intrinsic-part-our-daily-life-deepak-sehgal/>

Sharma, N., 2024. *appinventiv*. [Online]

Available at: <https://appinventiv.com/wp-content/uploads/2021/03/How-to-Ensure-Cybersecurity-in-the-Age-of-IoT-07.webp>

SOCIETY, S. C., 2021. *SINGAPORE COMPUTER SOCIETY*. [Online]

Available at: <https://files-scs-prod.s3.ap-southeast-1.amazonaws.com/public%2Fimages%2F1602032469479-How+to+Secure+Your+IoT+Devices+%28Recommendations%29.png>

SOCIETY, S. C., 2021. *SINGAPORE COMPUTER SOCIETY*. [Online]

Available at: <https://files-scs-prod.s3.ap-southeast-1.amazonaws.com/public%2Fimages%2F1602031848101-Internet+of+Things+%28IoT%29+security+challenges.png>

Solulab, 2025. *Solulab*. [Online]

Available at: <https://www.solulab.com/wp-content/uploads/2019/04/IoT-the-Future-of-Innovation.jpg>

Spectrum, I., 2013. *IEEE Spectrum*. [Online]

Available at: <https://spectrum.ieee.org/media-library/img.jpg?id=25571945&width=800&quality=85>

Thapa, M., 2018. *Mitigating Threats in IoT Network using Device Isolation*, s.l.: s.n.

Usha Devi Gandhi, P. M. K. R. V. G. M. R. S. & S. K., 2018. *HloTPOT: Surveillance on IoT Devices against Recent Threats*. *HloTPOT: Surveillance on IoT Devices against Recent Threats*, 22 Jan.

Wilford, E., 2022. *IOT ANALYTICS*. [Online]

Available at: <https://iot-analytics.com/wp/wp-content/uploads/2022/01/10-IoT-technology-trends-to-watch-in-2022-min.png>

Zetter, K., 2014. *WIRED*. [Online]

Available at: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

