iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71771

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

The Impact of IoT on Cyber Security

Aditya Kumar[1], Prof. Prasanna Kumar[2]
[1]*Student, Amity Institute of Information Technology, Amity University Patna*
[2]*Associate Professor, Amity Institute of Information Technology, Amity University Patna*

Abstract: ***Extending from home appliances, cars, to IoT wearable devices, The Internet of Things (IoT) connects various physical and non-physical items to the internet allowing for interaction, communication, and information transfer. Even though IoT provides chiropractic benefits to smart homes, healthcare, transport, IoT, and many industries, its rapid adoption poses equally dire challenges to cybersecurity. The massive scope of available interconnected devices proliferates the threat landscape available to cybercriminals, hence making breaches, data loots, or system tampering IoT networks more vulnerable.***
This document looks into how cybersecurity is impacted by IoT cyber insecurities imposed by smart devices with real-time data transfer threaten information integrity, privacy, and reliability of the systems. Besides that, the report hopes to identify the absence of effective mitigation within the IoT system by concentrating on known vulnerabilities like lack or weakness of authentication, missing patches, absence of secure protocols, and insufficient encryption. Documented cases of cyber incidents involving IoT devices have shown the need for strong security frameworks and this is what study aims to hope for.
By reviewing existing literature and evaluating case studies, this work seeks to determine the current issues IoT security faces and its gaps. It analyze the responsibility of stakeholders like producers, developers, and consumers toward adherence to best practices like secure device setup, continuous software installation, and network surveillance.
The findings suggest that IoT can transform the face of technology utilization; nevertheless, its merits will be fully enjoyed only if strong cyber security infrastructures are put in place. This work recommends the establishment of uniform security guidelines, increased public education, and policy modifications IoT governance as frameworks to build a reliable and secure domain.
Keywords: Internet of Things (IoT), Cybersecurity, Smart Devices, Network Vulnerabilities, Authentication and Encryption, Secure Communication Protocols, IoT Governance.

I. INTRODUCTION

Evidently, one of the most sensational developments in technology in the 21st century is The Internet of Things (IoT). It is regarded as a network of various electronic things that are interconnected, meaning devices like smart thermostats, fitness trackers, industrial sensors and even autonomous vehicles are able to monitor, automate, and make decision throughout IoT systems using AI without the need for human interaction. Because of the rapid development of technology, measuring the risks and understanding its impact on a person's daily life can be challenging. There has been an estimation that is liberated there will be over 29 billion interconnected devices by 2030. This ability to connect enhances quality, easiness, and fuel driven data innovation but comes with serious cybersecurity problems. The chances of IoT devices becoming targets for cybersecurity criminal has drastically increased. These benefits will permit new levels of effectiveness to be obtained but essential dynamic augmentations are needed to safeguard the growing risks linked with data manipulation. Many IoT devices have limiting constraints on their computing capabilities in terms of processing power, memory, and energy supply. Weak security protocols are difficult to implement with such restrictions. Functionality tends to take precedence over security, due to deadlines forcing companies to release products in a rush. Consequently, many IoT devices are sold with out-of-the-box configurations containing easily exploitable security vulnerabilities like weak default passwords, unencrypted communications, and outdated firmware.

Growth in cyberattacks focused on IoT devices have revealed new powerful risks to a wide range of users. The IoT focused security weaknesses of systems were laid bare by huge botnet IoT powered device attacks in 2016, rendering millions of devices inoperable were unprotected. The safety of sensitive personal information, reliable operation of vital systems, and even protection on a state level is damaged from such events.

The focus of this dissertation will be on examining the exacerbating impact of IoT on cybersecurity frameworks. Its primary objective will be to investigate the major vulnerabilities created by IoT technology, analyze real-world cases of IoT-related threats and breaches, and evaluate the existing protective measures within IoT ecosystems. In addition, the degree of responsibility these stakeholders as device manufacturers and consumers, network providers, and policy makers need to assume in securing IoT devices will also be discussed.

©IJRASET: All Rights are Reserved

Understanding the intersection of IoT and cybersecurity is crucial as society becomes increasingly reliant on smart devices. Without adequate security frameworks, the very technologies designed to simplify our lives can pose significant risks. This research will contribute to the ongoing dialogue on how to secure the future of IoT and ensure it can be integrated safely and sustainably into our connected world.

II. LITERATURE REVIEW

The Internet of Things (IoT) has been a focal point of discussions in the field of technology ever since it started growing in parallel with daily life. It provides outstanding advantages like automation, optimized processes, and the broadcasting of information in real time, but at the same time raises unnerving issues in cybersecurity.

Atzori et al. 2 in 2010 represents IoT as: "a dynamic global network infrastructure with self-configuring capabilities and composed of interconnected domains that are governed by interests of various quasi-legal entities." Such as devices of a home automation systems and medical implants create an ecosystem of interconnectivity, which simultaneously broadens the horizon in which attacks can be launched from. Roman, Zhou, and Lopez (2013) highlight that unlike traditional IT systems, IoT devices depend heavily on automation, which is done with little human oversight—thus creating many points of vulnerability.

One of the primary concerns regarding enabling effective cybersecurity within IoT is the absence of policy standardization across devices. Weber (2010) points out that many manufacturers of IoT devices do not incorporate proper encryption, authentication, and even update sign protocols due to design or cost constraints—resulting in devices being sent out with factory credentials.

Research by Sicari et al. (2015) draws attention to the issues regarding data privacy and integrity within IoT networks. IoT devices pose the risk of identity fraud, surveillance, and even physical controlled system hacking. The risk is grave resulting in sensitive data breaches that is done through continuous logging, processing, and transferring done by IoT technologies. Especially in Healthcare, smart industrial IoT and smart cities, this is very alarming. The failure or manipulation of systems or data can incur devastating costs in both human lives and financial resources.

Kolias et al. (2017) attribute the Mirai botnet attack of 2016, which is one of the most cited IoT security case studies, was analyzed by Kolias et al. (2017). It showed the possibility of commandeering poorly secured IoT devices to construct tremendous botnets capable of executing extensive Distributed Denial-of-Service (DDoS) attacks. The event intensified the demand for stricter security protocols which, alongside other works, generated the need to devise light-weight encryption and authentication systems tailored for low-resource devices.

Babar et al. (2011) offers another essential angle by offering a five-tier framework that outlines IoT's security challenges: perception, network, middleware, application and business. Their approach aids vulnerability assessment within these layers and provide tailor-made solutions like intrusion detection systems, anomaly detection, and blockchain.

Dr. Sharma and Dr. Chen's research in 2019 proves that interwoven AI systems provide more efficacy in monitoring IoT networks for unusual behavior or even an intrusion within the system as compared to traditional security systems. Furthermore, there is greater need for addressing issues like data quality, arbitrariness of the attacks on the system, and scaling for these advanced technologies.

As Tawalbeh et al. (2020) elaborate further, policies and regulations do emerge as one of the forefront issues to address. Other researchers defend that the laws IoT is bound within have to inevitably shift and adapt with how quickly the technology erupts. The researchers advocate for universal standards and regulations for the education and informing IoT users along the division of responsibilities for service providers and manufacturers. In spite of putting forth several scholarly works, the literature still agrees on the fact that a universal solution for cybersecurity in IoT is still out of reach. The existing technology approaches do not seem to address the problem sufficiently. There is a call for deeper collaborative efforts by governments, technology corporations, and academics that create principles fostering security-by-design, security awareness, and compliance monitoring programs.

To wrap things up, the increasing body of literature makes it clear that the risks posed by adopting IoT technologies is increasingly acknowledged. The solutions posed by developing technologies provide an answer only in part. Securing IoT networks is a complex issue requiring responsive innovation, changes in legislation, and designation of responsibility by the users. This literature is complemented by further research on current security strategies and developing sustainable measures to protect IoT ecosystems from advanced persistent threats.

III. SCOPE OF THE STUDY

The purpose of this research is to study the intersection of the Internet of Things (IoT) and cybersecurity. The focus is on the pervasive systems of digitization and interconnectivity. Their integration into everyday life: smart homes, wearables, industrial control systems and healthcare technologies, pose new security challenges. This study aims to map the security landscape, identify critical threats and assess the risks of IoT ecosystems.

This research will be concentrating on the cyber security challenges created by the IoT network's device heterogeneity, limited computing resources, lack of standard security frameworks, and multiple infiltration points. The scope of this research also includes both individual and organizational IoT systems to ensure a holistic view of security. More advanced techniques such as Artificial Intelligence (AI) and Machine Learning (ML), along with basic ones like firewalls, encryption, and authentication will be studied under IoT system security. This research will also focus on the governance policies and laws that define the way IoT systems are secured and monitored. The study scope is not restricted to a single region but includes a global viewpoint, taking into account international benchmarks and extensively recorded events like the Mirai botnet attack. Moreover, the study seeks to extract primary data through interviews or surveys with cybersecurity professionals and secondary data from relevant scholarly articles, reports, and case studies. This research is expected to provide value to a variety of stakeholders including developers, cybersecurity consultants, manufacturers of IoT devices, information technology managers, and policy makers. At the core, the objective is to provide actionable methodologies and steps to enhance cybersecurity measures for IoT devices and mitigate cyber threats in an interconnected environment.

IV. LIMITATIONS OF THE STUDY

While this study tries to explore the implications of IoT (Internet of Things) on Cybersecurity, it is bounded by certain limitations which affect the overall scale and generalizability of the results.

The availability and accessibility of data suffices as the study's limitation concerning inclusion and exclusion criteria.

Most organizations with prior cybersecurity incidents do not disclose comprehensive information regarding security breaches and their mitigation approaches. This lack of willing organizations shrinks the firsthand data pool for analysis, forcing an overreliance on secondary data drawn from published reports and academic studies. Another limitation factor involves the evolving nature of IoT and the Cybersecurity threat landscape. The introduction of new devices, protocols, and methods of attack means that the research conducted in this study will face obsolescence in a short span of time. This study, like others, captures the status and trends at the time of the research, forgetting to include ever-expanding advances and threats held in the future. Another drawback is the different technologies that compose an IoT device. The classification of IoT devices includes consumer-grade wearables and complex industrial IoT systems. Each of these has its own security architecture and risk profile. It is not easy to generalize other findings for all types of IoT applications, and the study may not comprehensively cover each sector's distinct challenges. The study also places greater emphasis on qualitative methods and descriptive evaluation. Due to logistical obstacles in gathering extensive primary data, the study has limited use of quantitative data. Although there was a deliberate attempt to use some expert testimony and practical illustrations, the absence of large sample size may undermine the statistical validity of some conclusions the study tries to make. Finally, due to constrained time and resources, the scope of the study emphasizes well- known issues and case studies pertaining to cybersecurity that may overshadow other equally important parts of the problem. As well, there are differences on the legal and regulatory side between countries which means this study may regionally bound cyberlaw policy and oversight fail to address some specific laws strategically. Even with these limitations, the study develops the groundwork for understanding how IoT devices impact cybersecurity and presents practical suggestions on securing IoT devices.

V. OBJECTIVES

1) To analyze the impact of IoT on various sectors like healthcare, smart homes, transportation and the manufacturing industry, as well as its components and evolution.
2) To analyze potential risks in IoT systems and voids in user, organizational, and national security.
3) To review available literature related to the standards and tools crafted for the safeguarding of IoT devices and data against cyberaggression.
4) To analyze available literature on breaches and incidents to learn how IoT weaknesses are exploited and how organizations would respond to such attacks.
5) To assess the level of responsiveness from organizations toward heightened IoT security requirements and the adaptability strategies undertaken.
6) To formulate guidelines that would enhance IoT framework security and recommended practices for safer digital environments.

VI. RESEARCH METHODOLOGY

The objectives of the study were achieved using the framework described in the previous chapter, which details the methods.

It encompasses the study's framework, approaches to data gathering, sampling methods, as well as the methods for data interpretation.

1) Research Design: This study employs both descriptive and analytical research methods. Descriptive research aids in understanding Cybersecurity challenges precisely concerning the Technology IoT. Analytical research is used to study the available documentation of incidents and the corresponding security measures developed in relation to IoT.
2) Data Collection Methods Primary Data: Data is obtained by administering formal questionnaires and conducting interviews with Cybersecurity and IT specialists, as well as IoT users. Secondary Data: Secondary data is sourced from some of the research articles, academic journals, cybersecurity reports, company case studies, whitepapers, and trustworthy websites focusing on IoT and Cybersecurity.
3) Sample Size and Sampling Technique Sample Size: 100 participants comprising IT specialists, cybersecurity practitioners, and IoT device users; Sampling Method: Random sampling is applied here so that every individual within the population has an equal opportunity to be included.
4) Tools and Instruments Used:

- Survey Tool: Google Forms is the platform that we use for the dissemination and gathering of responses to the survey.
- Data Analysis Tools:
- Microsoft Excel: Employed in arranging and graphically representing the data collected in the form of charts and graphs.
- SPSS (Statistical Package for the Social Sciences): Used in carrying out high level statistical examination and analysis of the data obtained from the survey.

5) Data Analysis Techniques:

Quantitative Analysis: Analysis of data from surveys is done through percentage analysis and trends is found through graphical representation.

Qualitative Analysis: Data collected through interviews alongside open-ended questions is analyzed by thematic analysis with the aim of discovering themes pertinent to the challenges IoT cybersecurity and solutions.

6) Ethical Considerations:

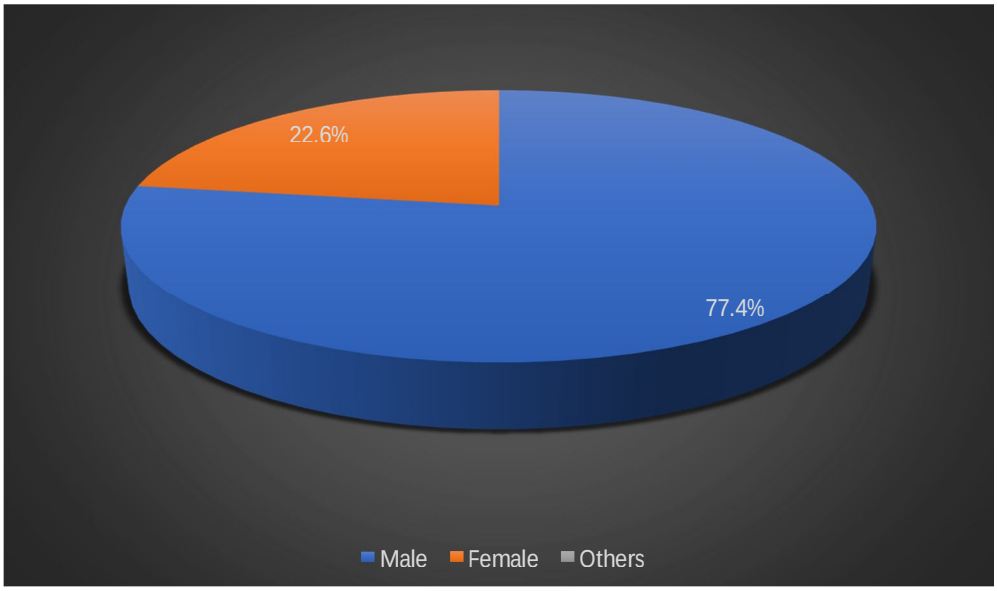
The identity, personal information, and responses of the participants are kept private and secure.

Data will only be collected after voluntary consent is granted and the respondent is fully informed about the study.

Information obtained will only be utilized for the purposes of scholarly work and academic research.

VII. ANALYSIS & INTERPRETATION OF DATA

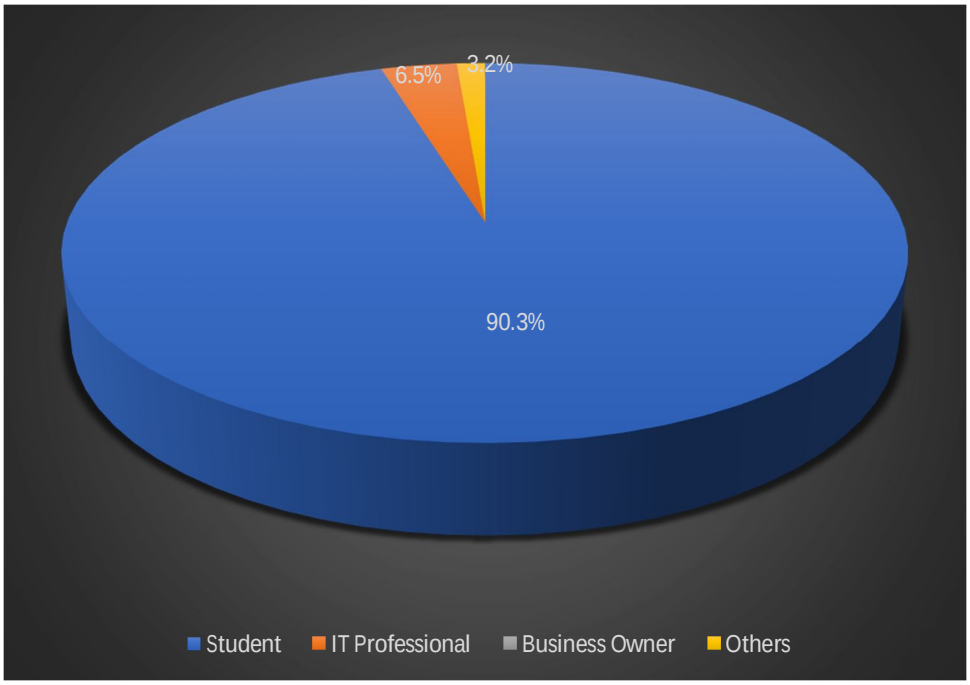
1) *What is your Gender?*



Based on the provided graph details, Male (77.4%): Most of the respondents identify as male and thus are representing the majority of the participants.

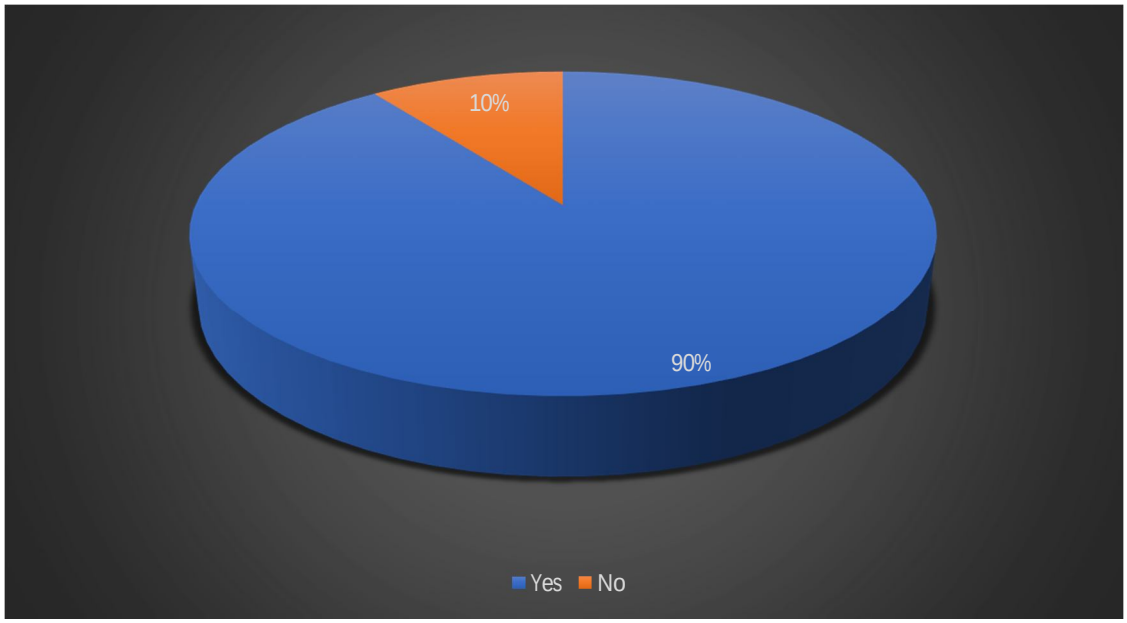
Female (22.6%): Minor constituency as who Identify as female.

2) What is your Occupation?



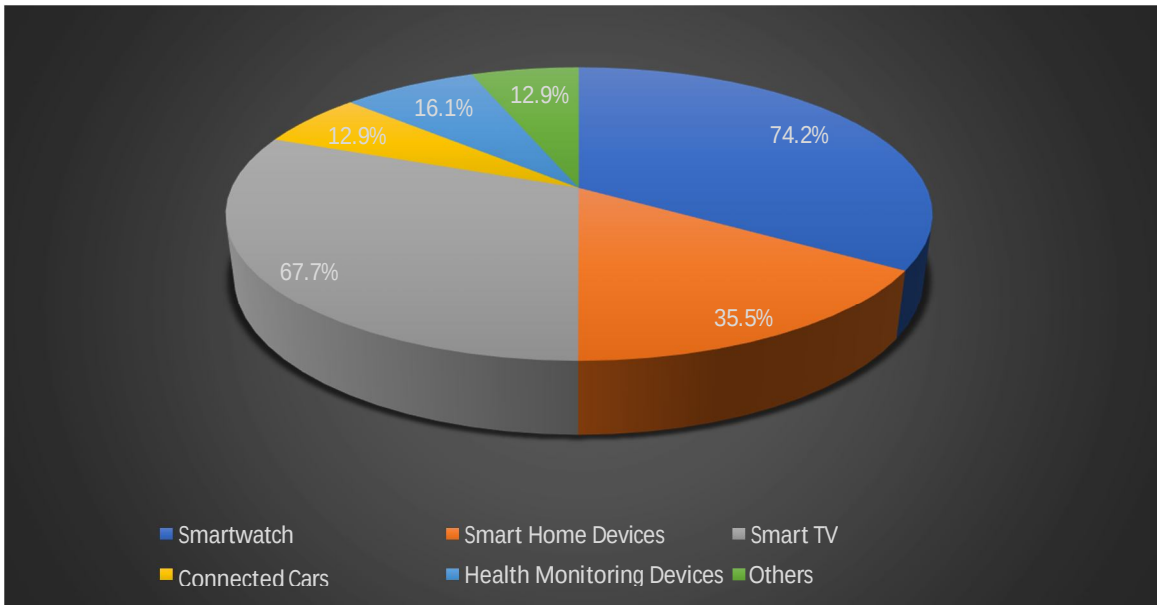
Based on the provided graph details, Student (90.3%) most of the participants are Students.
IT Professional (6.5%): Respondents are relatively small in numbers and are currently in IT Professional
Business Owner (3.2%): Business Owner makeup the smallest proportion of participants.

3) Are you aware of the Internet of Things (IoT)?



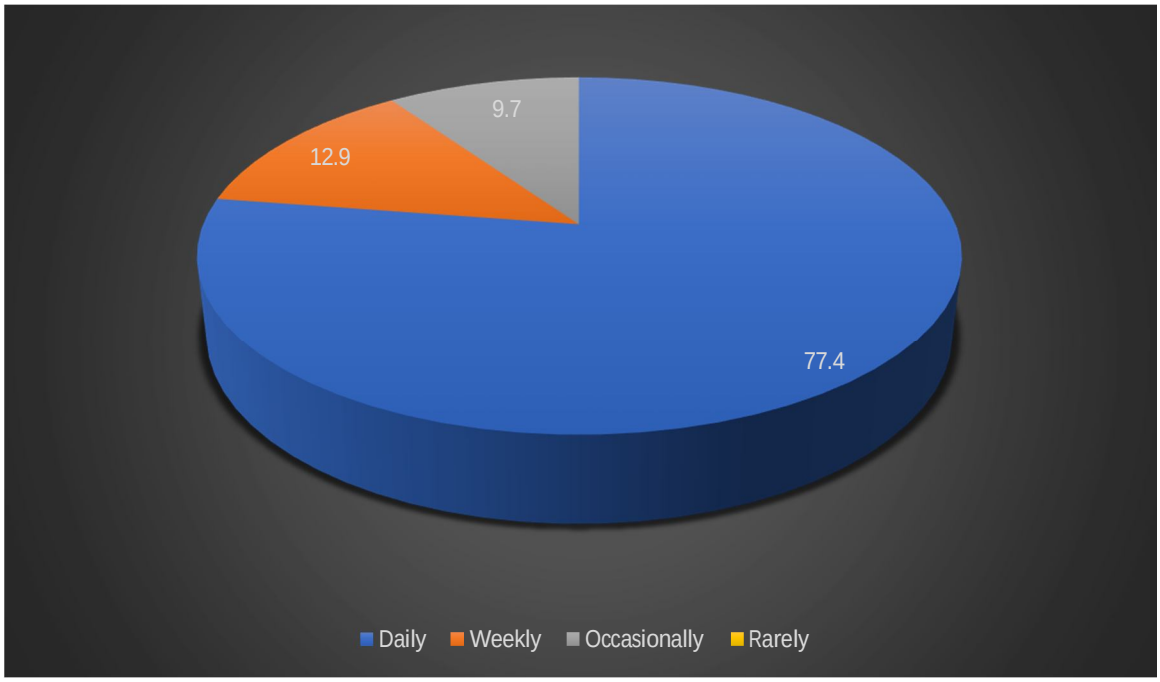
Based on the provided graph details:
A large majority (90%) of the participants are aware of IoT, showing high general awareness.
90% of respondents answered Yes, indicating they are aware of IoT.
Only a small minority (10%) are not familiar with the concept.
10% of respondents answered No, indicating they are not aware of IoT.

4) Which IoT devices do you currently use?



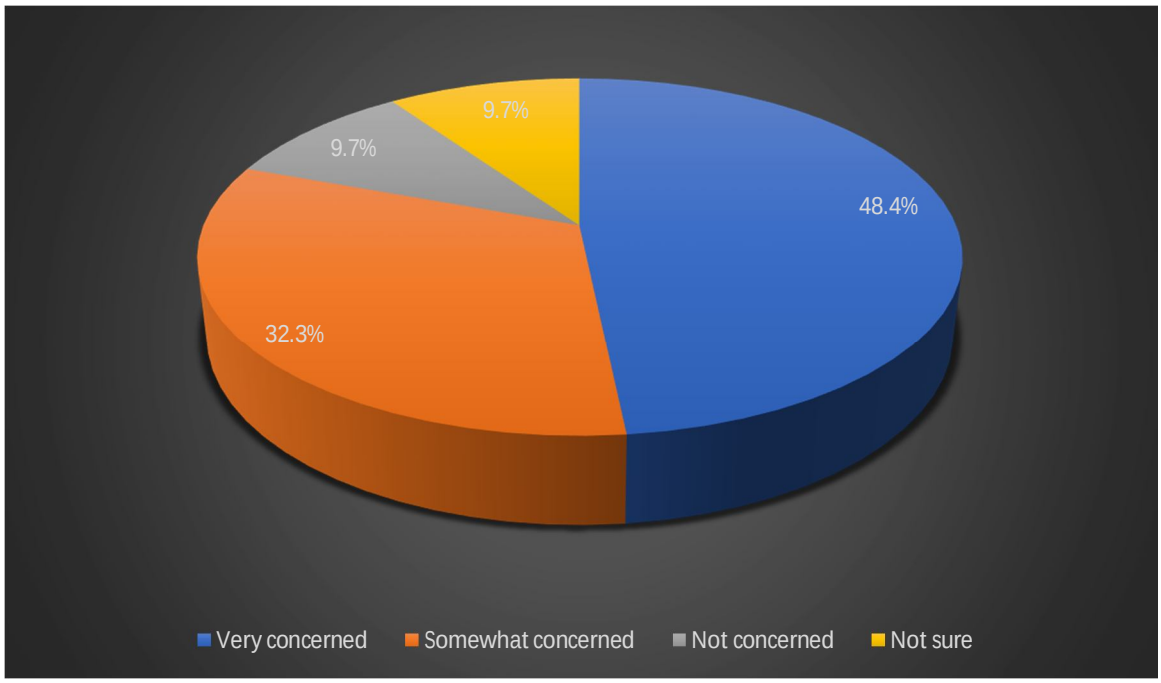
Based on the provided graph details:
Smartwatch (74.2%) is the most used IoT device, indicating a strong trend toward wearable technology.
Smart TV (67.7%) follows closely, suggesting users widely embrace smart entertainment systems.
Smart Home Devices (35.5%) are used by over a third of respondents, showing gradual adoption as smart living becomes more common.
Health Monitoring Devices (16.1%) and Connected Cars (12.9%) have relatively low usage, likely due to cost, niche applicability, or limited availability.
Others (12.9%) may include devices like smart appliances, security cameras, or IoT- enabled lights, showing some variety in use.

5) How often do you use IoT devices?



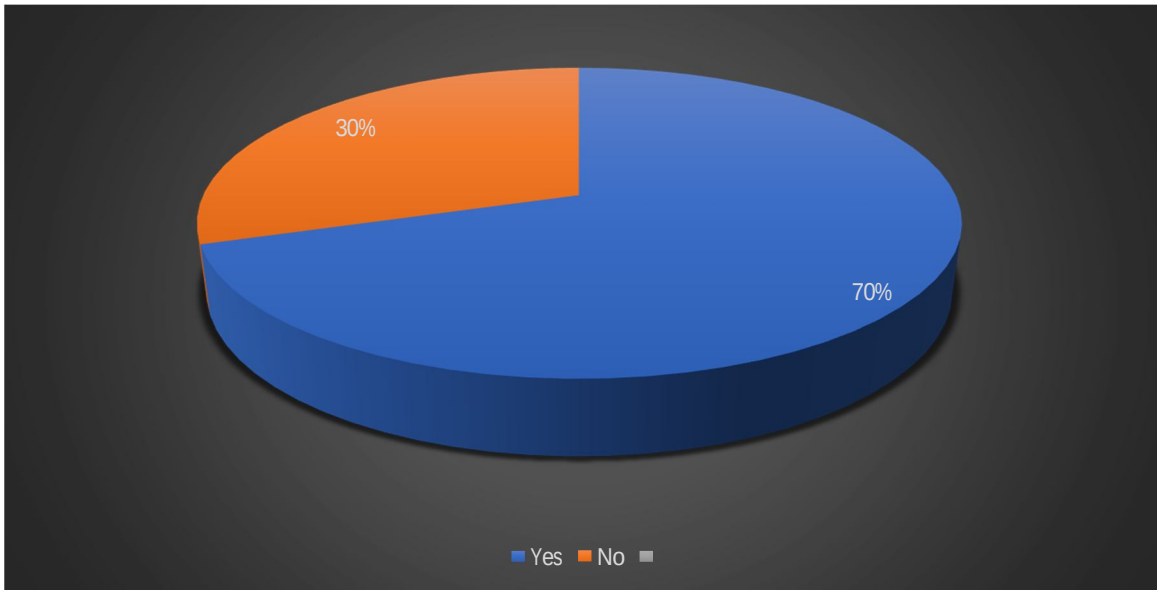
Based on the provided graph details:
According to the graph shown above, Daily (77.4%): Majority of users interact with IoT devices every day.
Weekly (12.9%): Use IoT devices periodically, maybe for specific tasks. Occasionally (9.7%): Use is infrequent or based on specific needs.

6) Are you concerned about the security of your IoT devices?



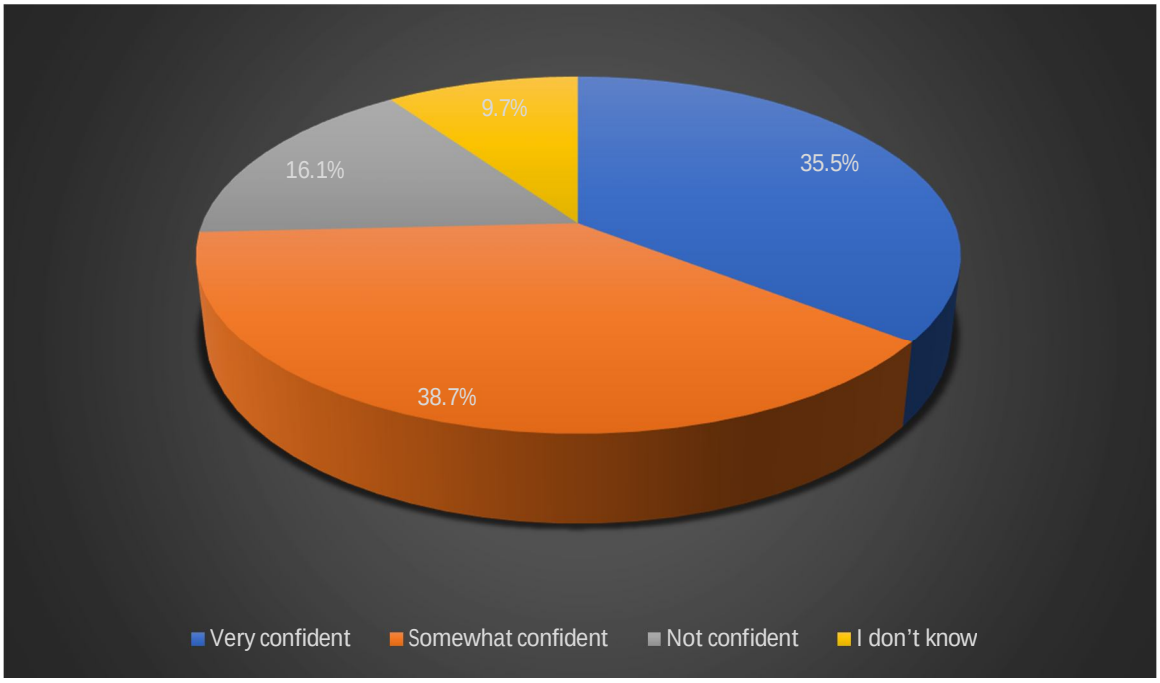
Based on the provided graph details: 48.4% of respondents are very concerned. 32.3% are somewhat concerned. 9.7% are not concerned. 9.7% are not sure.

7) Have you ever faced a security issue (like hacking, data leak, etc.) through an IoT device?



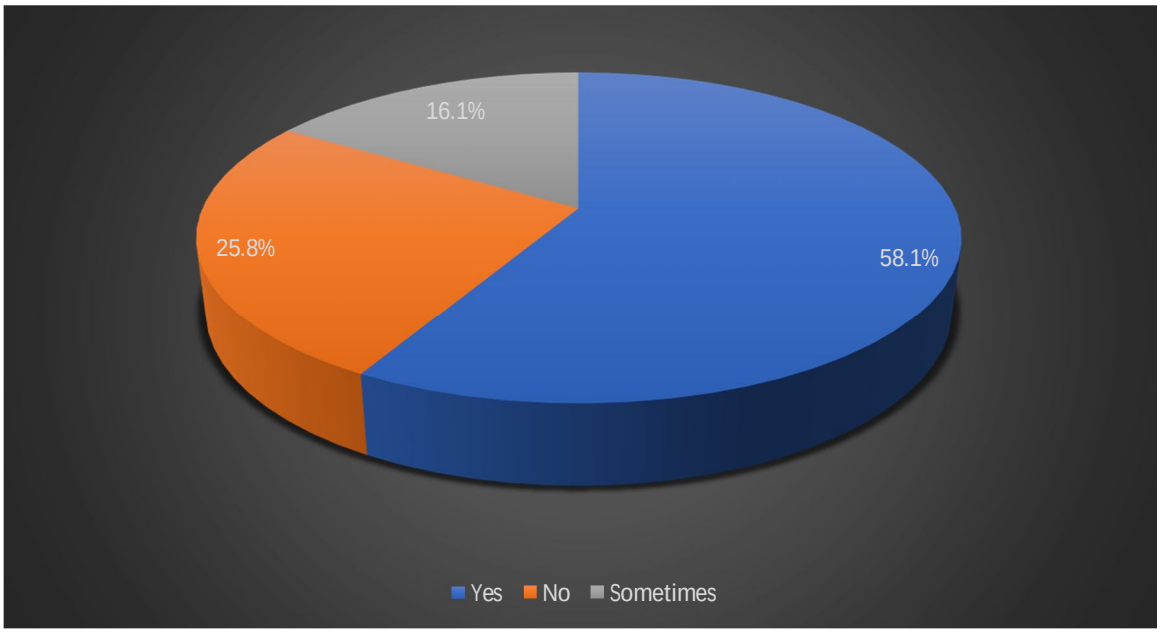
Based on the provided graph details:
70% of respondents answered Yes – they have experienced a security issue. 30% of respondents answered No – they have not experienced such issues.

8) How confident are you about the safety of your personal data on IoT devices?



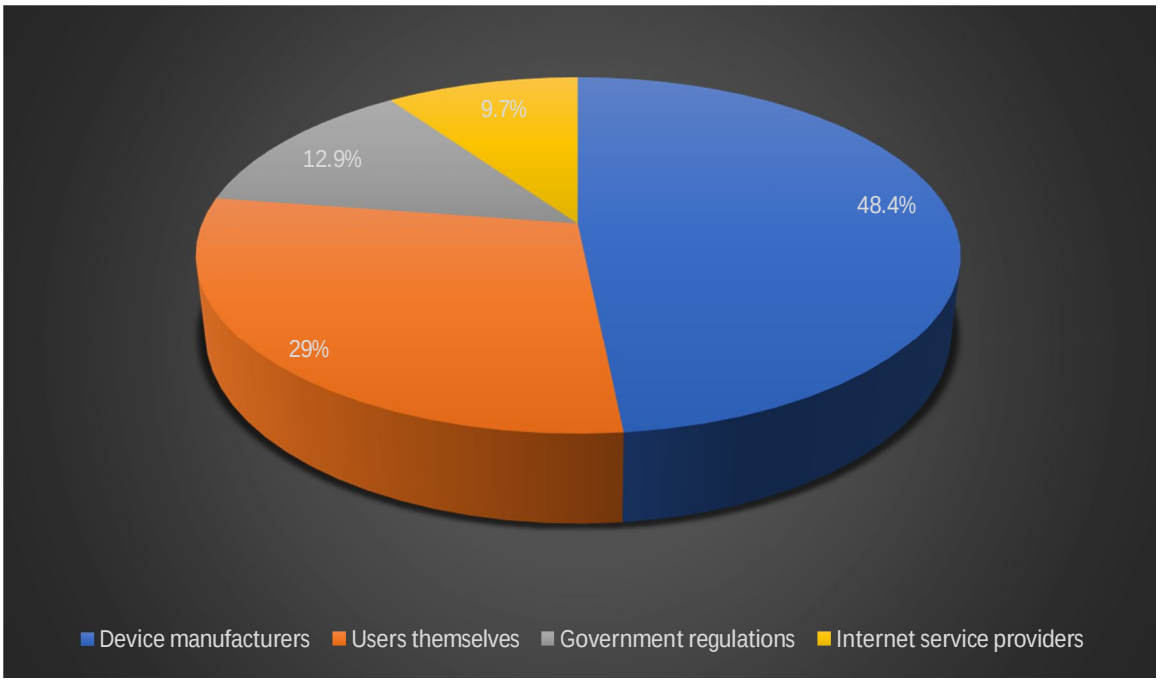
According to the graph shown above:
This includes 38.7% who are somewhat confident and 35.5% who are very confident, suggesting a general trust in the security and reliability of IoT systems.
However, 16.1% of users are not confident, and an additional 9.7% are uncertain

9) Do you regularly update the software/firmware of your IoT devices?



A majority (58.1%) of users regularly update their IoT devices, which is a positive sign for maintaining device security and functionality.
However, 25.8% of respondents do not update their devices, exposing them to potential vulnerabilities and cyber threats due to outdated firmware/software.
The remaining 16.1% update occasionally, suggesting that while they may be aware of the importance, it's not a consistent habit.

10) Who do you think is primarily responsible for IoT security?



Device manufacturers are seen as the primary stakeholders, with nearly half of the respondents (48.4%) placing the responsibility of IoT security on them. This reflects public expectations that security should be built into devices at the design and manufacturing stage. 29% believe users themselves are primarily responsible, showing that a significant portion of respondents recognize the role of user behavior and proper usage in maintaining security.

Only 12.9% trust government regulations, indicating either a lack of confidence in regulatory bodies or a perception that laws alone are insufficient for ensuring security.

Internet service providers (ISPs) received the lowest share at 9.7%, suggesting that the public perceives ISPs as having a minimal role in direct IoT device security.

VIII. MAJOR FINDINGS

This research focuses on the impact of IoT (Internet of Things) technology on cybersecurity and how it's affecting individuals and organizations. It is based on primary data from surveys and interviews as well as secondary data from articles and reports, several major findings were observed:

A. Vulnerabilities IoTs Are Causing Expanding

The study showed that the installation of IoT devices like smart home appliances, fitness trackers, connected vehicles, and industrial IoT devices has widened the scope of cyber threats. Many IoT devices have weak security measures and can be targeted by hackers. Respondents blame default passwords, absence of updates, and poor encryption for IoT devices' lack of adequate security.

B. Gaps in User's Cybersecurity Awareness

Data showed that an alarming number of IoT users do not understand the cyber risks that come with these devices. Prioritizing convenience has made users ignore basic security practices like changing default passwords or updating the device firmware.

This lack of awareness is what has caused the number of IoT-related cyberattacks to increase over the years.

C. Common Cyber Threats in IoT Ecosystem

The list of prominent threats includes:

Unauthorized data access and breaches are becoming increasingly common. The Distributed Denial of Service (DDoS) assaults utilizing IoT botnets.

Misrepresentation and device misuse.
Prying and privacy invasion through surveillance.
Infection through malware transmitted over unsecure IoT networks.
Participants noted the serious implications posed by the compromising of IoT devices which can lead to organizational and personal data breaches.

D. Challenges in Implementing Strong Cybersecurity Measures

As outlined in the findings, improvement in cybersecurity technologies is evident, however the protection of IoT ecosystems remains hard:
Absence of universal security measures set by different manufacturers.
Availability of small sized IoT devices does pose a challenge due to limited computational ability.
Loopholes in systematic maintenance and timely updating and patching of connected devices.
Control over thousands of interconnected devices is expensive to manage and complex to ensure security, as reported by the Organizations.

E. The Role of Regulations and Policies

As discovered during the study, while there is an effort by government and international bodies to create regulations concerning IoT security, their enforcement lacks consistency.
That governance should impose stricter requirements alongside good standards as many respondents agreed in order to serve user protection ensuring design security from the manufacturers enable built-in functionality from the start.

F. User Training and Awareness

The study emphasized the significance of user education on cybersecurity risk reduction.
Respondents were of the opinion that proactive awareness programs, training sessions, and basic security procedures for non-technical users could effectively mitigate the rate of successful cyberattacks on IoT devices.

G. Embracing Sophisticated Security Techniques

Other research findings also suggest that businesses and other organizations are embracing newer technologies to safeguard their IoT networks, which include:
Multi-factor authentication (MFA) Network separation
AI-driven threat detection
Regular vulnerability assessments and penetration testing
The adoption pace, however, is slow for small and medium enterprises (SMEs) due to budgetary limitations.

H. Requirement for Proactive Strategies

As mentioned previously, the research suggests that cybersecurity for IoT ecosystems cannot operate in a reactive paradigm. However, as time goes on, there is developing emphasis towards more proactive approaches such as:
Building security into the hardware layer during initial design steps Performing regular security checkups
Developing timely response procedures for breaches and tailored response strategies for rapid breach mitigation.
Such companies seem to perform better in terms of cyber resiliency as those employing more proactive approaches reported fewer successful cyberattacks than those relying on traditional cyber defense strategies.

IX. CONCLUSION

IoT devices have changed how people, companies, and industries interact with one another through smarter, more integrated solutions. Despite the speed and ease of connecting IoT devices, the resultant potential for cybersecurity breaches is worrying. This research shows IoT devices make cyber threats more convenient, efficient, and varied, undermining growth IoT claims to offer.
The research highlights that a majority of the devices are configured with little to no cybersecurity, opening them up to increased incidences of hacking, data exploitation, and even malware intrusion. The user's ignorance concerning changing basic passwords, updating relevant software, or protecting the network is worrisome. Furthermore, the absence of stringent policies and uniform dictates from IoT industry leaders aggravates the peril of cyber warfare targeting IoT systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Underappreciating the nineth degree of danger stemming from remote devices is another informant's main highlight. Although medium and large organizations are increasingly adopting preventive measures like network segmentation, AI-powered threat monitoring, and regular vulnerability checks to safeguard smaller companies, budget and resource constraints still hinder SMEs.

The research additionally emphasizes the heightened call for an active strategy to IoT security. It is critical that manufacturers implement 'security by design,' guaranteeing robust protective features on devices. Compliance with dire security standard policies must be heightened by the government and regulatory agencies to enforce accountability for cybersecurity requirements. Most critically, users need to be educated about safe IoT practices.

All things considered, as IoT expands and alters life and business activities, its success depends on overcoming its programed cybersecurity issues. Device manufacturers, regulatory bodies, organizations and users themselves all need to combine efforts to strengthen the IoT environment. A unified approach is essential to harness the growth of IoT while maintaining the controls necessary for protecting safety, privacy, and security.

BIBLIOGRAPHY

[1] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

[2] Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. Computer, 44(9), 51–58. https://doi.org/10.1109/MC.2011.291

[3] Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An overview. Internet Society. https://www.internetsociety.org/resources/doc/2015/iot-overview

[4] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[5] Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

[6] Hossain, M. S., Fotouhi, M., & Hasan, R. (2019). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. Proceedings of the IEEE, 107(3), 387–398. https://doi.org/10.1109/JPROC.2019.2893046

[7] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors, 18(9), 2796. https://doi.org/10.3390/s18092796

[8] Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. IEEE Symposium on Security and Privacy (SP), 636–654. https://doi.org/10.1109/SP.2016.44

[9] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20(8), 2481–2501. https://doi.org/10.1007/s11276-014-0761-7

[10] SecurityToday. (2022). The Growing Importance of IoT Security. https://securitytoday.com/articles/2022/03/01/the-growing-importance-of-iot- security.aspx

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Annexure

1) What is your gender?
a) Male
b) Female
c) Others

2) What is your Occupation
a) Student
b) IT Professional
c) Business Owner
d) Others

3) Are you aware of the Internet of Things (IoT)?
a) Yes
b) No

4) Which IoT devices do you currently use?
a) Smartwatch
b) Smart Home Devices (Alexa, Google Home, etc.)
c) Smart TV
d) Connected Cars
e) Health Monitoring Devices
f) Others

5) How often do you use IoT devices?
a) Daily
b) Weekly
c) Occasionally
d) Rarely

6) Are you concerned about the security of your IoT devices?
a) Very concerned
b) Somewhat concerned
c) Not concerned
d) Not sure

7) Have you ever faced a security issue (like hacking, data leak, etc.) through an IoT device?
a) Yes
b) No

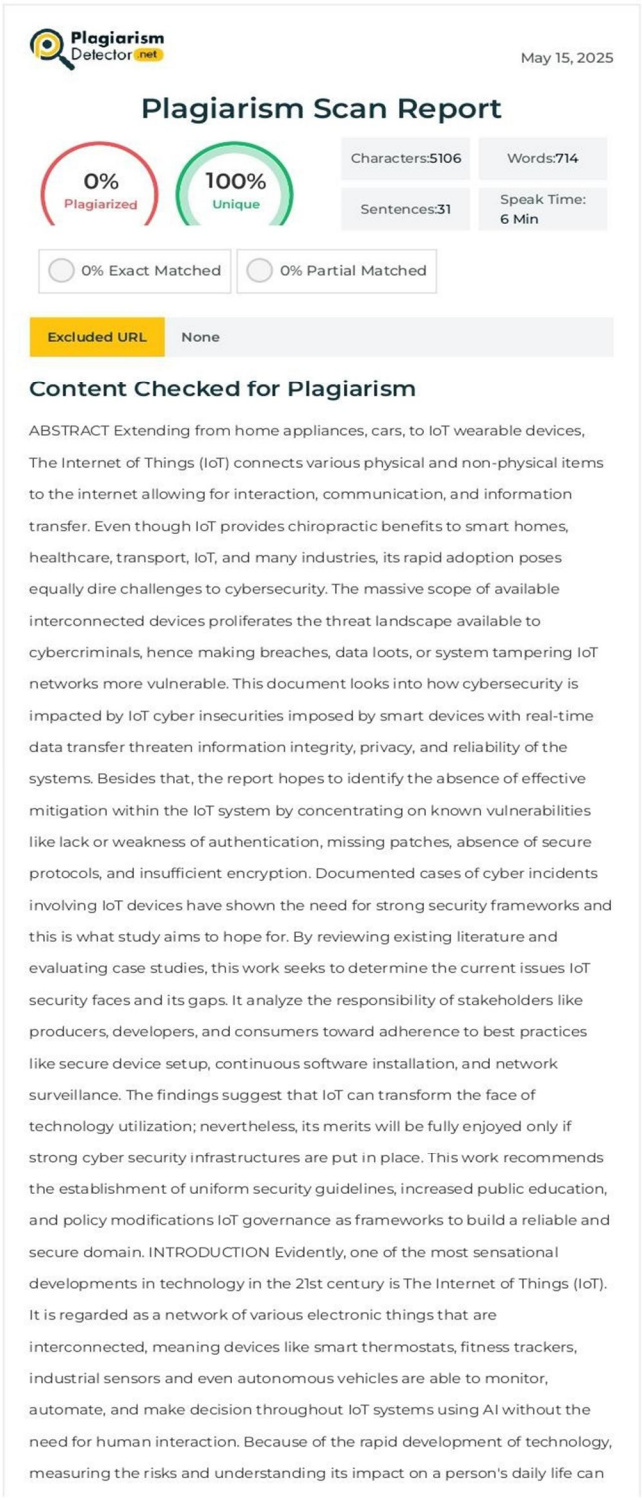
8) How confident are you about the safety of your personal data on IoT devices?
a) Very confident
b) Somewhat confident
c) Not confident
d) I don't know

9) Do you regularly update the software/firmware of your IoT devices?
a) Yes
b) No
c) Sometimes

©IJRASET: All Rights are Reserved

10) Who do you think is primarily responsible for IoT security?

a) Device manufacturers
b) Users themselves
c) Government regulations
d) Internet service providers



Plagiarism Detector .net

May 15, 2025

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:5106 | Words:714

Sentences:31 | Speak Time: 6 Min

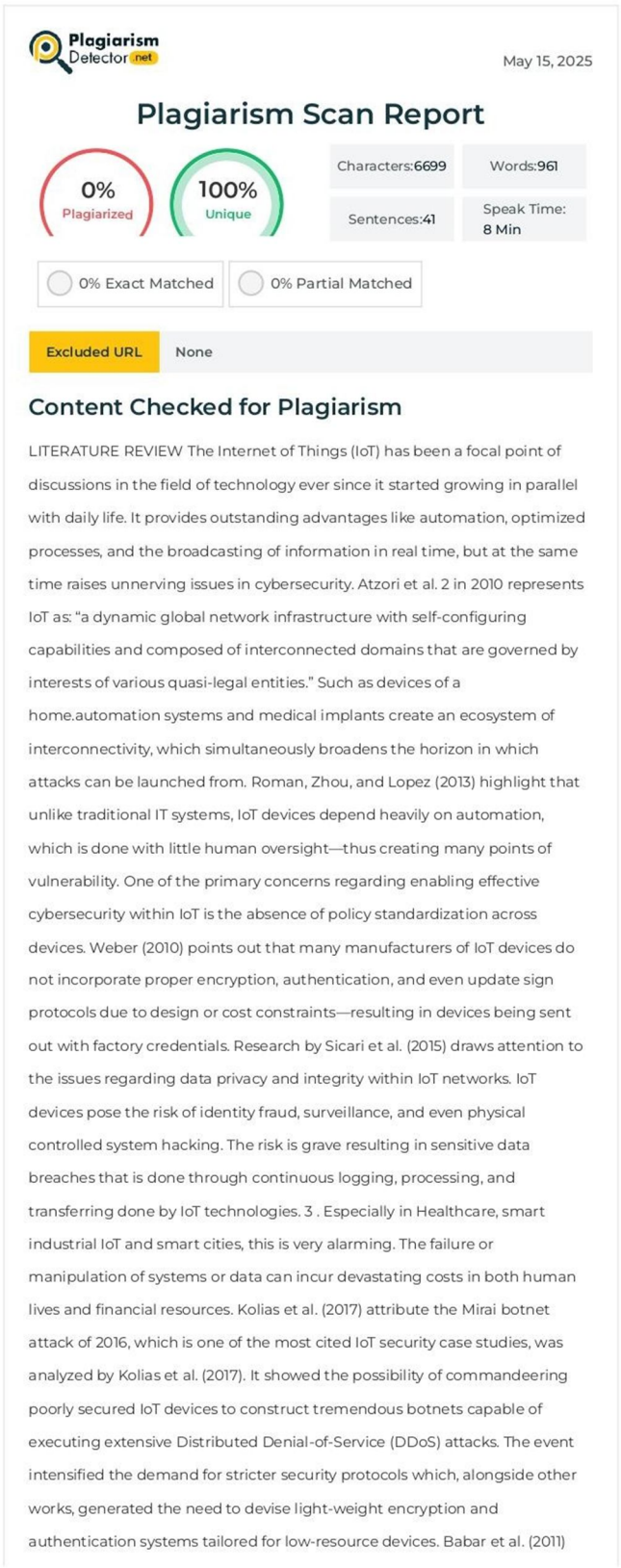
0% Exact Matched | 0% Partial Matched

Excluded URL: None

Content Checked for Plagiarism

ABSTRACT Extending from home appliances, cars, to IoT wearable devices, The Internet of Things (IoT) connects various physical and non-physical items to the internet allowing for interaction, communication, and information transfer. Even though IoT provides chiropractic benefits to smart homes, healthcare, transport, IoT, and many industries, its rapid adoption poses equally dire challenges to cybersecurity. The massive scope of available interconnected devices proliferates the threat landscape available to cybercriminals, hence making breaches, data loots, or system tampering IoT networks more vulnerable. This document looks into how cybersecurity is impacted by IoT cyber insecurities imposed by smart devices with real-time data transfer threaten information integrity, privacy, and reliability of the systems. Besides that, the report hopes to identify the absence of effective mitigation within the IoT system by concentrating on known vulnerabilities like lack or weakness of authentication, missing patches, absence of secure protocols, and insufficient encryption. Documented cases of cyber incidents involving IoT devices have shown the need for strong security frameworks and this is what study aims to hope for. By reviewing existing literature and evaluating case studies, this work seeks to determine the current issues IoT security faces and its gaps. It analyze the responsibility of stakeholders like producers, developers, and consumers toward adherence to best practices like secure device setup, continuous software installation, and network surveillance. The findings suggest that IoT can transform the face of technology utilization; nevertheless, its merits will be fully enjoyed only if strong cyber security infrastructures are put in place. This work recommends the establishment of uniform security guidelines, increased public education, and policy modifications IoT governance as frameworks to build a reliable and secure domain. INTRODUCTION Evidently, one of the most sensational developments in technology in the 21st century is The Internet of Things (IoT). It is regarded as a network of various electronic things that are interconnected, meaning devices like smart thermostats, fitness trackers, industrial sensors and even autonomous vehicles are able to monitor, automate, and make decision throughout IoT systems using AI without the need for human interaction. Because of the rapid development of technology, measuring the risks and understanding its impact on a person's daily life can

Page 1 of 2



Plagiarism Detector.net

May 15, 2025

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:6699

Words:961

Sentences:41

Speak Time: 8 Min

0% Exact Matched

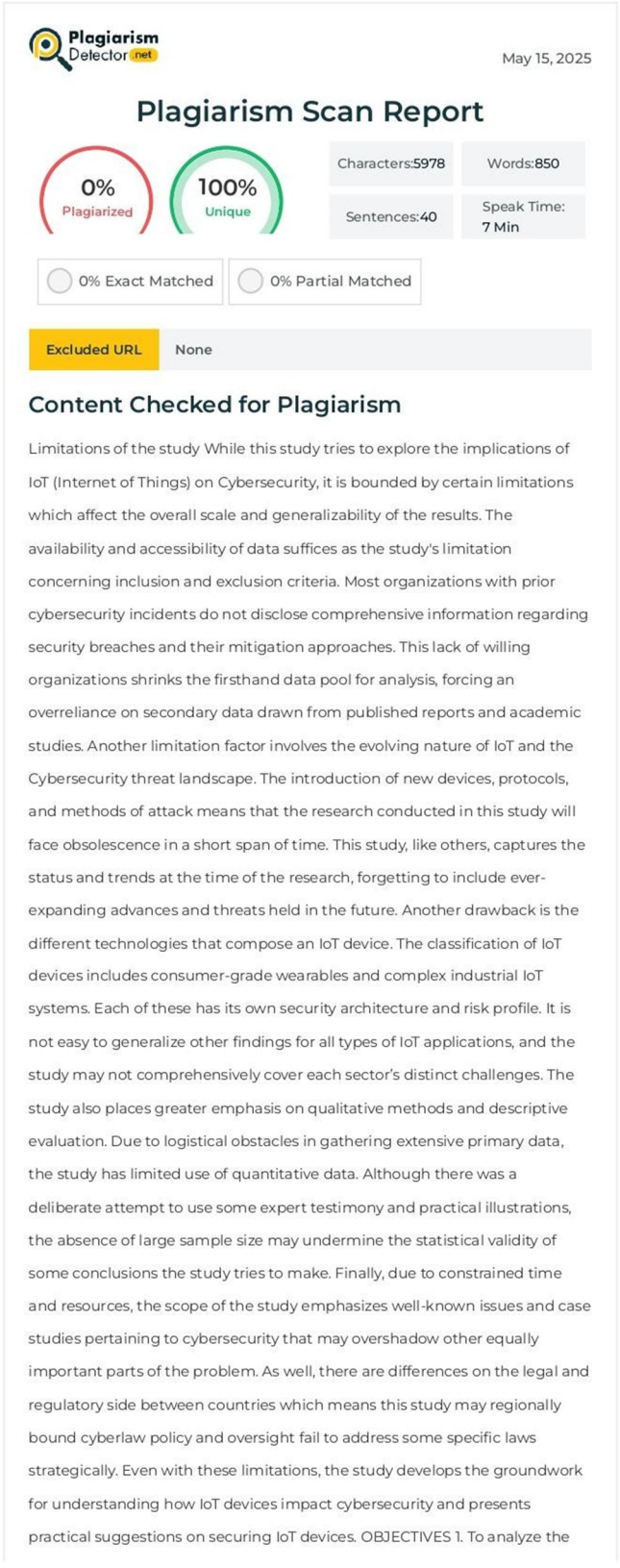
0% Partial Matched

Excluded URL: None

Content Checked for Plagiarism

LITERATURE REVIEW The Internet of Things (IoT) has been a focal point of discussions in the field of technology ever since it started growing in parallel with daily life. It provides outstanding advantages like automation, optimized processes, and the broadcasting of information in real time, but at the same time raises unnerving issues in cybersecurity. Atzori et al. 2 in 2010 represents IoT as: "a dynamic global network infrastructure with self-configuring capabilities and composed of interconnected domains that are governed by interests of various quasi-legal entities." Such as devices of a home.automation systems and medical implants create an ecosystem of interconnectivity, which simultaneously broadens the horizon in which attacks can be launched from. Roman, Zhou, and Lopez (2013) highlight that unlike traditional IT systems, IoT devices depend heavily on automation, which is done with little human oversight—thus creating many points of vulnerability. One of the primary concerns regarding enabling effective cybersecurity within IoT is the absence of policy standardization across devices. Weber (2010) points out that many manufacturers of IoT devices do not incorporate proper encryption, authentication, and even update sign protocols due to design or cost constraints—resulting in devices being sent out with factory credentials. Research by Sicari et al. (2015) draws attention to the issues regarding data privacy and integrity within IoT networks. IoT devices pose the risk of identity fraud, surveillance, and even physical controlled system hacking. The risk is grave resulting in sensitive data breaches that is done through continuous logging, processing, and transferring done by IoT technologies. 3 . Especially in Healthcare, smart industrial IoT and smart cities, this is very alarming. The failure or manipulation of systems or data can incur devastating costs in both human lives and financial resources. Kolias et al. (2017) attribute the Mirai botnet attack of 2016, which is one of the most cited IoT security case studies, was analyzed by Kolias et al. (2017). It showed the possibility of commandeering poorly secured IoT devices to construct tremendous botnets capable of executing extensive Distributed Denial-of-Service (DDoS) attacks. The event intensified the demand for stricter security protocols which, alongside other works, generated the need to devise light-weight encryption and authentication systems tailored for low-resource devices. Babar et al. (2011)

Page 1 of 3



Plagiarism Detector .net

May 15, 2025

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:5978

Words:850

Sentences:40

Speak Time: 7 Min

0% Exact Matched

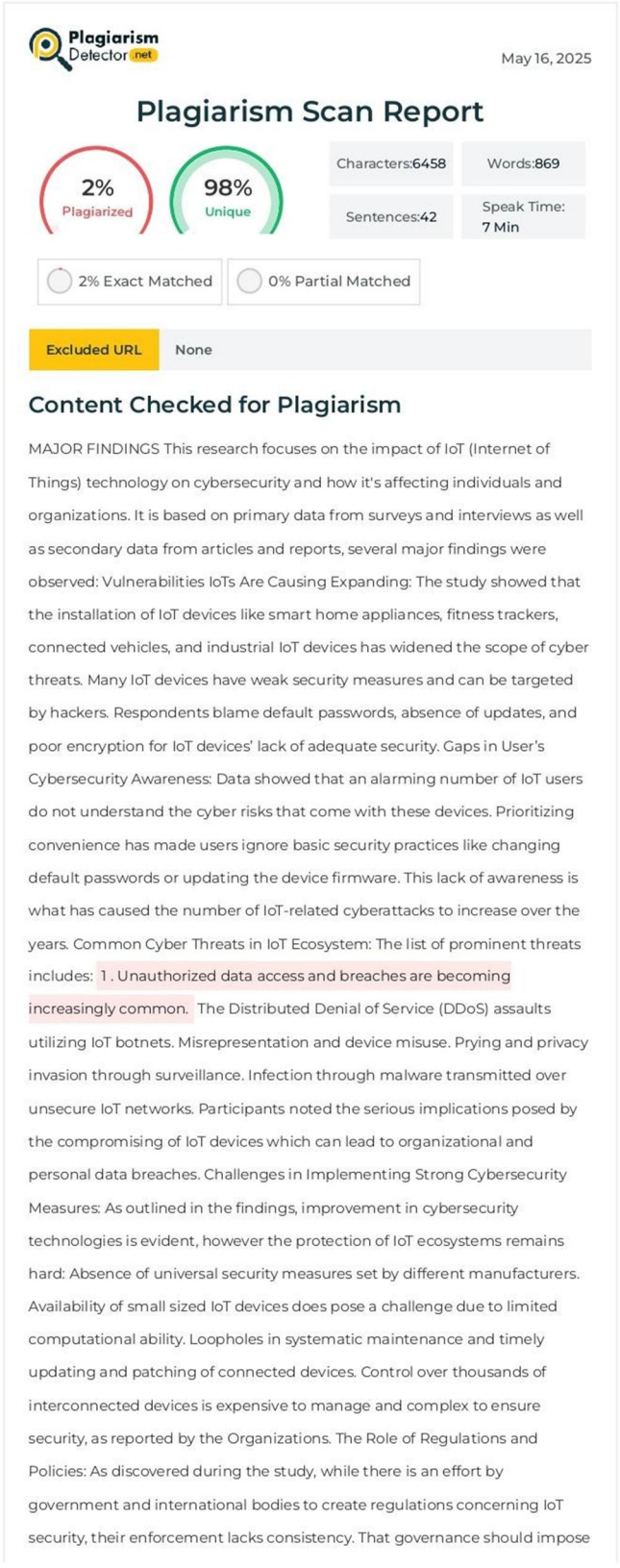
0% Partial Matched

Excluded URL None

Content Checked for Plagiarism

Limitations of the study While this study tries to explore the implications of IoT (Internet of Things) on Cybersecurity, it is bounded by certain limitations which affect the overall scale and generalizability of the results. The availability and accessibility of data suffices as the study's limitation concerning inclusion and exclusion criteria. Most organizations with prior cybersecurity incidents do not disclose comprehensive information regarding security breaches and their mitigation approaches. This lack of willing organizations shrinks the firsthand data pool for analysis, forcing an overreliance on secondary data drawn from published reports and academic studies. Another limitation factor involves the evolving nature of IoT and the Cybersecurity threat landscape. The introduction of new devices, protocols, and methods of attack means that the research conducted in this study will face obsolescence in a short span of time. This study, like others, captures the status and trends at the time of the research, forgetting to include ever-expanding advances and threats held in the future. Another drawback is the different technologies that compose an IoT device. The classification of IoT devices includes consumer-grade wearables and complex industrial IoT systems. Each of these has its own security architecture and risk profile. It is not easy to generalize other findings for all types of IoT applications, and the study may not comprehensively cover each sector's distinct challenges. The study also places greater emphasis on qualitative methods and descriptive evaluation. Due to logistical obstacles in gathering extensive primary data, the study has limited use of quantitative data. Although there was a deliberate attempt to use some expert testimony and practical illustrations, the absence of large sample size may undermine the statistical validity of some conclusions the study tries to make. Finally, due to constrained time and resources, the scope of the study emphasizes well-known issues and case studies pertaining to cybersecurity that may overshadow other equally important parts of the problem. As well, there are differences on the legal and regulatory side between countries which means this study may regionally bound cyberlaw policy and oversight fail to address some specific laws strategically. Even with these limitations, the study develops the groundwork for understanding how IoT devices impact cybersecurity and presents practical suggestions on securing IoT devices. OBJECTIVES 1. To analyze the

Page 1 of 3



Plagiarism Detector .net

May 16, 2025

Plagiarism Scan Report

2% Plagiarized	98% Unique	Characters:6458	Words:869
		Sentences:42	Speak Time: 7 Min

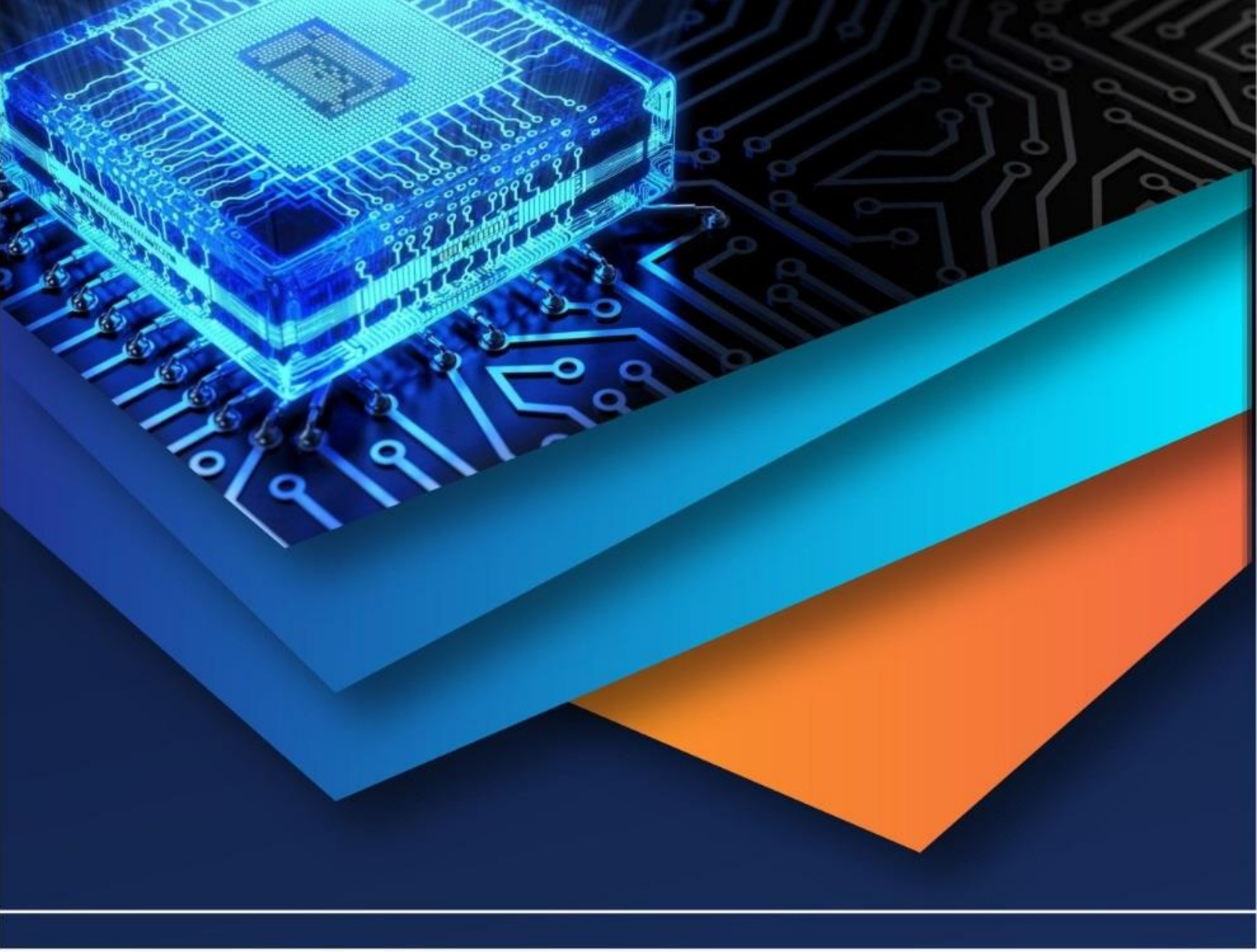
2% Exact Matched | 0% Partial Matched

Excluded URL: None

Content Checked for Plagiarism

MAJOR FINDINGS This research focuses on the impact of IoT (Internet of Things) technology on cybersecurity and how it's affecting individuals and organizations. It is based on primary data from surveys and interviews as well as secondary data from articles and reports, several major findings were observed: Vulnerabilities IoTs Are Causing Expanding: The study showed that the installation of IoT devices like smart home appliances, fitness trackers, connected vehicles, and industrial IoT devices has widened the scope of cyber threats. Many IoT devices have weak security measures and can be targeted by hackers. Respondents blame default passwords, absence of updates, and poor encryption for IoT devices' lack of adequate security. Gaps in User's Cybersecurity Awareness: Data showed that an alarming number of IoT users do not understand the cyber risks that come with these devices. Prioritizing convenience has made users ignore basic security practices like changing default passwords or updating the device firmware. This lack of awareness is what has caused the number of IoT-related cyberattacks to increase over the years. Common Cyber Threats in IoT Ecosystem: The list of prominent threats includes: 1. Unauthorized data access and breaches are becoming increasingly common. The Distributed Denial of Service (DDoS) assaults utilizing IoT botnets. Misrepresentation and device misuse. Prying and privacy invasion through surveillance. Infection through malware transmitted over unsecure IoT networks. Participants noted the serious implications posed by the compromising of IoT devices which can lead to organizational and personal data breaches. Challenges in Implementing Strong Cybersecurity Measures: As outlined in the findings, improvement in cybersecurity technologies is evident, however the protection of IoT ecosystems remains hard: Absence of universal security measures set by different manufacturers. Availability of small sized IoT devices does pose a challenge due to limited computational ability. Loopholes in systematic maintenance and timely updating and patching of connected devices. Control over thousands of interconnected devices is expensive to manage and complex to ensure security, as reported by the Organizations. The Role of Regulations and Policies: As discovered during the study, while there is an effort by government and international bodies to create regulations concerning IoT security, their enforcement lacks consistency. That governance should impose

Page 1 of 3



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)