JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybersecurity In Internet Of Things

[1]Tanisha Vichare, [2]Sejal Vishwakarma, [3]Sneha Gokarnkar

[1]Student at Sheth L.U.Jhaveri. and Sir M.V. College of Arts, Science, and Commerce, [2]Student at Sheth L.U.Jhaveri. and Sir M.V. College of Arts, Science, and Commerce, [3]Asst. Professor at Sheth L.U.Jhaveri. and Sir M.V. College of Arts, Science, and Commerce

Abstract: This paper reviews IoT cybersecurity technologies and cyber risk management frameworks, then presents a four-layer IoT cyber risk management framework, and finally, it applies a linear programming method for the allocation of financial resources to multiple IoT cybersecurity projects. This paper's goal is to reduce cybersecurity risk for organizations and users by protecting IoT assets and privacy. As the threat of cyberattacks continues to grow, cybersecurity has emerged as one of the most important areas of the Internet of Things.

IndexTerms - **Internet of Things; cybersecurity; risk management; linear programming; IT assets; cyberattack; vulnerabilities; cyber threat; risk assessment**

I. INTRODUCTION

Cybersecurity is the process of protecting networks, computers, and data from assaults and unwanted access. Think of it like securing your home's windows and doors to keep intruders out, but with digital technologies instead. Protecting our information from cybercriminals who could steal data, hurt us, or interfere with services is essential given the rise in both personal and professional activities conducted online.

Cybersecurity and the Internet of Things have become even more relevant in modern times. Few decades earlier Cyber Security and the Internet of Things were considered as separate disciplines. They were not studied together. Things have changed drastically over the years and Cybersecurity and Internet of Things have become one of the most studied topics in industry as well as academia. Cybersecurity primarily revolves around the phenomenon of protecting systems, software and various other computers from attacks on the connected as well as standalone networks.

This enables systems to be run securely on any compute environment such as data centres, personal computers, mobile phones and IoT devices. Internet of Things is the science of connecting all possible devices with the internet. When a machine or a computer is said to have Internet of Things technology, it implies that the machine can be controlled or monitored by sitting anywhere in the world. It usually has abilities such as monitoring, alarms and recording previously unknown problems to the system.

1.1 Literature Review

Yang Lu and Li Da Xu talks about the ways in which Internet of Things devices will transform the worldwide network of connected devices. It also demonstrates how the Internet of Things' technological advancements are still in their early stages. There are a number of problems with this technology that need to be resolved, it says. Then it goes into greater detail on the primary problem, security, which is the largest danger facing the Internet of Things. It looks at how cybersecurity can be applied to IoT devices in different ways. In terms of security, the article specifically stresses the integration and protection of diverse connected devices and the technologies that are utilized for communication with those devices.

In Lee(2020) specifies Since safe data transfer across the network is necessary for the operation of devices, processing stations, and the complete Internet of Things system, the network layer is crucial to the system's overall security performance. To identify attacks, take remedial action, and keep an eye on packets, an intrusion detection system (IDS) is employed. The intrusion detection system (IDS) uses statistics to identify anomalies, an evolutionary algorithm to classify intrusions based on behavior, error conditions, and attempted intrusions, protocol verification to classify suspicious behavior, and data mining techniques like deep learning and the random forest method to classify patterns of network breaches.

Roberto Omar Andrade describes IoT services are provided through network protocols like DNS, HTTP, and MQTT. Attackers attempt to take advantage of flaws in these protocols by employing methods like polymorphic code, DNS spoofing, DNS cache poisoning, Denial of Service (DoS), Distributed DoS (DDoS), and URL interpretation. Attackers can generate shellcodes or download script files with commands after successfully logging in via Telnet. Furthermore, IoT solutions take into account UPnP for automatically identifying IoT devices that are linked to a network. However, this service may become vulnerable since an attacker might obtain critical information by using the UPnP service discovery protocol.

Thanaa saad Alsalem(2023) says That covered the ongoing state of the Internet of Things and its problems. The research paper's primary objective was to provide an overview of security standards, difficult problems, and upcoming trends in IoT security. The methodology employed by the authors was primarily centered on a review of relevant literature. Its findings demonstrated that authentication, access, and control methods were the focus of contemporary IoT research.

Objectives of the Study

- **Good Security Practices:** Using measures like strong passwords, firewalls, encryption, and frequent software updates helps protect digital systems and networks from unauthorized access and cyberattacks.

- **Alertness and Awareness:** Cybersecurity guidelines and staying vigilant when browsing, one can significantly reduce cyberthreats and protect personal information and electronic gadgets.

Hypothesis H0: There is an anomaly or intrusion affecting the Cybersecurity In IOT.
Hypothesis H1: The Cybersecurity In IOT is operating normally without any intrusions or anomalies.

1.2 Scope

IoT cyber security is a field of technology focused on safeguarding networks and connected devices inside the Internet of Things. In the Internet of Things, a network of networked computers, digital and mechanical equipment, objects, animals, and people are connected to the Internet. With more and more devices becoming connected, cybersecurity in the Internet of Things is tackling a wide variety of problems and potential solutions. It includes safeguarding Internet of Things devices and networks from a range of dangers, such as cyberattacks, data breaches, and illegal access. Ensuring reliable firmware upgrades, protecting device authentication and authorization, and preserving the security and integrity of data transferred across devices are important areas of concern.

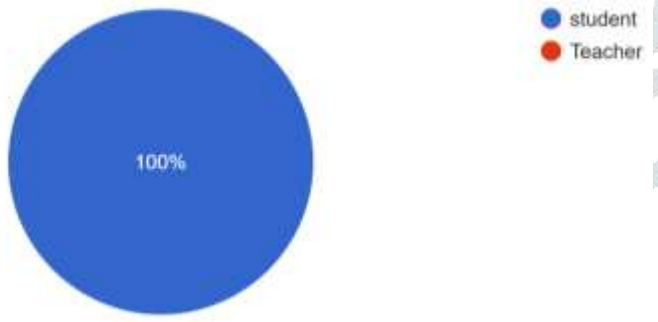
RESEARCH METHODOLOGY

2.1 Data Collection

This study uses primary data acquired through a questionnaire taken by people from across the Mumbai Maharashtra. The data is examined using the chi-square test.

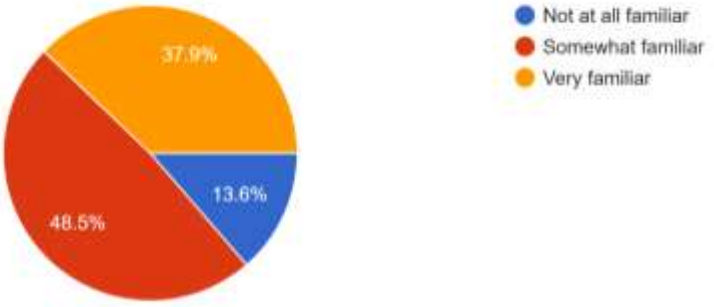
2.2 Data Analysis and Interpretation

Figure 1:- Role in Education of Respondents.



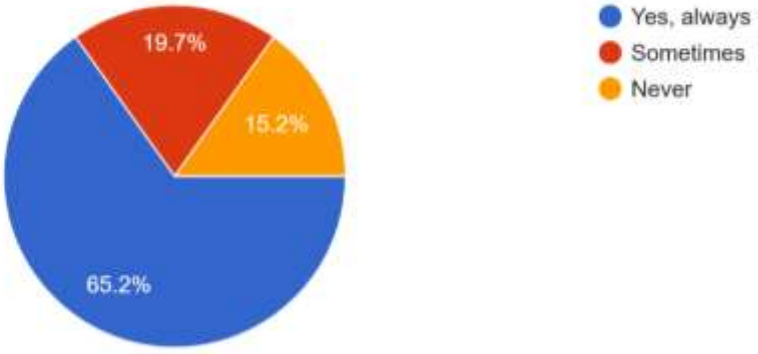
Out of 66 responses, above graph depicts that the maximum number of respondents are students who use cybersecurity IOT devices Based Tools in their day-to-day life.

Figure 2. Familiar with IOT devices of Respondents.



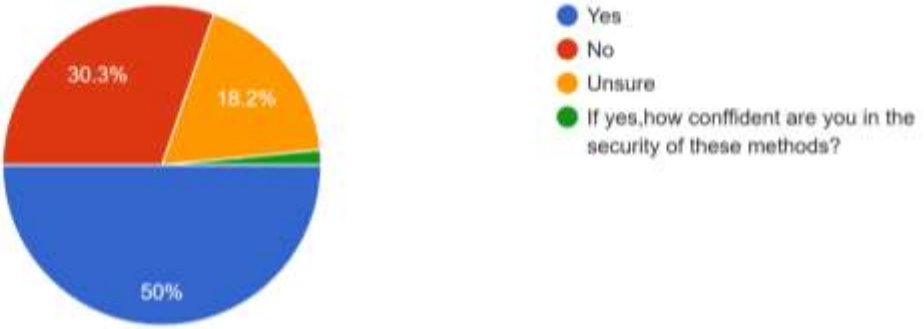
The above pie chart demonstrates the level of familiarity among 66 response with the cyber security in the context of the IOT.

Figure.3 The password of IOT devices of Respondents.



The above chart states that the user uses the unique and strong passwords for their IOT devices that can protected from hackers with 65 % of response.

Figure.4 IOT devices that require authentication of the Respondents.



50% of above graph responds that requires physical Access that is physically present to operate or access the device or biometric authentication like fingerprint or facial recognition for security purpose.

I. RESULTS AND DISCUSSION

3.1 Chi-square test

The Chi-squared test assists in establishing whether there is a relationship between security-related variables in IoT, such as device types or security settings, and the incidence of cybersecurity including attacks.it examines whether specific devices or security configurations are more likely have security problems.

Formula:

Chi-square (χ 2) Test in r x c Contingency Table = $\sum i \sum j ((Oij - Eij) ^2 / Eij)$

Where: **O =Observed values, E = Expected values**

Table 1: Observed Values of respondents who are familiar with Cybersecurity in IOT.

Responses	Not at all familiar	Somewhat familiar	Very familiar	Total
Negative	0	2	3	5
Sometimes	0	1	1	2
Yes	0	1	1	2
Yes, always	0	1	1	2
Yes,always	0	1	2	3
Yes	0	1	2	3
Sometimes	0	0	1	1
Yes, always	0	1	1	2
Neutral	2	15	6	23
Never	2	0	0	2
No	2	0	0	2
Never	1	0	0	1
Sometimes	1	0	0	1
Sometimes	0	12	4	16
No	0	3	0	3
Never	0	1	0	1
Yes, always	0	2	0	2
Yes	0	9	4	13
Never	0	1	0	1
Sometimes	0	3	1	4
Yes, always	0	5	3	8

Yes, always	0	3	2	5
No	0	1	1	2
Yes, always	0	1	1	2
Yes	0	2	1	3
Yes, always	0	2	1	3
Positive	5	14	13	32
Never	3	1	1	5
No	1	0	1	2
Never	1	0	1	2
Yes	2	1	0	3
Never	2	1	0	3
Sometimes	0	5	7	12
No	0	0	2	2
Yes, always	0	0	2	2
Yes	0	5	5	10
Sometimes	0	1	1	2
Yes, always	0	4	4	8
Yes,always	2	8	5	15
Yes	2	8	5	15
Sometimes	0	1	0	1
Yes, always	2	7	5	14
Unsure	2	1	3	6
Never	1	0	1	2
No	1	0	1	2
Never	1	0	1	2
Sometimes	1	1	1	3
No	0	0	1	1
Sometimes	0	0	1	1
Yes	1	1	0	2
Sometimes	1	1	0	2
Yes,always	0	0	1	1
No	0	0	1	1
Sometimes	0	0	1	1
Column total	**9**	**32**	**25**	**66**

Expected Value = (Row Total * Column Total) / Grand Total
Table 2: Expected Values

Responses	Not at all familiar	Somewhat familiar	Very familiar
Negative	0	2.424242424	1.136363636
Sometimes	0	0.96969697	0.757575758
Yes	0	0.96969697	0.757575758
Yes, always	0	0.96969697	0.757575758
Yes,always	0	1.454545455	1.136363636
Yes	0	1.454545455	1.136363636
Sometimes	0	0	0.378787879
Yes, always	0	0.96969697	0.757575758
Neutral	3.136363636	11.15151515	8.712121212
Never	0.272727273	0	0
No	0.272727273	0	0
Never	0.136363636	0	0
Sometimes	0.136363636	0	0
Sometimes	0	7.757575758	6.060606061
No	0	1.454545455	0
Never	0	0.484848485	0
Yes, always	0	0.96969697	0
Yes	0	6.303030303	4.924242424
Never	0	0.484848485	0
Sometimes	0	1.939393939	1.515151515
Yes, always	0	3.878787879	3.03030303
Yes,always	0	49.77272727	1.893939394
No	0	0.96969697	0.757575758
Yes, always	0	0.96969697	0.757575758
Yes	0	1.454545455	1.136363636
Yes, always	0	1.454545455	1.136363636
Positive	4.363636364	15.51515152	12.12121212
Never	0.681818182	2.424242424	1.893939394
No	0.272727273	0	0.757575758
Never	0.272727273	0	0.757575758

Table 3: Calculating ((Oij – Eij) ^2/Eij)

Responses	Not at all familiar	Somewhat familiar	Very familiar
Negative	0	0.4929258895	2.991132625
Sometimes	0	0.0007380146774	0.02372907256
Yes	0	0.0007380146774	0.02372907256
Yes, always	0	0.0007380146774	0.02372907256
Yes,always	0	0.000738014677	0.7725781467
Yes	0	0.000738014677	0.7725781467
Sometimes	0	0	0.08096676431
Yes, always	0	0.000738014677	0.02372907256
Neutral	2.072820851	1.273416433	1.257397802
Never	55.03598151	0	0
No	55.03598151	0	0
Never	0.1164626931	0	0
Sometimes	0.1164626931	0	0
Sometimes	0	1.451465639	1.269458012
No	0	1.81950111	0
Never	0	0.06482339889	0
Yes, always	0	1.063506786	0
Yes	0	1.369999127	0.968509336
Never	0	0.06482339889	0
Sometimes	0	1.062558061	0.416633489
Yes, always	0	1.060767643	0.09949031357
Yes,always	0	1.167091025	0.09353736562
No	0	0.0007380146774	0.02372907256
Yes, always	0	0.0007380146774	0.02372907256
Yes	0	0.4345532749	0.2999642444
Yes, always	0	0.4345532749	0.2999642444
Positive	0.8128897005	32.39058574	0.9789057276
Never	11.77875313	1.338772344	0.79912764

No	0.09677879569	0	0.02372907256
Never	0.09677879569	0	0.02372907256
Yes	9.678805826	0.3381962704	0
Never	9.678805826	0.3381962704	0
Sometimes	0	0.933344832	1.484524176
No	0	0	1.77366902
Yes, always	0	0	1.77366902
Yes	0	0.4591325961	1.106910011
Sometimes	0	0.0007380146774	0.02372907256
Yes, always	0	0.3368630937	0.9798955499
Yes,always	2.045454545	0.916150363	0.8738790735
Yes	2.045454545	0.916150363	0.8738790735
Sometimes	0	0.06482339889	0
Yes, always	1.909090909	0.6332611062	0.6374500672
Unsure	0.8181818182	1.559797766	0.7556029166
Never	0.2727272727	0	0.02372907256
No	0.2727272727	0	0.02372907256
Never	0.2727272727	0	0.02372907256
Sometimes	0.4090909091	0.3381962704	0.0299964244
No	0.1363636364	0.06482339889	0.08096676431
Sometimes	0.1363636364	0	0.08096676431
Yes	0.2727272727	0.0007380146774	0
Sometimes	0.2727272727	0.0007380146774	0
Yes,always	0	0	0.08096676431
No	0	0	0.08096676431
Sometimes	0	0	0.08096676431

Calculating the summation of values of **((Oij – Eij) ^2/Eij),** to derive value of χ^2

$\sum i \sum j ((O_{ij} - E_{ij}$ ^2 /$E_{ij}) =$ **162.3841577**

To test the hypothesis at 0.05 level of significance, deduce the p-value using the formula:
p-value = CHISQ.DIST. RT(χ^2,Degree of Freedom)

Where Degree of Freedom = (Total number of rows – 1) * (Total number of Columns – 1) Degree of Freedom = 100

Therefore,
p-value = CHISQ.DIST.RT(162.3841577,100)

p-value = 0.008032881026

II. FINDINGS

Calculated p-value becomes less than the acceptance level of significance at 0.05, hence rejecting the null hypothesis and accepting the alternative hypothesis at a 0.05 level of significance.

III. CONCLUSION

The study shows that there are particular security issues because of the variety of IoT devices. It is challenging to put in place a unified cybersecurity strategy because these devices are made by multiple manufacturers, each of which has their own security standards and procedures. Cybercriminals may be able to take advantage of vulnerabilities caused by disparities in security measures between devices. Certain gadgets, for instance, might not have firmware that is up to date or support encryption, making them vulnerable to assaults. In addition to making it more difficult to secure IoT networks, this lack of consistency in security procedures raises the possibility of broad breaches because one weak item might jeopardize an entire system. Risks to data privacy are yet another important issue raised by the study. IoT devices gather enormous volumes of sensitive and personal data, which, if improperly secured, may be subject to unwanted access. If this data is transmitted over the internet without sufficient encryption, it may be intercepted by hostile actors. For example, the disclosure of private data might have serious repercussions in industries like healthcare, where IoT devices track patient health.

IV. SUGGESTION

In order to improve cybersecurity in the Internet of Things (IoT) setting, a multifaceted strategy is necessary. To start, when designing and developing IoT devices, manufacturers should give top priority to strict security standards. To avoid weaknesses, they should use safe coding techniques and reliable authentication methods. Users should also be made aware of the dangers posed by IoT devices; thorough training courses can enable people to identify dangers and take precautions like updating software and changing default passwords. Furthermore, without requiring user intervention, automated software upgrades can guarantee that devices receive crucial security patches.

1. **Authentication and Authorization of Devices**

   Before permitting devices to join to the network, be sure that strong authentication procedures are in place to confirm their identity. To limit access according to user roles and device capability, put in place the appropriate authorization controls.

2. **Strong Password Guidelines**

   Encourage people to update their default login credentials and establish strong password regulations. Make sure every system or device has a strong, one-of-a-kind password.

3. **Keeping an eye on and recording**

   Keep an eye on IoT devices for any odd activity. Logging should be used to monitor network traffic and device activities in order to promptly identify and address any suspicious activity.

4. **Protection of the Supply Chain**

   Examine the security stance of suppliers and manufacturers of IoT devices to make sure they are safe both during production and transit. Keep third-party risks in mind.

5. **Monitoring and Logging**

   Continuously monitor IoT devices for unusual activity. Implement logging to track device actions and network traffic to help detect and respond to suspicious behavior quickly.

6. **Data Encryption**

   Encrypt sensitive data both in transit and at rest to prevent unauthorized interception and data breaches. Use secure protocols like TLS/SSL for communication between devices and servers

V. REFERENCES

1] In Lee (21 July 2020) Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management
https://www.researchgate.net/publication/345207580_Internet_of_Things_IoT_Cybersecurity_Literature_Review_and_IoT_Cyber_Risk_Management

2] Swapnil Suraj(14 may 2021) Cyber Security and Internet of Things
https://www.researchgate.net/publication/351576013

3] Parsam Dinesh Babu:Computer science and Engineering Saveetha Engineering College, Anna University, Chennai, India
C Eswara Naidu: Electronics and Communication Engineering Saveetha Engineering College, Anna University, Chennai, India
Published in: 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)

4) Cybersecurity Analysis and Future Research Directions for the Internet of Things:
Submission received: 28 February 2023 / Revised: 4 April 2023 / Accepted: 14 April 2023 / Published: 19 April 2023 https://doi.org/10.3390/s23084117.

5) Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation
by Aaron Echeverria, Cristhian Cevallos
Submission received: 15 February 2021 / Revised: 3 March 2021 / Accepted: 5 March 2021 / Published: 6 April 2021
https://doi.org/10.3390/app11073260