IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY IN THE AGE OF INTERNET OF THINGS

PRANAV SRIVASTAVA (1210212040)

PAWAN KUMAR (1210212038)

ANAND CHAUHAN (1210212012)

Masters of Computer Application 2nd Year

(School Of Computer Application)

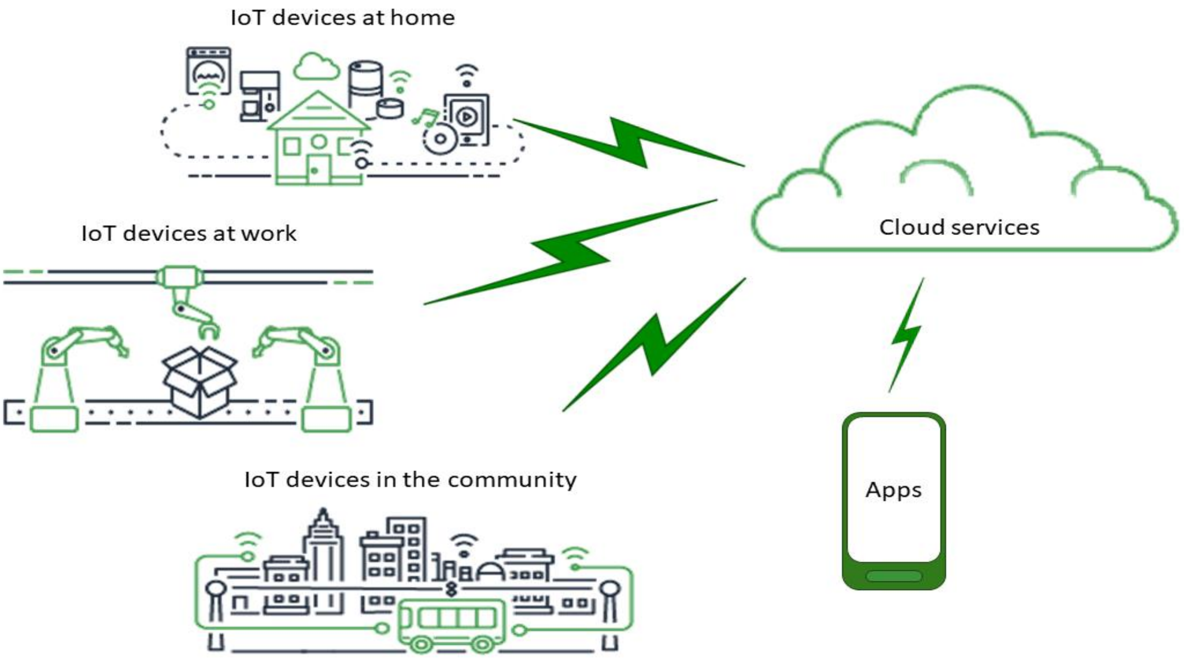
Babu Banarasi Das University, Lucknow, India

ABSTRACT. The internet of things (IoT) has significantly changed how we work, live, and interact with our surroundings. The growth of connected devices has made cybersecurity a top priority for people, businesses, and governments. This article presents an overview of cybersecurity in the Internet of Things (IoT) era while examining the risks, difficulties, and defence mechanisms for IoT networks and devices. In the study, possible dangers and threats to IoT security are discussed, including IoT device vulnerabilities, IoT device lack of standardisation, and the problem of security patching and upgrades. Additionally, the article assesses the current level of IoT security, considering current security standards and protocols, and it covers the difficulties in putting in place practical security measures. The relevance of encryption and access control, the function of blockchain technology, and best practises for securing IoT devices and networks are explored as IoT security strategies. The article offers suggestions for future paths in IoT security research and development and finishes with case studies and examples of effective IoT security implementations. [1]

Introduction:

The term "Internet of Things" (IoT) describes physical equipment, cars, and other items that have connectivity, software, and sensors built in so they can gather and exchange data online. These gadgets, which range in size from tiny sensors to massive machines, are frequently employed to track and manage many elements of our environment, from smart cities and houses to machinery and transportation networks.

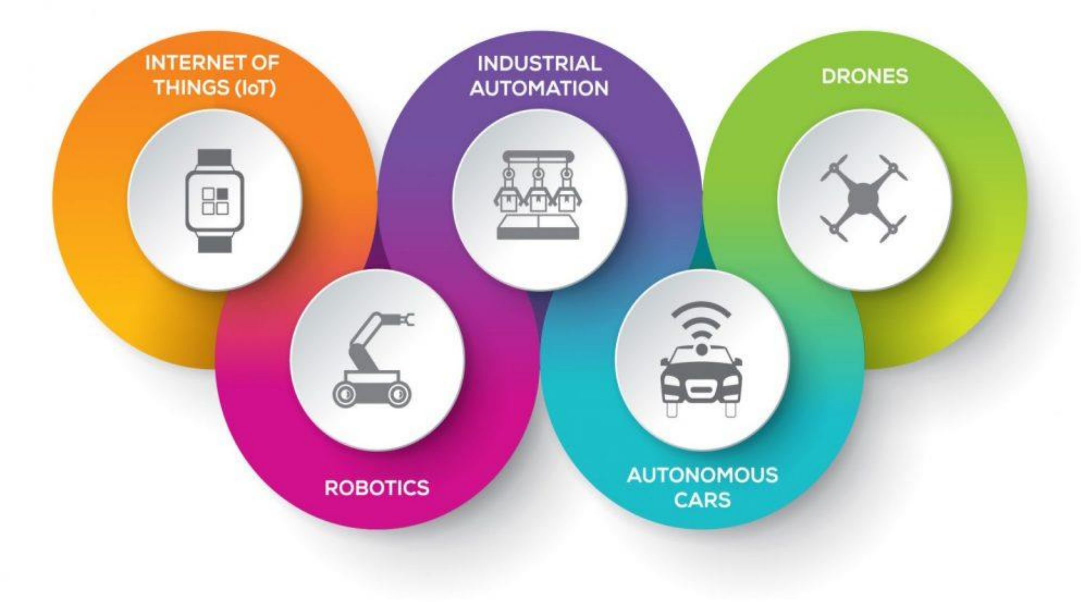
IoT has spread throughout today's society, with an estimated 30 billion gadgets expected to be online by 2021. By 2025, Statista predicts that there will be 75 billion people on the planet. The ubiquitous availability of internet connectivity, the rising need for automation, and the accessibility of low-cost sensors have all contributed to the development of IoT. By enabling real-time monitoring, analysis, and optimisation of many processes, IoT has the potential to change many industries, from healthcare and manufacturing to transportation and agriculture. Though each linked device represents a possible entry point for cyber attackers, the development of interconnected gadgets also poses substantial hurdles for cybersecurity. [2]



2.The need for Cybersecurity in IoT. As Internet of Things (IoT) devices proliferate, organisations and people now have more opportunity to gather and analyse data in real-time. But the rise of linked gadgets also brings about fresh cybersecurity difficulties.

IoT cybersecurity is essential since these gadgets capture and send private information including financial data, personal information, and other confidential information. In addition to controlling vital systems and infrastructure, such as electricity grids, transportation networks, and healthcare systems, these devices are also tempting targets for cybercriminals.

Cybersecurity The lack of standards in IoT devices, the complexity of securing compact and embedded systems, the problems with security patching and updates, and the possibility of third-party intrusions are just a few of the hurdles that IoT must deal with. [1]



3.Purpose of The Research Paper. The goal of the study paper "Cyber security in the age of the internet of things" is to present an overview of the difficulties, dangers, and mitigation measures involved in securing IoT networks and devices against potential cyber threats. The purpose of the article is to analyse the current status of IoT security, including current security standards and protocols, and to assess the difficulties in putting in place practical security measures. Along with case studies and illustrations of effective IoT security implementations, the paper also analyses potential dangers and threats to IoT security.

4. Risk And Threats to IoT Security:

4.1 Overview of the potential risks and threats to IoT security. Some of the most significant risks and threats to IoT security include:-

- Device vulnerabilities: IoT devices often have limited computational resources and are built with as focus on functionality rather than security.
- Lack of standardization: The lack of standardization in IoT devices makes it difficult to ensure that they all meet a minimum level of security. This lack of standardization also makes it challenging to establish uniform security protocols for IoT devices.
- Weak encryption: Many IoT devices rely on weak encryption protocols, making them susceptible to cyber attacks that exploit encryption weakness.
- Third-party breaches: IoT devices often rely on third-party services and platforms, such as cloud services, which can be vulnerable to attacks. A breach in these services can lead to a breach of the IoT devices that rely on them.

- Insecure software updates: IoT devices must be regularly updated to patch security vulnerabilities. However, the update process can be vulnerable to attacks, and if an update is not secure, it can introduce new vulnerabilities.
- Physical attacks: IoT devices can be physically attacked, such as being tampered with or stolen, leading to the loss of sensitive data or the disruption of critical infrastructure.
- Lack of user awareness: Users of IoT devices may not be aware of the potential risks and threats associated with their devices, making them more susceptible to cyber-attacks. [2]

4.2 Examples of IoT Security Breaches. There have been several high-profile IoT security breaches in recent years, highlighting the potential risks and threats associated with interconnected devices. Here are some examples of IoT security breaches:

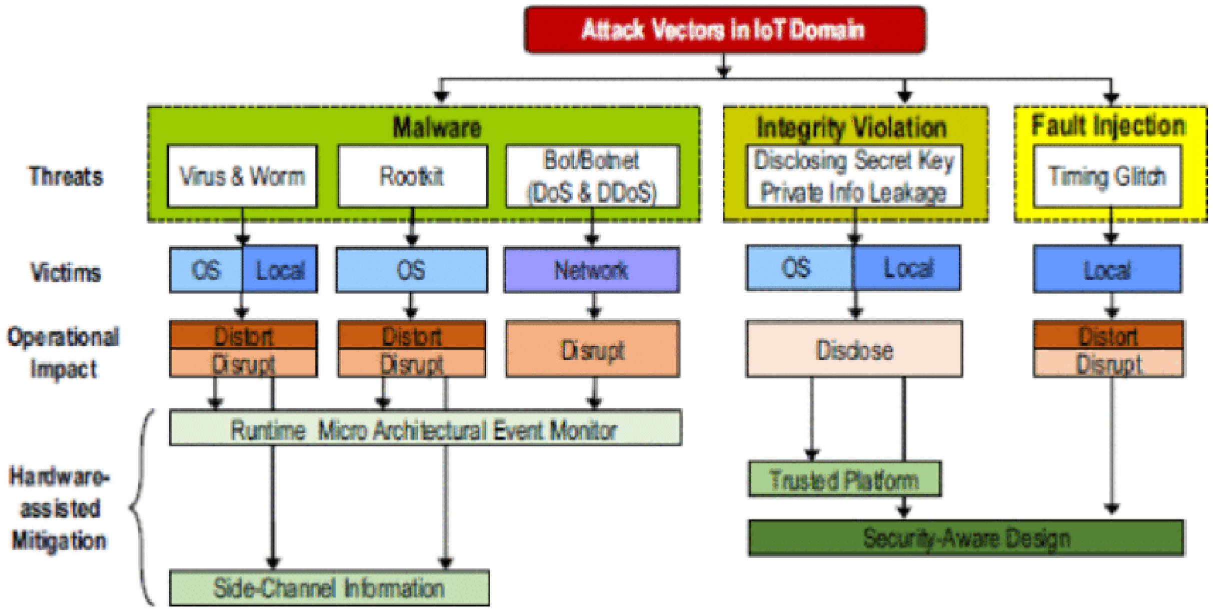
1. Mirai Botnet: In 2016, the Mirai Botnet infected thousands of IoT devices, including routers, cameras, and digital video recorders, by exploiting weak passwords and unpatched vulnerabilities. The botnet was then used to launch a massive distributed denial-of-service (DDoS) attack on DNS provider Dyn, causing significant internet disruption.

2. WannaCry Ransomware: In 2017, the WannaCry ransomware attack infected more than 200,000 computers in over 150 countries. The attack exploited a vulnerability in Microsoft Windows, which allowed it to spread rapidly. IoT devices, such as medical devices and CCTVs cameras, were also impacted.

3. Stuxnet: Stuxnet was a sophisticated cyber-attack that targeted Iran's nuclear program in 2010. The attack targeted Siemens industrial control systems, which were connected to centrifuges used for uranium enrichment. The attack caused significant damage to the centrifuges, highlighting the potential for lot device to be used in cyber warfare.

4. Jeep Cherokee Hack: In 2015, security researchers demonstrated that they could remotely take control of a Jeep Cherokee through its internet-connected entertainment brakes, and transmission, highlighting the potential risks associated with connected cars.

5.Hotel Room Key Card Hack: In 2018, researcher demonstrated how they could use a lot-based attack to hack into and open hotel room key card locks. The vulnerability allowed attackers to enter hotel rooms without key and potentially steal personal belongings or sensitive information. [2]

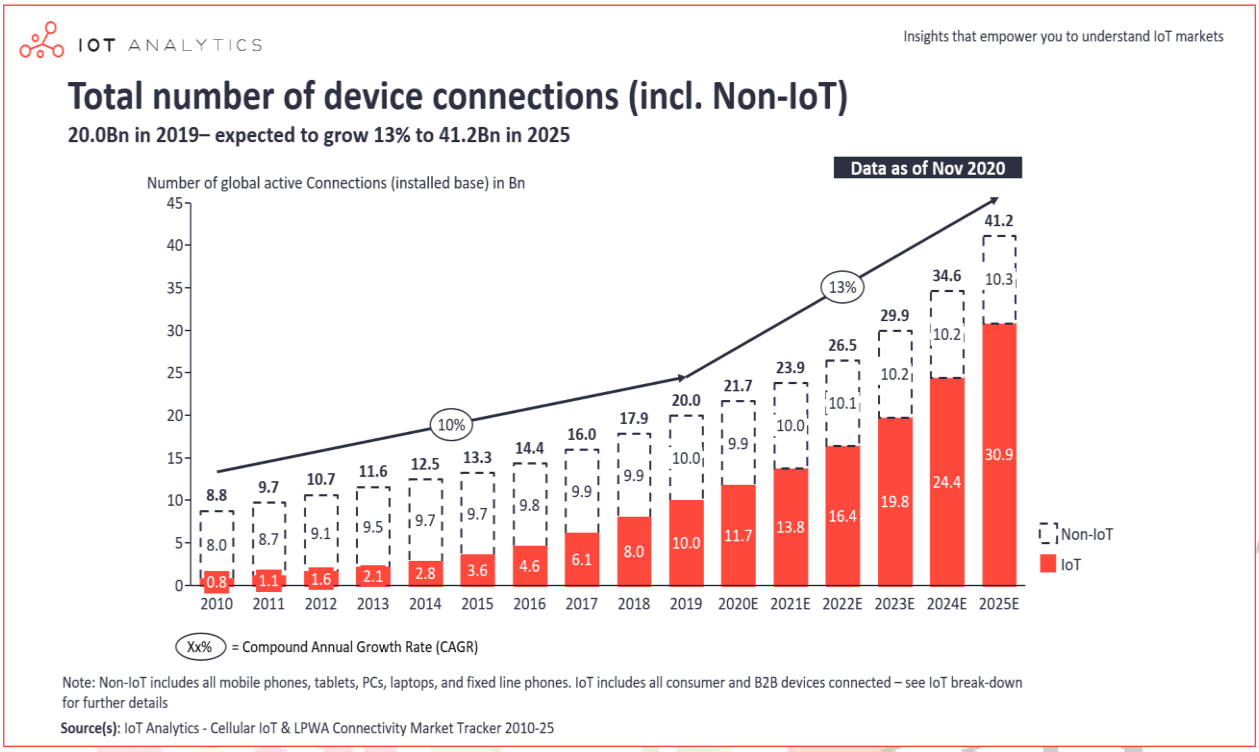


4.3 Discussion on Vulnerability of IoT. IoT devices are susceptible to several vulnerabilities that can leave them open to potential cyber-attacks. These vulnerabilities include:

- Weak authentication and authorization: IoT devices often have weak or default passwords that can be easily guessed or exploited by attackers. Additionally, some devices lack proper authorization mechanisms, which can allow unauthorized access to the device and its data.
- Inadequate encryption: IoT devices often rely on encryption to secure data in transit and at rest.
- Lack of security updates: IoT devices may not receive regular security updates, leaving them vulnerable to known exploits and vulnerabilities.
- Physical security: IoT devices may be physically vulnerable to tampering, theft, or destruction, which can compromise the device's security.
- Malware and viruses: IoT devices can be infected with malware and viruses, which can be used to launch attacks or steal data.
- Insufficient network security: IoT devices may not be properly secured on the network, allowing attackers to gain access to other devices on the network.
- Lack of standardization: IoT devices are often built with a focus on functionality rather than security. As a result, there is a lack of standardization in security protocols and practices across different devices, making it difficult to establish uniform security standards. [3]

5. Current state of IoT security: IoT security is currently in a complicated and dynamic condition. IoT devices come with a number of advantages and conveniences, but they also have inherent security vulnerabilities because of their connectivity, shoddy default settings, and lack of security upgrades.

The sheer number of devices that need to be secured presents one of the major challenges in IoT security. It is getting difficult to maintain and safeguard all of the linked devices as there are more of them. Furthermore, a variety of suppliers with various levels of security standards frequently produce these devices.



Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Source(s): IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker 2010-25

Unauthorised access, data breaches, and ransomware attacks are a few typical IoT security issues. Protecting this data from unauthorised access is essential since IoT devices frequently collect sensitive data such personal information, credit card information, and health information.

A considerable focus has been placed on creating IoT-specific security solutions, such as encryption, authentication, and access control, to address these issues. In order to promote better security practises, industry standards, laws, and recommendations have also been created. [4]

6. Research Methodology:

Overview of the Methodological Approach The five steps that make up the research technique for this work are as follows: 1. Definition of Topic Selection and Research Questions 2. Data Gathering 3. Analysis of Data 4. Definition of Topic Selection and Research Questions for Data Reporting Relevance, public opinion, and the need to raise awareness of the problem were the three criteria that were given top priority while choosing the research topic. 'Cyber Security and Internet of Things' was ultimately chosen as the study topic after a quick analysis of all the available topics to compare them against these criteria. Since it relates to the author's personal affinity for home IoT devices, this was also the subject that piqued their attention the most. Techniques for Collecting Data for this study were mostly gathered through archival research, which entails accessing manuscripts, records, and documents from depositories, libraries, and online resources. To ensure high quality data points, research, and analysis for this study, research publications and papers were gathered from digital libraries of reputable organisations like IEEE (Institute of Electrical and Electronics Engineers) Xplore and ACM (Association for Computing Machinery). To find relevant resources, keyword searches at websites like scholar.google.com and researchgate.net were also conducted. By obtaining literature from reputable sources, one may be sure that the writers are experts in their fields and that the papers have undergone adequate peer review. To ensure current and pertinent information, the research articles to be utilised as references had to be extremely recent (not published before 2017). Techniques for Analysing Data For this study, which examines documents and communication artefacts such texts in a variety of formats, photographs, audio, or video, content analysis was predominantly used for data analysis. Here, content analysis is utilised to analyse trends in the written journals that were obtained from online libraries in a methodical and repeatable way. Several sets of questions and keywords were defined to search through those texts after the sources for analysis were chosen, for example, the author's suggestions to improve cybersecurity in IoT, the datasets used to support their research, the author's opinions on cybersecurity threats, research methodologies, and so forth. Techniques for Reporting Data The data was compiled and reported in APA style formatting (6th edition) for the research paper. The content is divided into several easily accessible sections by the paper's table of contents and is supported by literature references in a methodical manner. [5]

Conclusions:

The study came to a number of conclusions, including the following: 1. The broad application of IoT devices and its security- The Internet of Things (IoT) sector now accounts for practically all newly produced machines, devices, and other pieces of equipment. The device ecosystem is getting more centralised and entangled with other systems. Just looking at a few IoT systems in isolation is insufficient. It becomes essential to analyse using the wider picture in order to determine the full extent of the situation at hand. Therefore, a researcher should consider the broad scope and their defined qualities when performing a study in this field. 2. Techniques for safeguarding IoT systems, including their software and hardware Several techniques that have been covered in numerous articles and were used in this investigation. While some articles favoured hardware solutions, others favoured software ones. Both of them were present in some of the articles. Software approaches were found to be simpler to implement and to require less intervention based on real-world implementations of the qualitative study performed on the methodologies. Even while certain hardware solutions are more secure, they have their own set of problems, most of which have to do with cost and implementation. While software-based techniques tend to work well for most common applications, hardware methods are often well suited for systems that need exceptionally high levels of security. Low power consumption and ensuring that devices may continue to function even with a small compute and limited energy resources were themes that pervaded IoT devices. 3. The following phase of the article entails developing a special framework to duplicate cybersecurity in IoT. It is believed that the author of the post will include some techniques of practical application of these models because having only a model is rarely useful. However, these models do have one advantage: they make sure that the research and analysis are presented in a way that is consistent and repeatable. [3]

References:

Articles from Indian journals:

Reddy, P. V. V., Prasad, M. R., & Padmaja, R. P. (2016). Security challenges and solutions for the Internet of Things. International Journal of Advanced Research in Computer and Communication Engineering, 5(2), 302-306.

Mishra, D., Kumari, P., & Sharma, D. (2018). Cybersecurity in IoT: Challenges and solutions. International Journal of Computer Sciences and Engineering, 6(6), 386-390.

Reports and white papers by Indian organizations:

Data Security Council of India (DSCI). (2017). Internet of Things Security Primer.

National Critical Information Infrastructure Protection Centre (NCIIPC). (2015). Guidelines for securing the Internet of Things.