CYBER SECURITY IN INTERNET OF THINGS(IOT)

Submitted To :
DR. KEERTHY A S

Submitted By :
MUHAMMAD ANSHAD P A
ROLL NO : MCA2336

About IOT:

The Internet of Things (IoT) is a network of interconnected gadgets that communicate and share data with each other with the help internet. These devices can be household appliances and industrial gear .And these devices will have software, sensors, and other technologies which allows to gather data and exchange data.

The rapid development of the IOT has completely transformed multiple industries such as healthcare, transportation, and manufacturing. This enhances productivity and enabling more intelligent decision-making. Even so, the worldwide use of IoT devices has also brought out major cybersecurity obstacles. IOT devices are frequently deployed in large numbers and function in a wide range of contexts. which makes them attractive targets for hackers. To safeguard private information, stop malicious activity, and preserve user privacy, IoT system security is essential.

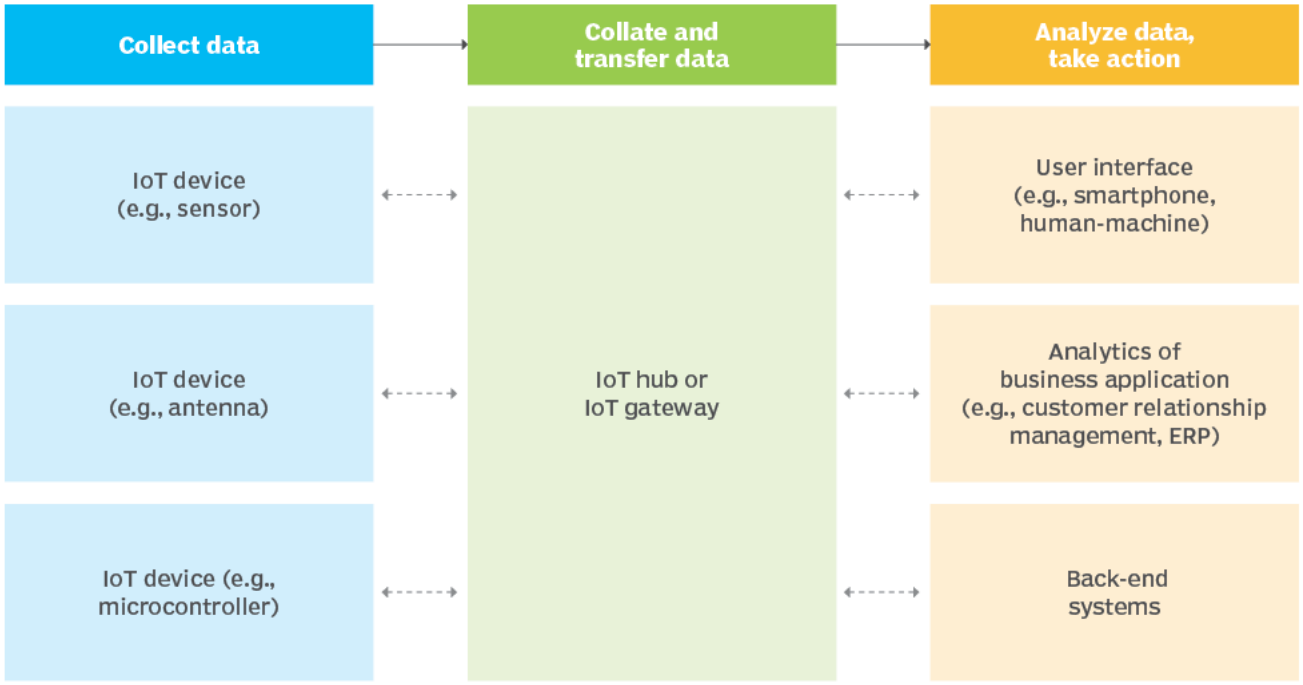

fig 1.1

Current State of IOT:

The spread of IoT has been increasing fast. There are billions of devices currently in operation globally. Statista's report (2023) predicts that the quantity of IoT devices will reach 30.9 billion by 2025. These gadgets are utilised in many different kinds of applications. Used in : smart homes, healthcare, industrial automation, and transportation. Smart Homes: IoT technologies found in smart homes has smart thermostats, security cameras, and voice assistants. These technologies improve the convenience, energy efficiency, and security for homeowners. Healthcare: Wearable tech, remote monitoring tools, and intelligent medical

equipment are all part of the Internet of Things in this field. These technological advancements enhance patient care and allow for real-time health monitoring. Industrial Internet of Things (IIoT): IIoT devices are used in manufacturing, managing the supply chain, and predicting when repair needs to be done. They streamline operations, minimise downtime, and improve production. They increase productivity, streamline processes, and cut down on downtime. Transportation: Smart logistics, connected vehicles, and traffic control systems are all examples of IoT uses in transportation. These methods make things safer, less crowded, and more efficient.

What all are the issues in Cybersecurity IOT ?

Threats and Flaws

A lot of IoT devices don't have strong security features, which makes it easier for people who aren't supposed to be there to get in.

- Unsafe communication: Most of the time, data sent between IoT devices and a central computer is not encrypted, which means that it can be read and changed by someone else.
- Constant lack of new ideas: IoT devices are often used once and then forgotten, leaving software that is out of date and easy to hack.
- Physical attacks: IoT devices can be accessed and changed directly, which could mean that security is breached.
- Attack in general Spreading Denial of Service (DDoS): Attackers can take control of many Internet of Things (IoT) devices by using DDoS to harm target systems and interrupt service.
- Data breaches: Because IoT devices store and send private information, they are easy targets for hackers who want to steal that information and invade users' privacy.
- Man-in-the-middle (MitM) attacks: Hackers can listen in on unprotected channels of contact to change or steal data.
- malware: IoT devices can get malware, which lowers their performance and demands a ransom payment.

fig 1.2

Examples of well-known IoT security breaches

"Mirai Botnet": In 2016, the Mirai botnet took over thousands of IoT devices, like cameras and routers. This led to huge DDoS attacks that shut down popular websites and apps.

The "Stuxnet worm" attacked industrial computer systems and did a lot of damage to Iran's nuclear programme.

Cybersecurity Strategies and Solutions

Several steps and solutions have been suggested and applied to help to reduce the cybersecurity issues in IoT.

Best Strategies for Network and Device Security in Internet of Things:

- Strong verification: putting multi-factor authentication and original credentials for every gadget into use.
- Encrypting data at rest and in flow helps to guard it against illegal access.
- Making sure IoT devices get regular software upgrades and patches will help to fix flaws.
- Separating IoT devices from essential network infrastructure can help to reduce the effect of such breaches.
- Security by Design: Including security elements into IoT products under development and design.

Standards and Security Policies:

Between devices and servers, SSL/TLS—Secure Socket Layer—and Transport Layer Security—protocolues offer secured routes of communication.
Wi-Fi Protected Access 3 (WPA3) improves wireless network security by means of more robust encryption and authentication.

Encryption and Authentication's Function

IoT security depends on encryption and authentication fundamentally. While authentication confirms the identification of devices and users, encryption guarantees that data is just accessible to authorised persons. Protecting IoT systems from cyberattacks depends on strong encryption techniques and safe authentication methods being followed.

Developing Technologies

Blockchain technology provides IoT transaction and data security from a distributed, tamper-proof standpoint.

Trends and directions for future research

IoT security will change in the future based on new technologies and trends. Some important areas for future study are:

Predictions for the Future of IoT Security:

- Better AI and ML Applications: AI and ML will continue to be improved so they can find and respond to threats before they happen.

- Quantum-Resistant Encryption: The study of ways to secure data that can't be broken by quantum computers.
- Standardisation of IoT Security Protocols: Work is being done to make sure that all IoT devices and networks follow the same security rules.

Places to do more research

- Privacy-Preserving Technologies: Making technologies that protect privacy without affecting how they work.

Interoperability means making sure that security methods work in a variety of IoT devices and ecosystems.

- User Education and Awareness: Making users and devs more aware of and educated on the best ways to keep IoT devices safe.

References :

1. Statista : Retrieved from https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

2. Stuxnet Worm : Retrieved from https://en.wikipedia.org/wiki/Stuxnet

3. fig 1.1 : https://cdn.ttgtmedia.com/rms/onlineimages/iota-iot_system.png

4. Fig 1.2 : https://resources.appsealing.com/4svc/wpcontent/uploads/2021/04/01142941/infographic-1-01.png