Sri Lanka Institute of Information Technology

Introduction to Cyber Security

D.G.C.H. RAJASOORIYA

Y2.S1.WD.CS.01.02

MALABE CAMPUS

IoT Security

Table of Contents

Tables of figures

Abstract

The Internet of Things (IoT) extends to billions of devices allowing for extreme data transfer inter-silo as well as inter-automation. Nevertheless, the former bulks the latter risk owing to the device usage, which is the use of the devices aforementioned for exploitation of systems, for instance, bot networks, unwelcome software, and breaking into other people's systems. This paper detailed the evolution of IoT security from the emerging years of the technology to the current systems that incorporate zero trust architecture and AI security systems. It also explores the Integration of New Technologies, which are to be Improvements of Security Features and Attainment of the Cloud-based Inner discovery worlds giant, to Security of SaaS based Inner Discovery platform. The paper discusses the authors' stance on security policy issues and risk management approaches with respect to the Internet of Things ecosystems. The last section describes how advanced technologies, such as digital twins, which are useful in threat monitoring, can also be instrumental in the deployment of IoT devices.

Introduction

The ability to link physical objects to the digital world is thus revolutionizing every single aspect of the individual's day-to-day activities, work, and relationships. Over broad scope, the Internet of Things encompasses smart homes and health devices, industrial equipment automatization as well as smart cities. For this reason, the advancement of the so-called Internet of Things enables these objects to collect and share information with and among each other, without the involvement of human beings. This encourages a high level of automation, improvement of processes and encourages further development. Smart gadgets can help control power consumption, health-based wearables track the users' health status and self-driving cars control themselves at road junctions with traffic management systems. This also explains the astronomical growth as many people will be connected for a great number of devices tagged in the right period.

Old generation systems adapted in the IoT where functionality was the shallow goal rather than outlays of a security model. This has made the eco system prone to various levels of security threats including IoT malware, compromises of sensitive information, and denial of service (DDoS). Take for example the botnet attack termed as Mirai, which was publicized due to taking advantage of unsecured IoT appliances in people's homes to carry out a coordinated DDoS attack. Also, consider the Stuxnet computer worm that caused damage and even shutdown critical systems due to system vulnerabilities which could be attributed to the IoT paradigm. With the escalating use of IoT especially in key sectors such as health care, transportation and energy, security becomes an issue that cannot be ignored.

The security landscape of IoT is not static and keeps changing as new technology and threats arise. Most traditional approaches to IoT security are focused on the segregation of networks and assume that all devices trust each other. This model is not practical anymore given the current state of issues. Therefore, most enterprises are adopting Zero Trust frameworks, which place every device, user or service at risk until they prove from who they are and what are they doing. AI and ML are also essential in monitoring large amounts of data for abnormal behavior and actively taking actions against threats in a short period of time.

In looking up, new technologies and frameworks are being researched for the improvement of the security of IoT. Blockchain brings security by establishing a record of all the database interactions and transfers of information between devices without the possibility of alteration.

Post-quantum cryptography research is in progress with the aim of reinforcing the security resilience of IoT networks against the up-and-coming threat of quantum computing. With edge computing, central cloud infrastructure is relied on less because data is processed at the proximity of the data-generating devices to help mitigate latency and data confidentiality issues. In addition to this, the concept of digital twins that is the real-time and accurate representation of physical objects and the bodies is being developed such that it is used for defense monitoring and predicting threats.

In light of these developments, IoT security continues to remain an intricate challenge that can't be tackled using a simplistic approach. It requires not only technological means, but also policies, practices and them being incorporated in trained personnel. There are international instruments which define and regulate actions for IoT ecosystems such as GDPR or NIST Cybersecurity Framework. However, the security of any IoT ecosystem will rely on every agent involved including: producers, service providers, and consumers. Therefore, frequent software patching, safe device setting, and training of end users are significant in decreasing the risks associated with ensuring the safety and privacy of IoTs.

In this particular paper, we present the trends in IoT security from conceptualization to development, identifying significant security lapses, and the remedies employed. In addition, we look at the developments which can be expected concerning the security aspect of IoT in years to come. The objective is to explain in detail the existing problems and approaches in regard to safety of the Internet of Things, which would stress the need for further improvement of existing measures and monitoring of the existing cyberspace threats. [1] [2]

Evolution of Internet of Things (IoT) Security

1. Early IoT Development (1980s -1999s)

The concept of connecting devices to the internet began to emerge in the late 1980s. In 1982, a modified coke vending machine at Carnegie Mellon University was considered one of the first connected device. It could report inventory and the temperature of the drinks. Students could check this information remotely via the ARPANET, an early version of the internet.

Figure 1:IoT Device 1

In 1989, English computer scientist Tim Berners Lee proposes the framework of the World Wide Web and lays the foundation of the internet.

In 1990, John Romkey invented a toaster that can be turned on or off via the internet. It was connected to the internet with TCP/IP networking and controlled with a Simple Networking Management Information Base (SNMP MIB). It had one controlled to turn the power on and the darkness of the toast was controlled by how long the power was kept on. [3]

Figure 2:IOT Device 2

While the coke vending machine is generally regarded as the first device connected to the internet, Romkey's internet connected toaster is often considered the first IoT device in the modern sense, as it was designed to be controlled via the internet. [4]

In 1993, Quentin Stafford Fraser and Paul Jardetzky from the University of Cambridge build the Trojan Room coffee pot in their computer laboratory where an image of its interior is uploaded to the building's server thrice every minute for people to check the level of coffee when they want a cup.

The term Internet of Things was first coined by Kevin Ashton in 1999 while working at Procter and Gamble, visualizing RFID as a way to track objects in supply chains.

RFID (Radio Frequency identification)

A wireless communication technology called radio-frequency identification (RFID) uses radio waves to read the information contained on an electronic tag. Every RFID system comes with three primary parts. This will entail scanning transceivers, transponders, and antennas. Using a transceiver and scanning antenna, the reader or interrogator establishes a connection with an RFID tag. To activate or boot up this tag, the reader uses radio wave signals to connect with the tag. This tag converts a wave from an identical type of antenna into data when it is powered on. In reality, an RFID tag's transponder is what it is. RFID tags contain a substrate, an antenna, and an integrated circuit (IC). [5]

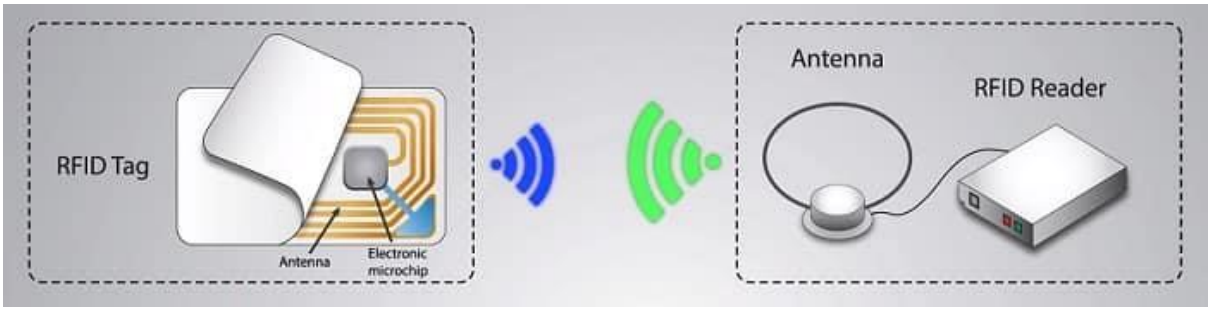

Figure 4:RFID components

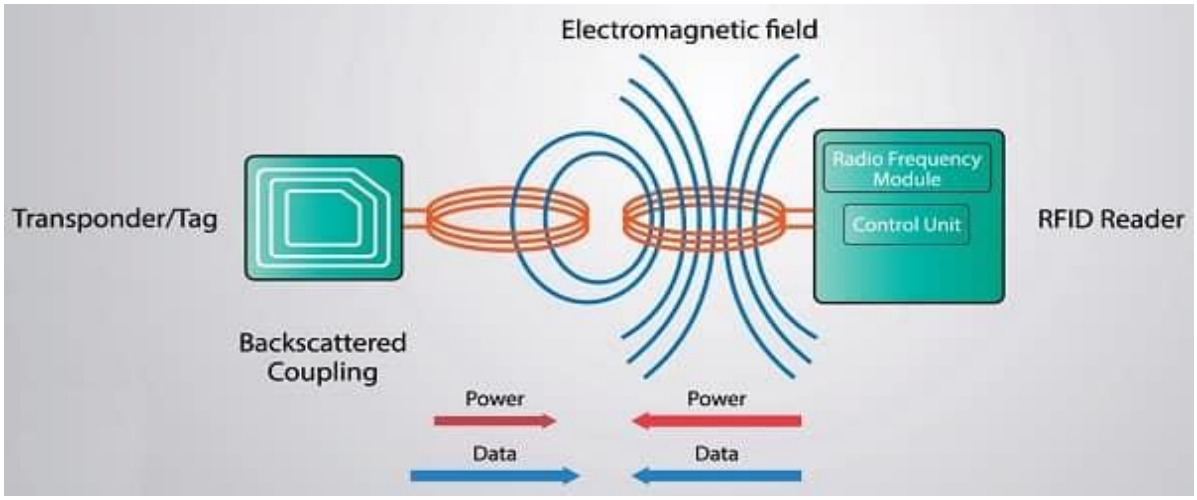

Figure 3:RFID Process

Wireless Sensor Network (WSN)

A wireless sensor is a device that can gather sensitive information and detect changes in local network. Movement sensors, temperature sensors and liquid sensors are the some of examples for wireless sensors. Wireless sensors do not perform heavy data processes and consume little power.

Types of wireless network topologies

The topology means that the arrangement or structure of how different devices(nodes) are interconnected and communicate with each other. Wireless topologies define how devices interact using radio waves or other wireless communication methods.

- Star topology

Multiple wireless devices are connected to a central hub or access point.

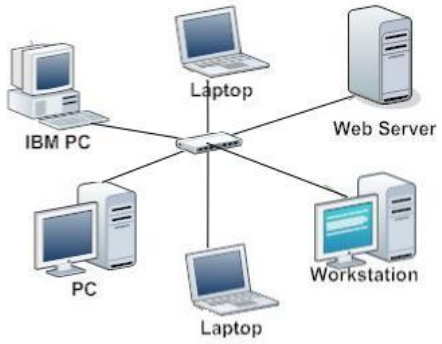

Figure 5:Star Topology

- Mesh topology

Each node in a mesh network is connected to multiple other nodes allowing data to take multiple paths to reach its destination.

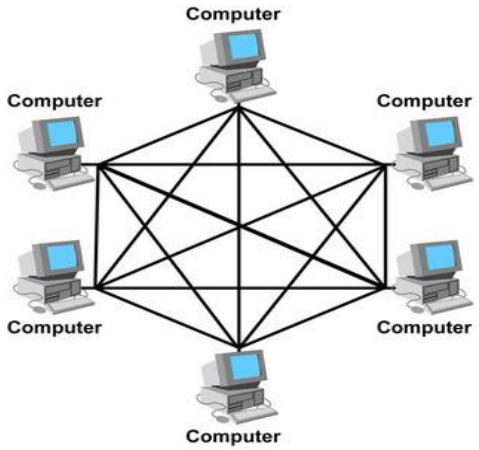

Figure 6:Mesh Topology

- Tree topology

Data is transmitted from one node to another along the branches of tree structure.

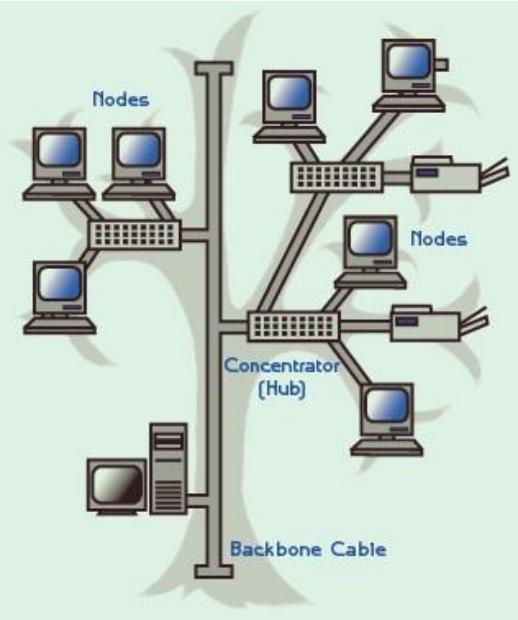

Figure 7:Tree Topology

Wireless Sensor Network Architecture

- Physical layer

Connects sensor nodes to the base station using technologies like radio waves, infrared or Bluetooth.

- Data Link Layer

Responsible for establishing a reliable connection between sensor nodes and the base station.

- Application Layer

Enables sensor nodes to communicate specific data to the base station using protocols like ZigBee.

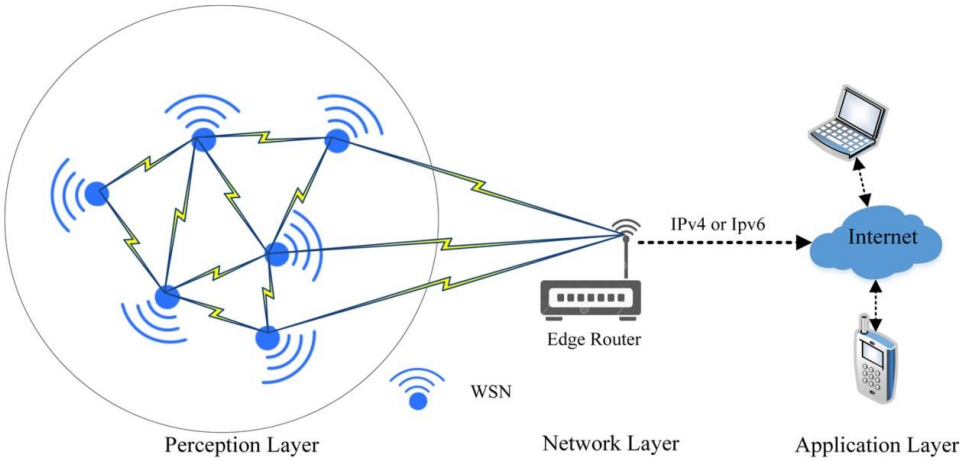

Figure 8:WSN Architecture

Wireless networks are a key component of IoT infrastructure as most IoT devices communicate and share data wirelessly.

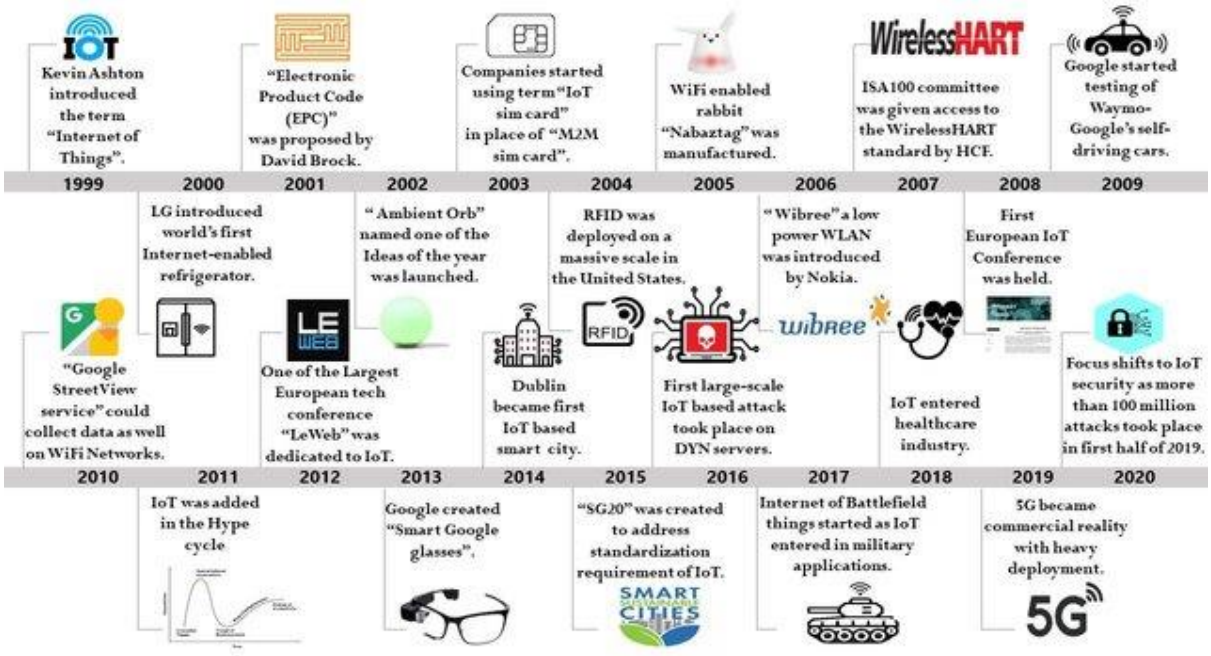

Figure 9:Evolution of IoT Technology

Security was not a primary concern in these early stages because the scale of IoT was small and devices were used in limited controlled environments.

Key characteristics of early IoT devices:

- Lack of standardized communication protocols.
- Devices were designed to prioritized functionality over security.
- Minimal or no encryption and authentication mechanisms were used.

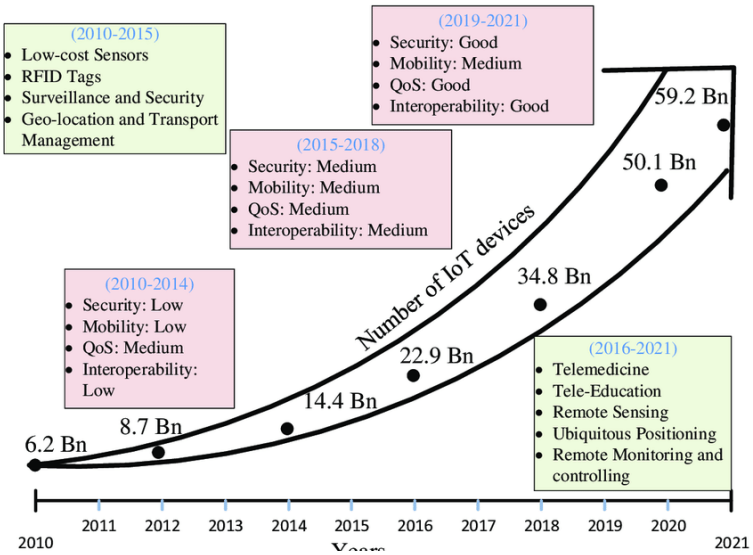

Figure 10:Rise of IoT Devices

2. Rise of Security Concern

As IoT started becoming more prevalent in the 2000s, the focus remained on functionality rather than security. IoT began expanding beyond industrial applications into consumer market with the rise of smart home devices, wearable technology and industrial IoT. The lack of standard security practices exposed IoT devices to numerous vulnerabilities. These are the some of examples for IoT security breaches.

Stuxnet worm: The Stuxnet computer worm infiltrated numerous computer networks. The Stuxnet message worm penetrated and destroyed more than 15 Iranian facilities. It is believed that the assault was initiated by a USB device of an arbitrary employee. The nuclear plant situated in Natanz was this among other attacked industries. It is universally known today that this computer virus was purposely designed to sabotage Iran's nuclear ambitions. Numerous scholars, however, suggest that the operation to deploy the Stuxnet computer worm in Iranian nuclear sites was conducted by Israel and the United States.

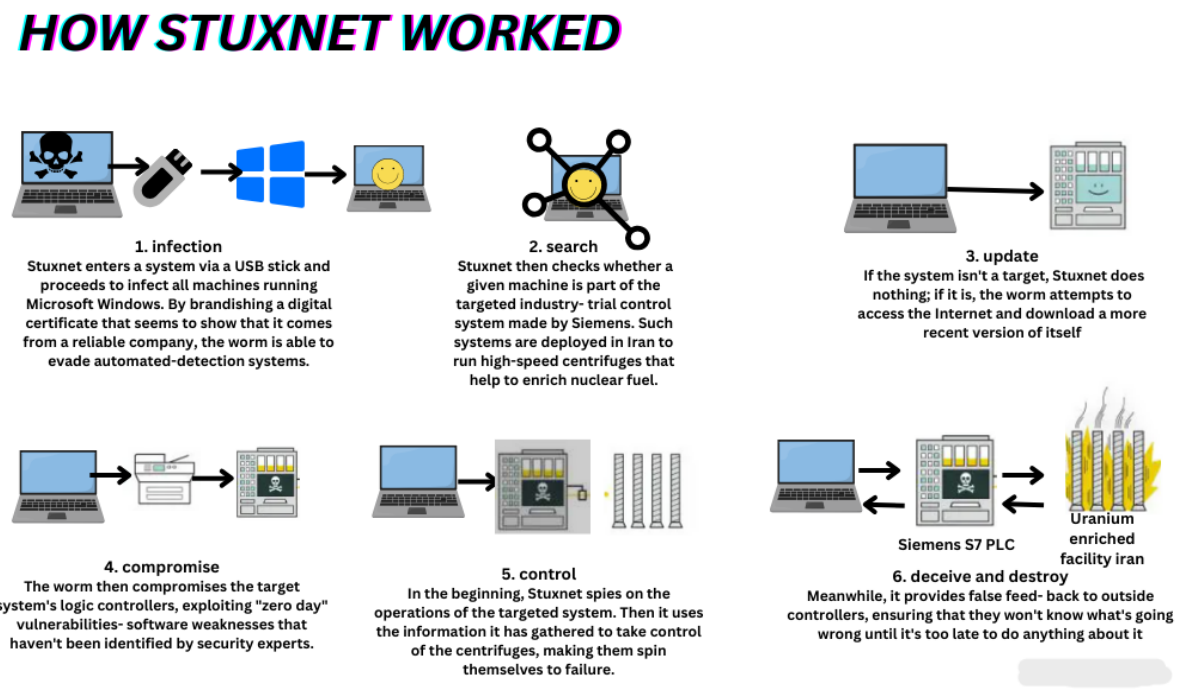

Figure 11:Stuxnet worm

Target breach: In the year 2013, around 40 million customer credit card information was compromised after accessing the point-of-sale data for approximately two thousand Target outlets dotted across the nation through a malware planted in their POS systems. A spear phishing attack was launched by the assailants against an outside contractor who was responsible for heating, ventilation, and air-conditioning (HVAC) systems for Target. Through this, personal information such as names, phone numbers, email accounts, payment card digits and credit card verification codes were compromised. Following this, the hackers used those compromised credential to penetrate into target's corporate network where they tamped down software on the positioned devices that had target's Point of Sale systems.

Jeep Hack: Car hacking made headlines in 2015, when two hackers conducted a remote car hack while the car was on the highway by triggering the wipers, turning on the radio at the maximum volume and subsequently offing the car engine to stop the vehicle entirely.

The Mirai botnet attack that compromised a large number of unprotected IoT products and used them to orchestrate an enormous denial of service attack against the DNS provider Dyn was one of the fundamental moments of the history of IoT security.

Mirai botnet attack: Mirai is a form of malware that specifically attacks IoT devices, including but not limited to routers, cameras, and other web connected devices. These devices are generally those that are either secured with default simple passwords or run unpatched obsolete software. The bots most commonly associated with this malware were the Mirai bot, which enabled the infiltration of devices that were susceptible to attacks. When the device was seized and commandeered, it would join an army of bots that could be used for DDoS attacks. [6]

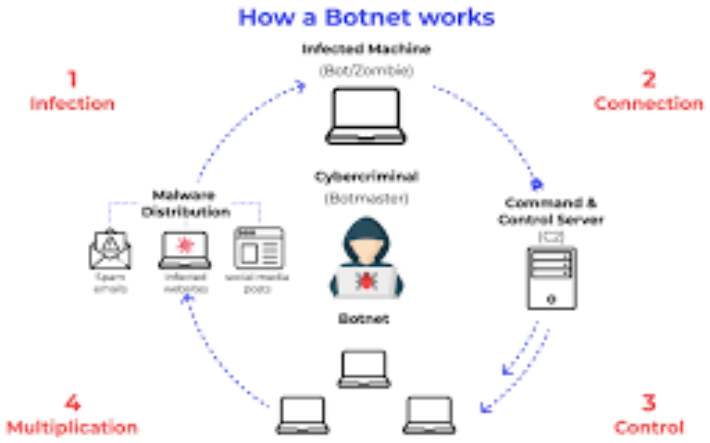

Figure 12:Botnet Attack

Distributed denial-of-service (DDoS) attack: It is a malicious attempt to disrupt the normal traffic of the targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. Once a botnet has been established the attacker is able to direct an attack by sending remote instructions to each bot. [7]

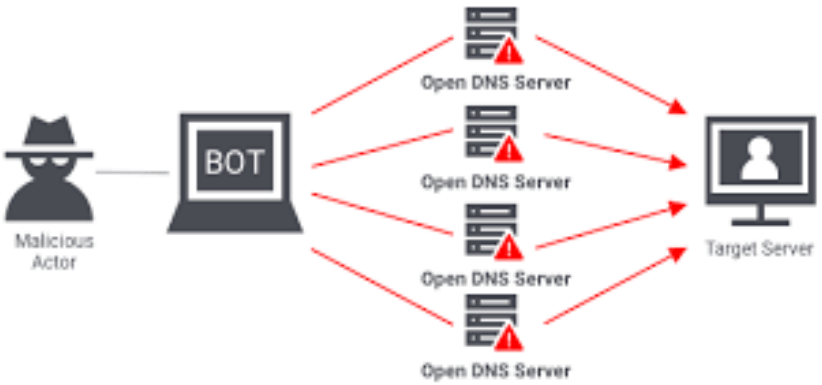

Figure 13:DDoS Attack

These examples highlight the critical need for robust IoT security and the potential dangers posed by unsecured IoT devices and systems. To safeguard IoT devices and data from security threads it is crucial to implement effective security measures.

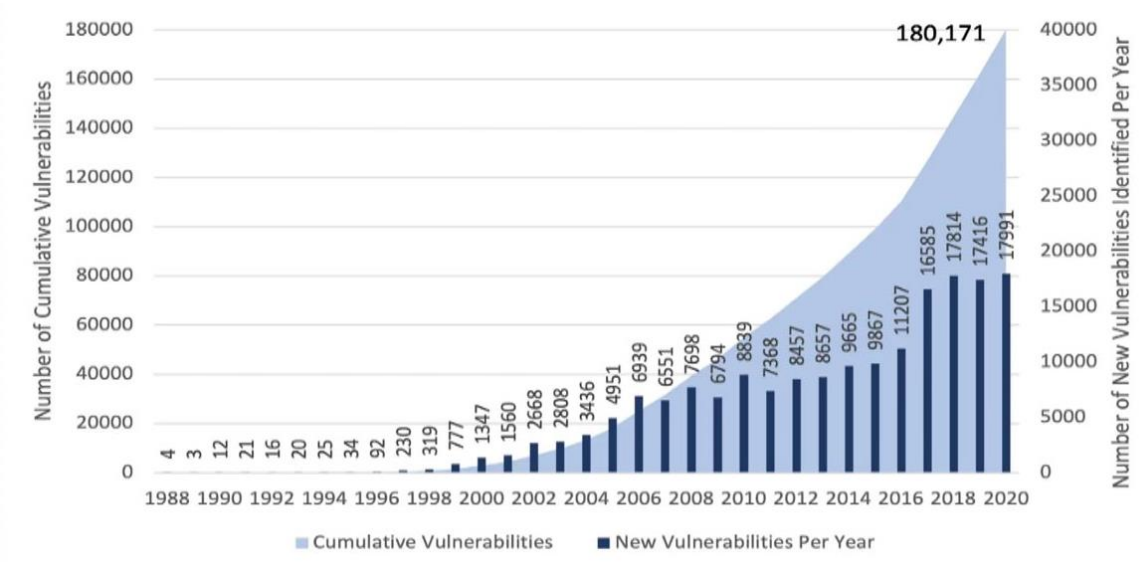

Figure 14:Identify vulnerabilities

3. Solution for IoT Security Challenges

Although the Internet of Things presents significant security challenges such as weak authentication and authorization, data privacy, network vulnerabilities, physical security and supply chain vulnerabilities compared to traditional systems, many researchers have proposed solutions to address these issues. In the following factors will explore some potential methods to improve IoT security.

- ✓ Trust management

Trust management is a critical aspect of the IoT, helping users navigate the risks and uncertainties with these systems. It involves ensuring user safety and privacy while fostering confidence in the network. Effective trust management allows users to have control over their interactions with IoT services and transparency in how these systems operate. Establishing reliable governance and creating decentralized trust models, trust mechanisms for cloud computing and trust-based applications at the node level are key areas of research. Automating trust evaluations is also essential to maintain fairness and reliability within the IoT ecosystems.

- ✓ Authentication

Several authentication models have been proposed for use with the IoT such as gateway model, trust chain model, security token model and global trust tree model. One method uses a single cipher for a request-reply technique highlighting the importance of strong password and multi-factor authentication.

- ➢ Strong passwords: Password should be long, complex and unique for each device to enhance security.
- ➢ Multi-factor authentication: This method requires two types of authentications before accessing an IoT device, adding an extra security.

In addition to authentication various forms of access controls should be implemented in IoT environment.

- ➢ Role based access control: Access to IoT resources should be restricted based on user roles or job functions, reducing the risk of unauthorized access.
- ➢ Device authentication: Devices should be authenticated using methods like digital certificates or unique identifies before connecting to the network.

- Network segmentation: segmenting IoT networks can limit the scope of potential security breaches by restricting access based on roles or functions.
- Audit logging: All access to devices, applications and data should be logged and monitored to detect unauthorized activity and ensure accountability.

✓ Privacy solutions

Data privacy is a key concern when implementing IoT security measures. Companies must protect their data and customer privacy through encryption, firewalls and access controls. Regular updates and patches are essential to address security vulnerabilities. A principle known as “privacy by design” emphasizes giving users control over their data. Transparency is also important ensuring users know who handles their data and how it is used. Effective data management policies are needed in cloud environments. One solution is user-driven enforcement for cloud-based services on the IoT. It allows users to manage sensitive data before it is sent to the cloud. Business must educate users on IoT security risks providing resources and regular reviewing security policies. Testing and monitoring systems frequently using automated tools for incident detection and conducting security audits are crucial. Additionally, business should have a robust backup and recovery plan in case of breaches. Encryption is vital for security data transmission and storage on IoT devices with end-to -end encryption ensuring only authorized parties can access the data. Manufactures should create privacy policies that are transparent, easy to understand and adhere to industry standards.

✓ Regulatory Solutions

A regular solution for IoT security involves adherence to security standards and regulatory frameworks that guide manufactures and service providers in mitigating cyber risks. As highlighted by the European Union’s strategic approach the development of the regulations ensures the safe deployment of IoT technologies.

- ISO/IEC 27001: Information Security Management System (ISMS)

This international standard specifies the requirements for establishing, implementing and continually improving an Information Security Management System (ISMS). It provides a systematic approach to managing sensitive information to ensure its confidentiality, integrity and availability. IoT devices collect and transmit personal or operational data. ISO/IEC

27001 helps ensure that this data is securely stored, processed and transmitted across devices and systems. It encourages encryption, access control and security audits.

- NIST Cybersecurity Framework

Created as a voluntary framework with rules by the National Institute of Standards and Technology (NIST). There are five functions in the framework. Identification, protection, detection, response, and recovery are the categories into which these falls. IoT ecosystems are easy targets for attackers because of their numerous systems and devices. NIST is made to assist organizations in identifying security and privacy risks, protecting assets from cyber threats with measures that are specific to these interconnected environments, and reacting swiftly in the event of an emergency. The NIST IR 8259 series and NIST SP 800-183 include specific IoT guidelines, such as firmware updates, data encryption techniques, and device configurations, all of which are essential to maintaining the security of your device.

- General Data Protection Regulation (GDPR)

The most extensive data privacy law to date is the General Data Privacy Regulation. IoT devices are well known for gathering a variety of personal information, from medical records to the activities of a smart home kit. Organizations must also adhere to technology standards such as data encryption, user consent, and data minimization services that can be made use of, as stated in the GDPR.

- Health Insurance Portability and Accountability Act (HIPAA)

In the United States, there is a law called HIPAA that sets out to protect medical records and PHI in particular. With the increased usage of medical IoT devices such as pacemakers, glucose meters and smartwatches etc. more healthcare data is being produced. HIPAA is only enforced in the situations above where data has to be kept inviolably safe from any unauthorized uses. Healthcare providers using these devices via the IoMT will need to manage patient data access, secure transmissions through data encryption, enforce user authentication and integrate on-going audits or adapt security policies.

- IEEE 802.1X: Network Access Control

Port-based network access control (PNAC) has been documented in the IEEE 802.1X that access to the network is restricted to only the authenticated devices. In today's society, several IOT devices are used in protected areas such as hospitals and industrial control

systems. Only such devices and users are permitted by PNAC, that is trusted. This standard uses support for the Extensible Authentication Protocol (EAP) as an example where the required information is obtained before entering the network. It may also be used in conjunction with security systems, including RADIUS servers for remote management purposes. Restricts non-permitted IoT systems from entering networks. As a result, the vulnerability of numerous cyber-attacks including botnet type attacks is greatly reduced.

- Physical security

Physical security of IoT is the devices and the infrastructure to be protected against unauthorized access, theft, or tampering. Such protection can be achieved by locking cabinets or rooms containing the IoT devices against illegitimate physical accesses. Devices are installed in locations growing to be very inconvenient for those who are not authorized. Besides, various control mechanisms provide different means to enable access to a device such as keys, access cards, biometric authentication, etc. Monitoring devices within an area almost entirely prevents loss of devices as persons are aware that there are cameras which can record their actions, and these can also provide evidence of loss in case such occurs. Tamper-evident seals signal unauthorized interference, while environmental sensors detect changes in conditions, such as temperature or humidity, which may be indicative of security risks. They are the elements which help in sustaining and maintaining confidentiality, integrity, and availability of information in an IoT system ensure reliability in carrying out functions while being safeguarded against physical attacks is assured.

- Network Segmentation

Network segmentation, which serves to divide a network into isolated subnets so that one compromised device cannot continue spreading malware or threats. This helps in preventing possible breaches by allowing the devices to be segmented according to type, duty or site and then quarantine such parts of your network if there are any anomalies. Application segmentation reduces the surface area and segments of critical data from tampering by isolating them based on importance or function. By categorizing users into the right subnetworks, you only expose specific user groups to certain information. Data segmentation does the same but marks for level of importance, protecting critical data from unauthorized users. Although segmentation provides benefits like minimizing the attack surface and aiding in access control, it also adds complexity as all segmented zones should be managed with consideration of segment-level security.

4. Current Phase (2019 – Present): Emergence of Zero Trust and AI-Driven Security

IoT devices have become deeply integrated into various fields such as industries, healthcare or smart city structures, we decided to organize a more proactive and universal security solution. As attacks grow more sophisticated, the old perimeter-based security model for IoT ecosystems can also put companies at greater risk. As a result of this, Zero Trust architectures have been embraced by many enterprises and AI-powered security solutions that help with protecting the devices and stream data.

- Zero Trust Security

In the current IoT security context, zero trust principles are essential because they eliminate the implicit trust assumption in networks. Until their identity and intent are established, all devices, users, and programs requesting access are regarded as possible threats. This will limit attackers' ability to move laterally throughout the network and lessen the likelihood of unauthorized access through JSON manipulation by limiting resource access to only authenticated and authorized organizations. Because access rights need to be continuously reevaluated in settings with extensive IoT deployments, such as healthcare and industrial facilities, continuous monitoring is an essential component of Zero Trust.

Figure 15:Zero Trust Security

- AI and Machine Learning for Security

The defenses of IoT networks are increasingly relying on Artificial intelligence (AI) and machine learning (ML) technologies. These systems analyze vast amounts of network traffic information to spot abnormal patterns such as device behavior changes or inconsistent connection attempts. Machine Learning algorithms designed for detecting threats, whether based on attack patterns, systems or illegitimate devices, can as well perform quite well with detecting potential threats such as DDoS attacks or compromised IoT devices enlisted in a botnet using cognitive intelligence tools. There are added benefits of ML which include the way it allows quick resolution of security problems through predictive capabilities that not only predict new security threats only but also control response actions to incidences.

Figure 16:AI and Machine Learning

- Secure Boot and Firmware Update

The security of IoT devices commences with a secure boot process, which in turn consists of various stages of the device each checking the credibility and the completeness of the preceding stage. The essence of this step is to prevent the installation of rogue firmware onto the device, also some devices can be shielded from attack. In addition, since the introduction of the devices, the ability to securely perform over the air updates on the devices has become paramount. OTA updates give the opportunity to the manufacturers to update the hardware without physical access to the device, which makes it very convenient for the very large and widespread networks of the IoT.

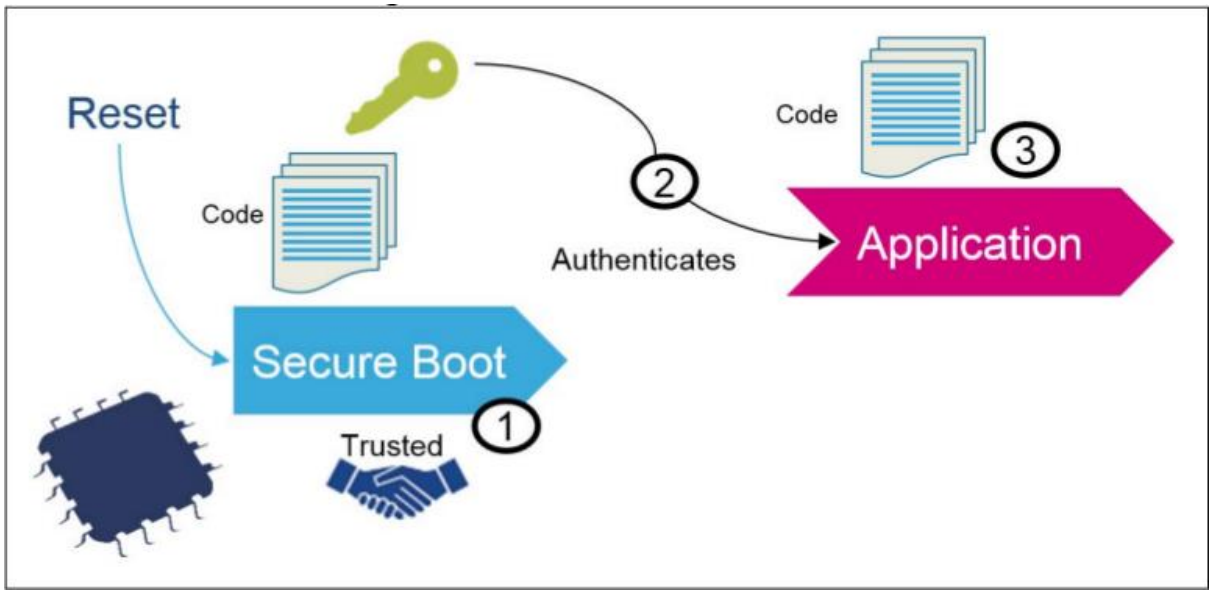

Figure 17:Secure Boot

- Device Identity and Access Management (DIAM)

Device Identity and Access Management (DIAM) enables detailed management strategies regarding the conduct and communication of every IoT device on the network. Instead of a traditional Access Management that focuses on users, DIAM manages devices by giving each device a discrete identity which is crucial in enforcing access policies. For instance, a smart sensor may be conditioned to communicate only with certain systems at specified times. DIAM also controls devices' operational thresholds hence controlling the extent of damage control that a rogue device or illegitimate access can bring. It also assists in effective device onboarding and offboarding which is necessary for preserving cleanliness in networks that experience rapid growth in the number of devices connected to the Internet.

Future Development of IoT Security

1. Blockchain for Secure IoT Networks

Security mechanisms that are based on distributed architectures are offered by the blockchain technology to solve the issues that are inherent in the central network of IoT systems. Blockchain technology guarantees security when interacting with IoT networks by incorporating clear and unchangeable records for devices communication and data transfer. This system prevents dependence on a single network hub, thereby enabling network access control to only approved devices. In addition, the security policies between the IoT devices can be automated through the use of smart contracts which improves the overall efficiency. Supply chains are one example of this since IOT devices incorporate blockchain technology to authenticate the products and monitor the flow of the goods to avoid fraudulent activities in the supply chain of the products. [8]

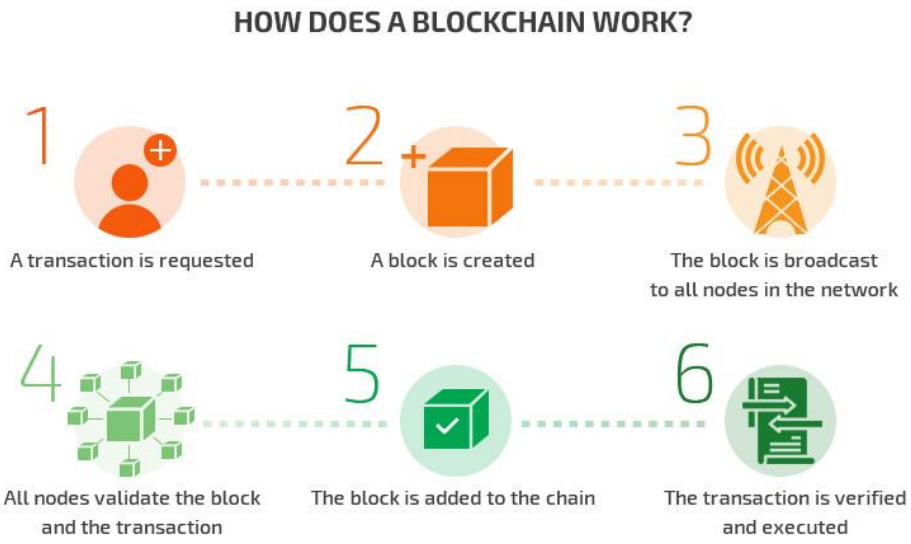

Figure 18:Blockchain

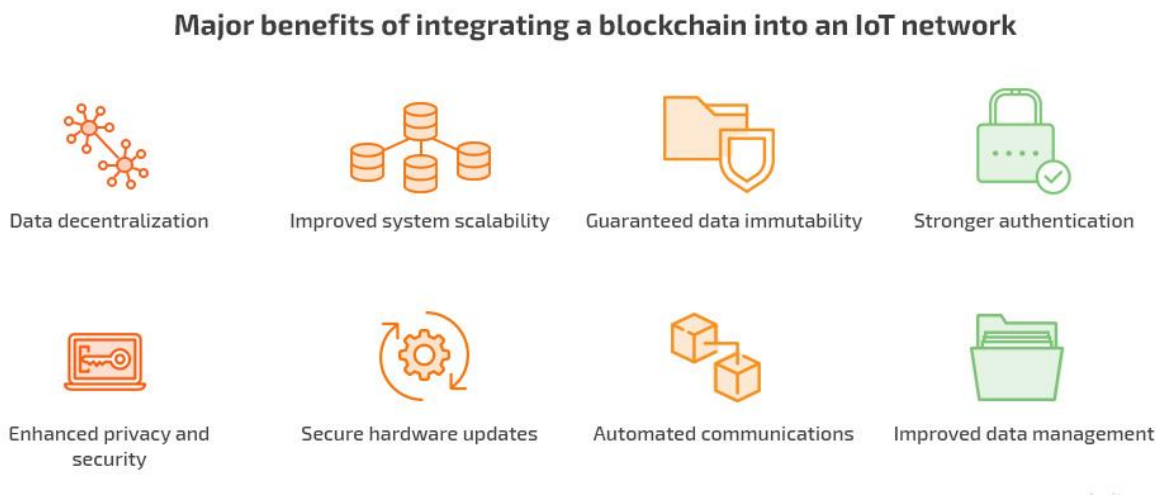

Figure 19: Benefits of Blockchain in IoT

2. Post-Quantum Cryptography for IoT

Post-quantum cryptography is developed in response to the danger brought about by quantum computers to existing systems of encryption which may be susceptible to attacks through brute force. In readiness for the era of quantum computers, new quantum-proof codes are being sought in relation to their cousin's, the devices connected to the internet. To this end, given that most of the IoT gadgets are resource constrained, it means that compromised by quantum-based attack also calls for light weight security measures that are still effective. For instance, in lattice-based cryptography and hash-based signatures, notions of post-quantum algorithms are researched to facilitate communication within the IOT bubble with inhibitions geared towards future quantum intrusion. [9]

3. Edge Computing Security for IoT

Edge computing modifies the data processing mode by bringing it close to the IoTs reducing the delays and enhancing the real time analysis. However, this increase in decentralization poses the new threat of security of data existing in many geographical places also known as edge nodes. Future trends tend to embed strong security measures enclave within the edge in order to be able to guard the data and services of the IoT. Edge computing means the applications are less dependent on the cloud infrastructure but puts the local sites in a compromising situation. The need to upgrade these edge nodes with encryption technologies, access control and secure boot mechanism will be paramount. In smart cities, traffic management lies with IoT devices with edge computing which can take in local traffic data

and handle incidents in a quicker manner, however, each node needs to be secured in order to restrict access.

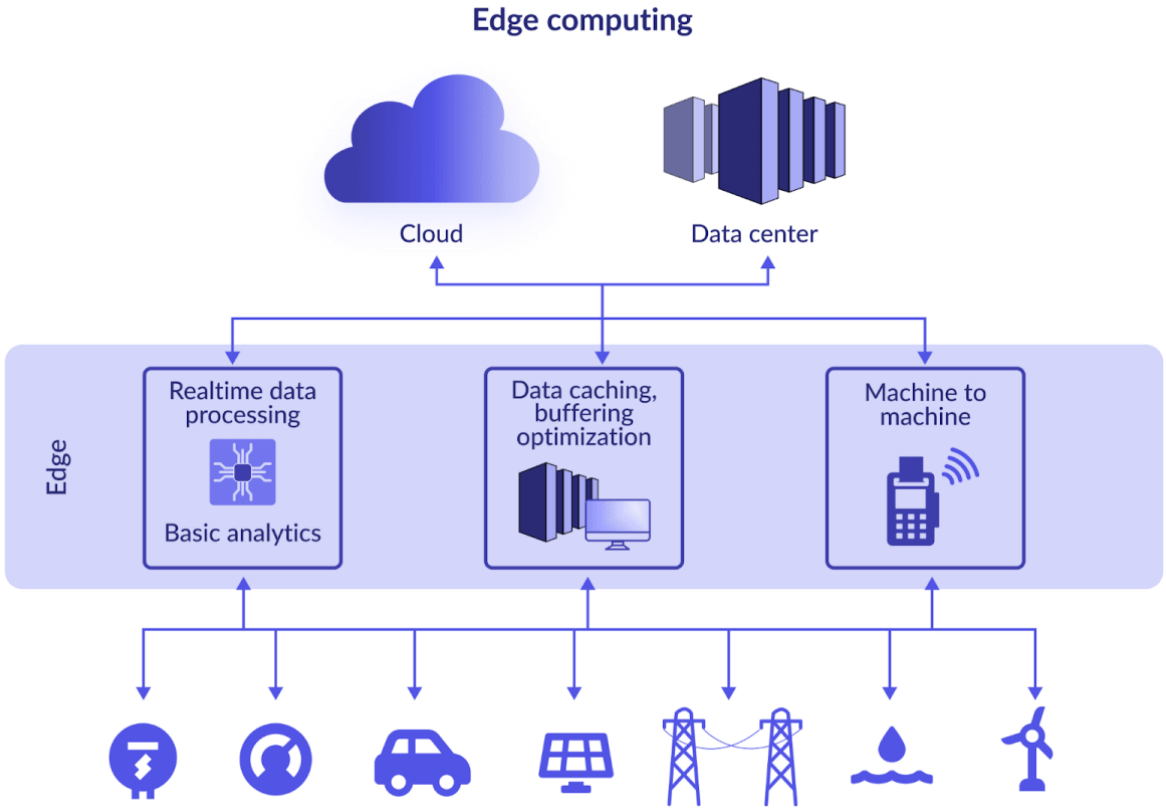

Figure 20: Edge Computing

4. Digital Twins for IoT Security Monitoring

The concept of a digital twin can refer to a virtual representation of a real-world object or system, where such object or system could be tracked, imagined or assessed in real-time. In the context of COI protection, the digital twin has capabilities that help in identifying and eliminating system threats as well as testing and providing a forecast of a potential threat in the system before it takes place. The technology is much better because the security boundaries associated with the IOT are all existing and active. There is no enforcement required since there is no physical penetration. Further, real-world systems' updating or enhancing procedures have also been practiced in a digital twin platform before doing it to the real system thus mitigating the causes of downtimes or mistakes. For example, the control systems of a digitally replicated factory's arcade can enable security forces to carry out

tactical testing of defense mechanisms against ransomware attacks by simulating the attacks themselves. [10]

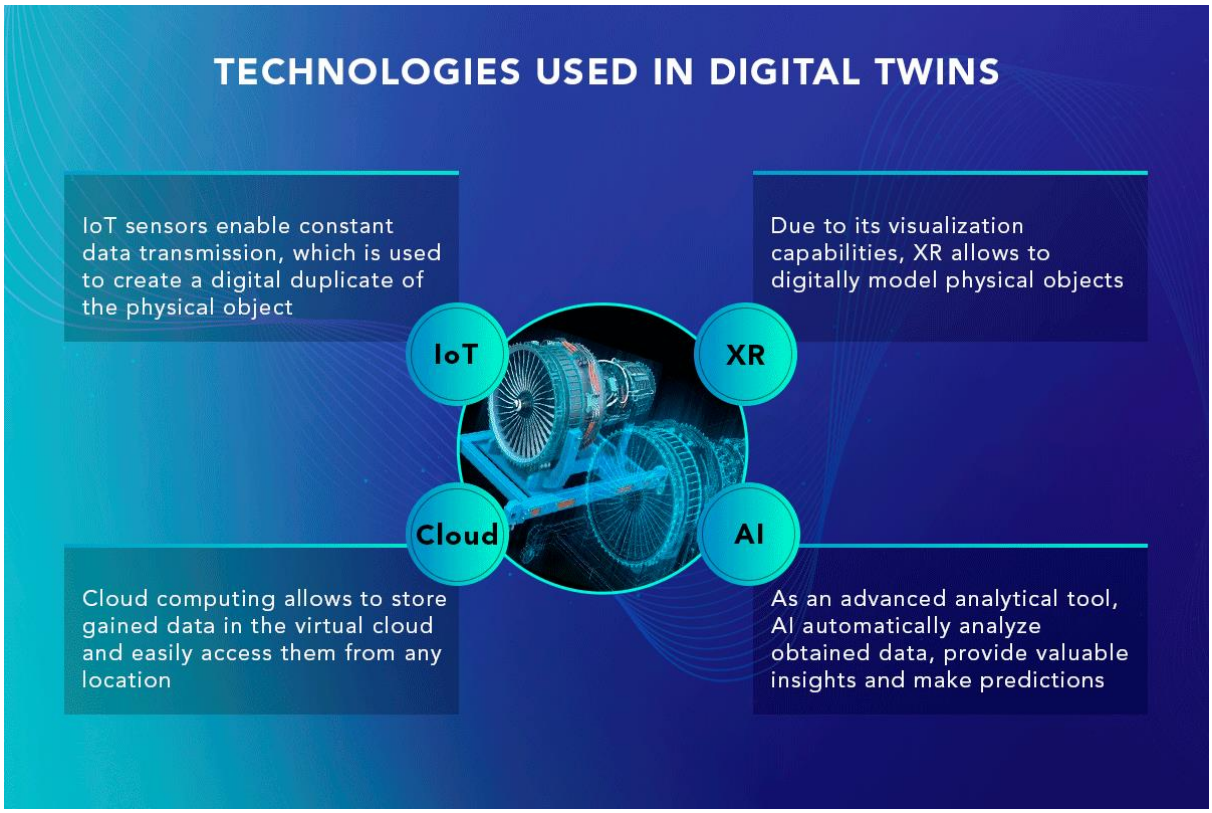

Figure 21:Digital Twin

Conclusion

As the Internet of Things undergoes further development, security has become a pressing issue to individuals and organizations as well as to the government. Most of the earlier IoT systems deployed barely had security as a priority. However, now, technologies such as the Zero Trust security models and Artificial Intelligence solutions have revolutionized the protection of devices and networks. Adoption of technologies such as blockchain, post quantum cryptography and edge computing in IoT networks is also promising in terms of future prospects. Nonetheless, a systemic approach must be employed to address IoT ecosystems security that utilizes the technology, regulation and trust management elements.

In the final analysis, the security of the Internet of Things will depend on the ability of manufacturers, service providers and end-users to engage in risk mitigating activities such as monitoring, enforcement of policies and innovation. New technologies for instance, such as digital twins, would provide even more possibilities in the prevention and management of risks in real time. With an upsurge in the openly interconnected world of IoT, it is imperative that sufficient security measures are advanced to protect the inter-connected systems in terms of safety, privacy and reliability.

References

[1] Pradyumna Gokhale, Omkar Bhat, Sagar Bhat, "Introduction to IOT," 2018.

[2] Rodrigo Roman and Javier Lopez,Stefanos Gritzalis, "Evolution and Trends in the Security of the Internet of Things," vol. 51, 2018.

[3] [Online]. Available: https://www.livinginternet.com/i/ia_myths_toast.htm.

[4] [Online]. Available: https://www.thingstel.com/blog/evolution-of-iot-over-the-years/.

[5] [Online]. Available: https://www.techtarget.com/iotagenda/definition/RFID-radio-frequency-identification.

[6] Kingsley Igulu, Barilemena Johnson, Agbeb Nornu Stephen,, "Security Challenges in IOT," researchgate, 2024.

[7] N. T. Y. Huan and Z. A. Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions," 2024.

[8] Jaspreet Singh,Gurpreet Singh,Gurpreet Singh, "Evaluating Security Principals and Technologies to," 2023.

[9] R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," no. Cyber Security and Privacy in IoT, 2021.

[10] Mayra Samaniego,Ralph Deters, "Digital Twins and Blockchain for IoT Management," 2023.