International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

Security And Privacy Concern In IoT Devices

Athira Anil[1], Athulya Ramesh Babu[2] , Joice Antony[3] , Kezia Elizabeth Vilson[4] , Soumya Koshy[5]

[1,2,3,4]UG – BCA Kristu Jyoti College of Management and Technology, Chethipuzha, Kerala, India
[5]Assistant professor, Department of computer application Kristu Jyoti College of Management and Technology, Chethipuzha, Kerala, India

ABSTRACT
The widespread adoption of IoT devices has revolutionized technology but has also raised security and privacy concerns. These challenges stem from interconnected nature, sensitive data generation, vulnerabilities in firmware, inadequate authentication, and insufficient encryption protocols. Privacy concerns arise from extensive data collection and processing capabilities, raising questions about user consent, data ownership, and potential misuse. Aggregation of data from multiple IoT devices can lead to comprehensive user profiling, potentially enabling intrusive surveillance and targeted attacks. To address these challenges, several approaches have been proposed. In this paper major issues related to the security and privacy of IoT are focused.
Keywords—: IoT security, IoT privacy, IoT , Hardware security, IoT attack

INTRODUCTION

The current technological tendency is to "connect the unconnected," which means that in the coming years any device that can be connected will be connected. The Internet of Things (IoT) is a network of physical items that are equipped with processing power and sensors to connect end users to wide-area networks for transmission. It is present all around us in things like cars, street lights, home appliances, medical equipment, and personal digital assistants like Google Home. IoT gateways, for instance, provide quick and simple access to the IoT world and are compatible with IoT servers (such as Microsoft Azure, Amazon AWS, IBM Cloud, Google Cloud, etc.) and specialized servers that handle MQTT. IoT devices are connected to the Internet on a global scale and exchange data via embedded sensors and software.

These gadgets minimize human effort required to make life easier and improve resource efficiency. These tools aid human decision-making and raise user-life standards. It's been almost 188 years since the first device was connected. When the first electromagnetic telegraph was developed in 1832, it was first used. At that time, the concept was referred to as "Embedded Internet" or "Pervasive Computing," and the first ever connected item was a Coca-Cola vending machine.

The importance and contribution of this research on IoT security and privacy are the well-being of humankind in accordance with people's preferences, wants, wishes, and desires without any explicit instructions to IoT devices. By assisting in surgery, weather prediction, wildlife identification, and vehicle tracking, these gadgets also benefit the community.

IoT is a developing technology due to the quick rise of intelligent devices, so it's crucial to comprehend the privacy and security issues. For the sake of people, it is essential to comprehend and deal with these difficulties. To manage these security and privacy issues in IoT, humans can benefit. Significant advice for IoT security and privacy issues are provided by this systematic literature review (SLR). 170 research articles were chosen as references in this study to conduct the survey for security and privacy issues in IoT

INTERNET OF THINGS (IoT)

The internet of Things, or IoT, is a network of interconnected computing devices, mechanical and digital machines, objects, animals, or people who can exchange data over a network without

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

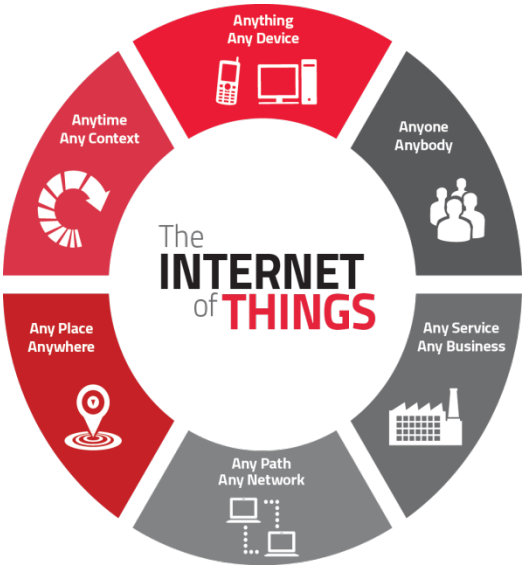
requiring human-to-human or human-to-computer interaction. The IoT can be defined in two ways based on

• Existing Technology
• Infrastructure

IoT based on existing technology: IoT is a new revolution to the internet due to the advancement in sensor networks, mobile devices, wireless communication, networking and cloud technologies.

IoT based on infrastructure: IoT is a dynamic global network infrastructure of physical and virtual objects having unique identities, which are embedded with software, sensors, actuators, and electronic and network connectivity to facilitate intelligent applications by collecting and exchanging data.

The main objective of IoT is to configure, control, and network the things that are typically not connected to the internet, such as thermostats, utility meters, Bluetooth-enabled headsets, irrigation pumps, sensors, or control circuits for an electric car's engine, in order to make energy, logistics, industrial control, retail, agriculture, and many other domains smarter.



LIMITATIONS OF IoT

The two major drawbacks in IoT devices are:

1. Battery life
2. Computing power

Extension to battery life:

Some IoT devices are solely constrained by the amount of energy needed to carry out the intended functions since they are utilized in locations without access to recharge. There are three approaches that may be used to solve this problem. The first is to utilize the bare minimum of safety requirements for the system, which is not really recommended if sensitive data is handled. The battery's power can be increased as a second option. However, the majority of Internet of Things cameras are small and light. There is no added capacity for a larger battery. The ultimate answer calls for power generation from natural resources (such as the sun, fire, wind, and agitation), however this would require upgrading the infrastructure, which would result in astronomical costs.

Computing Lightweight

In the context of the Internet of Things (IoT), computing "lightweight" refers to optimizing the computing resources and power consumption of IoT devices to ensure efficient and reliable operation within the constraints of low-power, low-memory, and low-processing capabilities that many IoT devices possess.

Here are some key considerations for achieving lightweight computing in IoT:

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

Edge Computing: Utilize edge computing, where data processing occurs locally on the IoT device or at the edge of the network, rather than sending all data to centralized cloud servers. This reduces latency and the amount of data transmitted over the network, leading to more efficient resource utilization.
Low-Power Hardware: Choose low-power microcontrollers or processors specifically designed for IoT applications. These components are optimized for energy efficiency and can perform the necessary tasks without draining the device's battery quickly.
Efficient Algorithms: Implement lightweight algorithms that require minimal computing power and memory. For example, use optimized data compression techniques, simple data filtering, and lightweight encryption algorithms suitable for resource-constrained environments
Data Reduction Techniques: Reduce the amount of data transmitted and processed. Use data aggregation and summarization methods to extract relevant information before sending it to the cloud or processing it locally.
Sleep Modes: Incorporate sleep modes and wake-on-event mechanisms to minimize the device's active time. This allows the device to conserve power when it's not actively performing tasks
Firmware and Software Optimization: Write efficient and optimized firmware and software to reduce processing overhead and minimize memory usage. Avoid unnecessary background tasks that could consume extra resources.
Protocol Efficiency: Select communication protocols that are lightweight and suitable for IoT applications, such as MQTT or CoAP, which have lower overhead compared to traditional protocols like HTTP.
Firmware and Software Updates: Implement efficient over-the-air (OTA) update mechanisms to minimize the size of firmware updates and optimize the update process.
Hardware Acceleration: If feasible, offload some computation tasks to hardware accelerators, such as dedicated cryptographic coprocessors or hardware for specific AI/ML tasks.
Cloud Offloading: For more complex tasks that cannot be performed on the device efficiently, offload computation to the cloud, but do so judiciously to avoid overwhelming the device or incurring excessive communication overhead
.

CHALLENGES IN IoT DEVICES

The term "Internet of Things" (IoT) refers to the interconnectedness of physical objects, such as vehicles, home appliances, and other goods, which enable these things to communicate and exchange data. These objects are embedded with electronics, software, sensors, and connectivity. The Internet of Things (IoT) idea entails expanding Internet connectivity to a variety of gadgets and common objects in addition to traditional devices like desktop and laptop computers, smartphones, and tablets. Offering enhanced device, system, and service connectivity that extends beyond machine-to-machine communications and encompasses a range of protocols, domains, and applications is the ultimate goal of the IoT.
The Internet of Things (IoT) has quickly expanded to play a significant role in how people live, interact, and conduct business. Web-enabled devices are transforming our universal rights into a larger switched-on space to live in all over the world. The Internet of Things is facing a variety of difficulties.

Security challenges in IoT :

1. Lack of encryption :-

Encryption is one of the biggest IoT security challenges even if it is a great technique to stop criminals from obtaining data.
These drives are accustomed to the processing and storage power offered by a conventional computer.
The end outcome is an increase in attacks where hackers may quickly change the security algorithm.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

2. Insufficient testing and updating :-

IoT (internet of things) makers are more eager to develop and deliver their gadget as quickly as possible without giving security much thought as the number of IoT devices rises.

The majority of these IoT products and gadgets do not receive enough testing and updates, making them vulnerable to hackers and other security risks.

3. IoT Malware and ransomware :-

Grows as the number of devices increases.

Ransomware exploits encryption to effectively lock out users from a variety of devices and platforms while retaining access to the important data and information of those users.

4. Inadequate device security :-

A lack of effective safeguards against cyber-attacks, hacking, data theft, and unauthorized access constitutes inadequate device security for electronic devices like computers, smartphones, and IoT devices. This can occur as a result of out-of-date software, weak passwords, unpatched vulnerabilities, a lack of encryption, and other security problems. To maintain the security and privacy of sensitive information kept on these devices, it is crucial to routinely update the software and put in place robust security measures. Many IoT devices have weak security features that are simple to exploit.

5. Lack of standardization :-

When there are no established standards or procedures in a given field or industry, it is said that there is a lack of standardization. Incompatibility between various systems, goods, or procedures could emerge from this, which would be confusing, ineffective, and less interoperable. Lack of standardization, for instance, can make it challenging for various devices and systems to communicate with one another and exchange data. This can be overcome and compatibility and uniformity ensured by establishing standards and procedures. It is challenging to consistently protect IoT devices due to a lack of standardization.

6. Vulnerability to network attacks :-

The ability of a network, system, or device to be infiltrated or abused by cybercriminals is referred to as vulnerability to network attacks. This could be caused by flaws in the network architecture, unpatched software, careless password management, or a lack of sufficient security procedures. Data theft, privacy violations, service disruptions, and monetary losses can all be caused by network attacks. Strong security measures, such as firewalls, encryption, and frequent software updates, should be put in place to lessen vulnerability to network attacks. Users should also be instructed on safe internet usage habits. Because Internet of Things (IoT) devices rely on networks, they can be attacked using DoS assaults and other types of attacks.

7. Privacy concerns :-

Issues with the gathering, keeping, using, and sharing of personal information are referred to as privacy concerns. This can involve worries about who has access to personal data, how it is being used, and if it is being safeguarded against unauthorized access or misuse. Private information is being gathered and kept on an unprecedented scale in the digital era, which has made privacy issues more crucial than ever. To resolve privacy concerns, people and organizations need to put in place the proper security safeguards to secure personal information, be open about how it is being used, and respect people's rights to govern their own information. In order to set standards and protect people's personal information, laws and regulations governing privacy have also been formed.

8. Software vulnerabilities :-

Software vulnerabilities are weak spots or errors in the coding of software that can be used by attackers to obtain unauthorized access, steal confidential data, or engage in criminal behavior. The usage of out-of-date or unsupported software can result in software vulnerabilities as well as flaws or mistakes committed throughout the development process. Attackers can take advantage of these flaws to take over a system, put malware on it, or steal confidential data. It is crucial for software developers to adhere to secure coding practices and for users to maintain their software updated and properly configured in order to lower the risk of software vulnerabilities. To further defend

DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

themselves from potential threats, businesses and people should put strong security measures in place including firewalls, antivirus software, and intrusion detection systems.

Design challenge in IoT :

The technical hurdles and trade-offs involved in developing connected devices that are both secure and functional are referred to as design issues in the IoT (Internet of Things). The following are some of the major IoT design challenges:

1. Interoperability:-

The capacity of various systems, devices, or components to function together effortlessly and exchange data efficiently is referred to as interoperability. Interoperability is a major issue in the Internet of Things (IoT) space since so many different types of devices are being connected to the internet. Lack of standardization in the IoT can cause communication and data sharing issues amongst devices, creating a disjointed and ineffective system. Organizations and industry groups are striving to create standards and protocols to guarantee interoperability across IoT devices in order to address this issue. This involves creating standard data formats, communication protocols, and security guidelines. The IoT's full potential and the capacity for linked devices to collaborate effectively and efficiently depend on interoperability. Ensuring that various IoT devices may communicate and exchange data effectively and effortlessly.

2. Security:-

In the Internet of Things (IoT), security is of utmost importance because it entails safeguarding sensitive information and systems against unauthorized access, theft, or damage. IoT devices frequently fall victim to cyber assaults because of their increased internet accessibility and their constrained computational power.

3. Scalability:-

A system's capacity to manage growing workloads or user populations without noticeably degrading its performance is referred to as scalability. Scalability is a significant issue in the Internet of Things (IoT) setting since there are an increasing number of connected devices, which generates a growth in data and communication volume.

4. Reliability:-

The capacity of a system to carry out its intended function repeatedly and without error is known as reliability. Reliability is a crucial issue in the context of the Internet of Things (IoT), as the failure of even a single IoT device can have serious repercussions.

5. Power consumption:-

The quantity of energy used by a system or device is referred to as power consumption. Since many Internet of Things (IoT) devices are made to be compact, low-power, and battery-operated, power consumption is a major concern in the IoT space.

Deployment challenges in IoT :

The implementation of Internet of Things (IoT) systems might bring a number of difficulties, such as:

1. Connectivity :-

When integrating devices, programs, and cloud platforms, it is the main worry.

It is incredibly important to have connected devices that offer essential information and front. However, where IoT sensors are needed to monitor process data and provide information, insufficient connectivity poses a problem.

2. Cross platform capability :-

Future technical advancements must be considered when creating IoT applications.

A balance between the functions of the hardware and software is necessary for its development.

Making ensuring that the device and IoT platform drivers work at their peak levels despite high device rates and fixes is a problem for developers of IoT applications.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

3. Data collection and processing :-

Data is a key component in IoT development. The processing or usefulness of the stored data is more important in this case.

Development teams must make sure they prepare adequately for the way data is gathered, kept, or processed inside an environment in addition to security and privacy.

4. Lack of skill set :-

Only with the right kind of experienced resource working on the IoT application development will all of the development issues listed above be overcome.

When developing IoT applications, having the proper talent can help you overcome the biggest obstacles every time.

5. Integration:-

Ensuring smooth integration of IoT systems and devices with current infrastructure and technology.

6. Network infrastructure:-

Constructing and maintaining the network infrastructure required to support the large number of IoT devices that are linked.

7. Device management:-

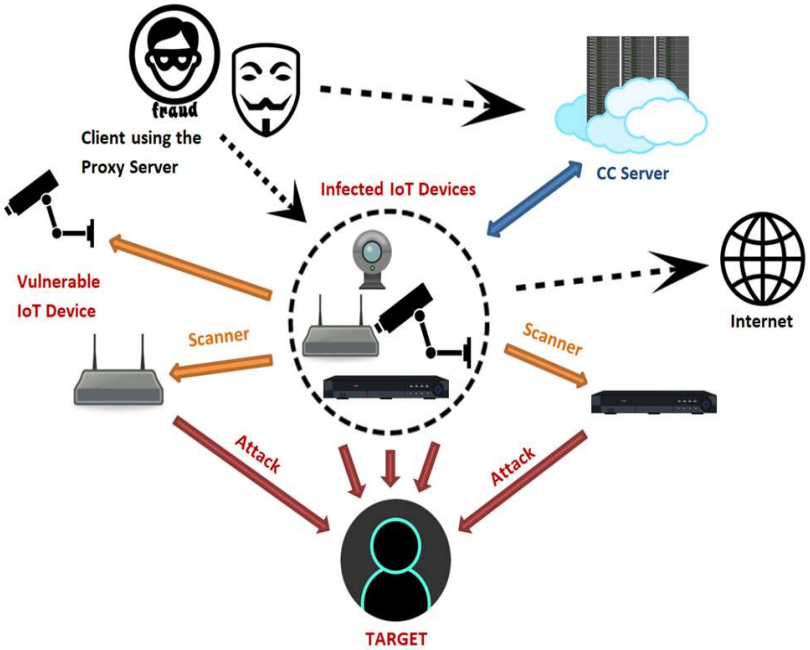
Handling and sustaining the vast deployment of IoT devices effectively.

8. Data management:-

Managing, processing, and analyzing the massive amounts of data created by IoT devices and integrating it with current data systems.

9. Security:-

Ensuring that the deployment of the Internet of Things is protected against threats including cyber-attacks, data breaches, and unauthorized access.



DIFFERENT ATTACKS ON IoT DEVICES

IoT security is a significant concern since it is dynamic, diverse, and has many tools that are networked. The opposition will attack the Internet of Things system via flaws in the protocol, malicious software, or by cryptographically breaking these nodes.

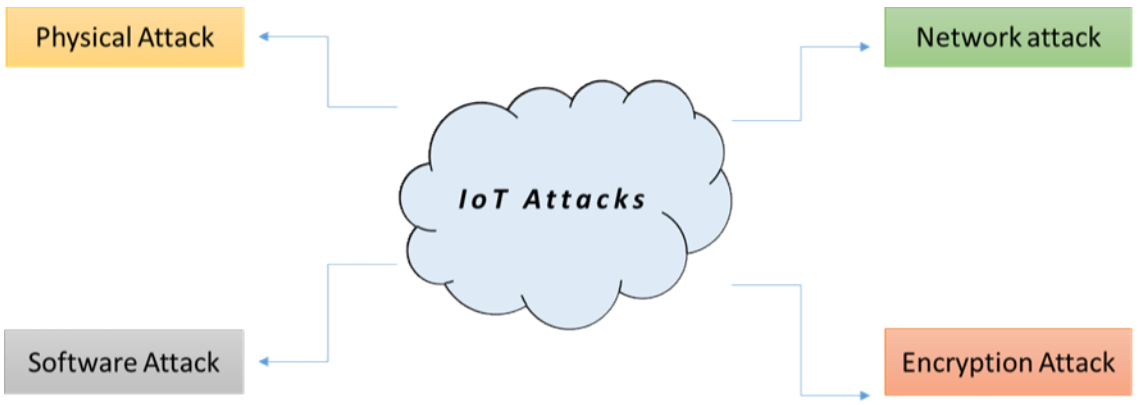
(Like a physical vulnerability) by causing harm to them, taking advantage of them, or deploying malicious software.

Shows, These faults allowed the assault to be divided into four groups: physical, network, software, and encryption attacks. This group's attack as a whole is regarded as one of the most hazardous.

Malicious injection node attack was a dangerous attack that came after a physical attack.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

The papers have still been modified since the services are not just halted.
The most dangerous threat comes from Sinkhole's network attack. Additionally, it can result in dangers including selective routing, packet alteration or reduction by an attacker, and it can draw all traffic to the base station. Worms from a system attack were chosen as the most unreliable threat. Worms are perhaps the most harmful and destructive type of internet malware. The auto replication programmer uses security holes in network software and hardware, which harms the machine. Without your knowledge, it may remove device files, steal data such as passwords, change passwords, activate screen locks, and more. The report divides IoT threats into four main classes based on physical, network, and cryptographic characteristics. While the intrusive party is close to the IoT, the physical attack starts. Network assaults take place when an attacker gains access to the IoT network, and a specific machine is used to cause harm. There are several flaws in the IoT application programmer attack that allow the attacker to access IoT devices via which the vulnerable code is used. Finally, an encryption attack will take place after the IoT encryption has been broken. The study found that in order to allow only authorized users to access and power IoT devices, a number of security measures were required for IoT, including authentication, digital certificates safeguarded booting, privacy encryption, and dependable software. In reaction to the abuse from other investigators



1. **Physical Attacks:-**

The hardware in IoT devices was the focus of several attacks:
• Lack of Sleep: The attacker seeks to shut nodes with higher power.
• WSN Node Jamming: The hacker obstructs wireless communication by interfering with the usage of a jammer. It makes denial-of-service assaults possible.
• Tampering node: The attacker modifies the node in order to gain access to private data like an encryption key.
• RF Interference: The server is attacked by the intruder using radio frequency waves to deny the service. When in touch with RFID, this signal is utilized.
•Physical damage attack: The intruder physically damages IoT device components, which results in a service denial.
• Injection of malicious code: The adversary physically installs a malicious code into the IoT node. IoT device power should be fully available to the intrusive party.
• Social engineering: The offender physically interacts with IoT device users and chats with them. The intrusive party obtains sensitive data to further its goals.

2. **Network Attacks:-**

The IoT system's server is the target of the assaults.
Utilize a wireless network assault, a router attack, etc. to get access to the network.

DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

• RFID spoofing happens when an attacker uses a fake. The gadget then receives the information sent by an RFID tag and records it. Attacks that use spoofing contain false information that appears to be accurate and that the computer recognizes.
Attacks on traffic analysis occur when a hacker intercepts and examines messages to get network intelligence.
• RFID Unauthorized Access: In RFID systems, the adversary can see, modify, or destroy node information if the proper authentication is not allowed.
•Sinkhole Attack: An adversary adopts a sinkhole attack and uses this node inside the network to launch an attack. The node in issue draws traffic because it provides its neighboring nodes with incorrect routing information. The data is then altered, and the packet size is decreased.
• Internet communication between the two nodes is cut off in middle attacks. By waking up, you learn crucial facts.
• Sybil Attack: In this attack, a malicious node impersonates and acts as several nodes. For instance, in a wireless sensor network, a single node device will cast many votes.

3. **Attacks on Software:-**

The attacker uses malware, worms, spyware, etc. to target victims and steal papers, disable facilities, etc.
• Harmful files: The intrusive party could have gained access to the computer and installed harmful scripts.
• Phishing Attacks: Through email spoofing and subpar websites, the attacker gains access to personal data including usernames and passwords.

4. **Encryption Attacks:-**

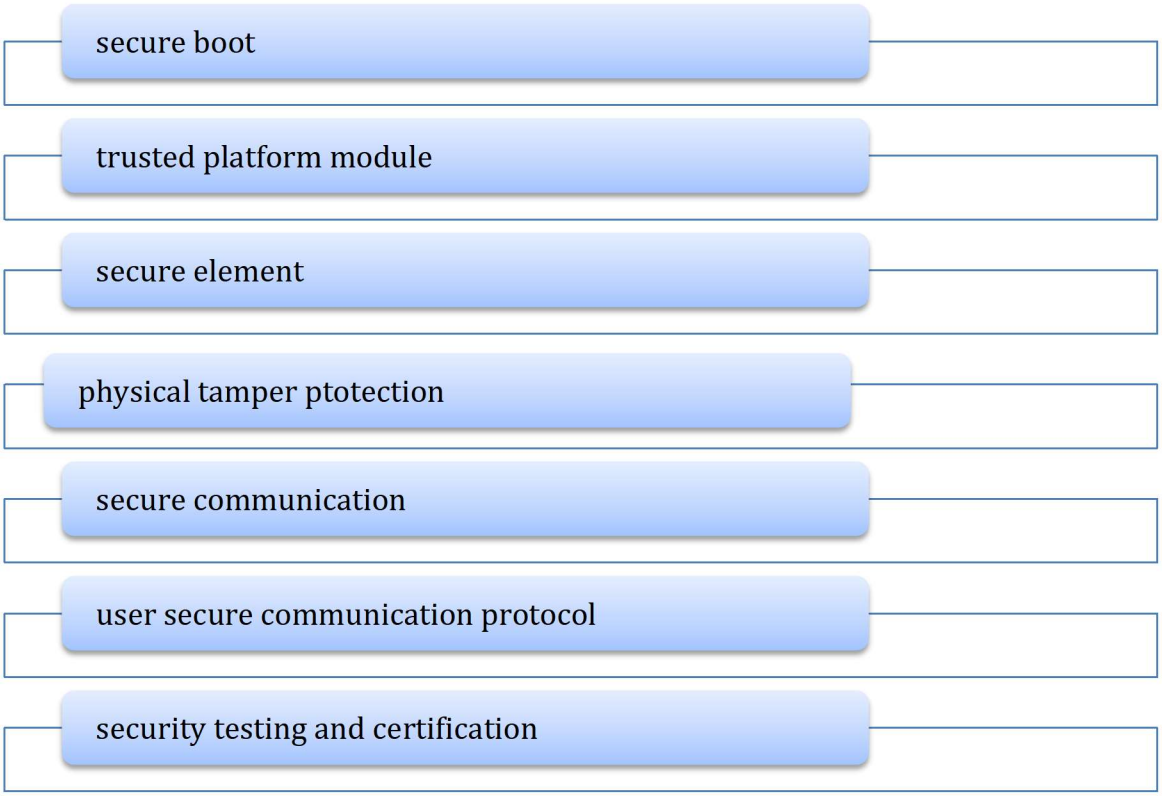
Threats are based on the private key and the broken encryptions.
• Attacking the side channel: The hacker makes advantage of the system's side channel information to encrypt it. The text contains information on performance, time required, amount of faults, etc. but not chip text or plaintext. Attackers utilize this information to find the encryption key. There are several side-channel attacks that target time, including timing assaults, basic and differential power analysis, and differential fault analytics.
Attacks that use timing rely on how long actions take. It provides details on the hidden keys. Cryptosystems take in different inputs at different times. The hitting of RAM cache, the instructions running during unfixed time, etc.
• Cryptanalysis An attack: In this instance, the opponent extracts the encryption key using either plaintext or cypher text. Depending on the methods employed, several types of assaults are conducted.
Text attack using cyphers, known plaintext assault choosing a text assault (plaintext, chip text, or midwayer).

HARDWARE SECURITY IN IoT

Hardware security is a crucial aspect of IoT (Internet of Things) devices as they are often connected to networks and handle sensitive data. Ensuring robust hardware security is essential to protect against potential attacks and safeguard the privacy and integrity of the device and its data. Here are some key considerations for hardware security in IoT devices:
Secure Boot: Implement a secure boot process that verifies the authenticity and integrity of the firmware and software during the device's boot-up. This prevents the device from running unauthorized or tampered code.
Hardware Encryption: Utilize hardware-based encryption modules to protect data both at rest and during transmission. This ensures that sensitive information remains confidential and cannot be easily intercepted or tampered with.
Trusted Platform Module (TPM): Incorporate a TPM or similar hardware security module that provides secure key storage, cryptographic operations, and device authentication. TPM helps prevent unauthorized access to the device and its data.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

Secure Element: Consider using a separate secure element or a dedicated hardware security chip for storing sensitive information, such as cryptographic keys and credentials. This isolation enhances security by preventing direct access to critical data.
Physical Tamper Protection: Implement physical tamper-resistant mechanisms to detect and respond to any attempts to physically access or compromise the device's hardware. This may include intrusion detection switches or anti-tamper coatings.
Secure Communication: Use secure communication protocols (e.g., TLS/SSL) to protect data transmitted between the IoT device and other connected systems. Encryption ensures data confidentiality and prevents man-in-the-middle attacks
Use secure communication protocols (e.g., TLS/SSL) to protect data transmitted between the IoT device and other connected systems. Encryption ensures data confidentiality and prevents man-in-the-middle attacks
Security Testing and Certification: Regularly test the hardware for vulnerabilities and perform security audits to identify and address potential weaknesses. Seek third-party security certifications to demonstrate compliance with industry standards and best practices.
By integrating these hardware security measures, IoT devices can significantly reduce the risk of security breaches and provide a more trustworthy and reliable experience for users. However, it's important to note that hardware security is just one part of the overall security strategy, and a holistic approach that includes software security, network security, and user education is essential for comprehensive IoT device security

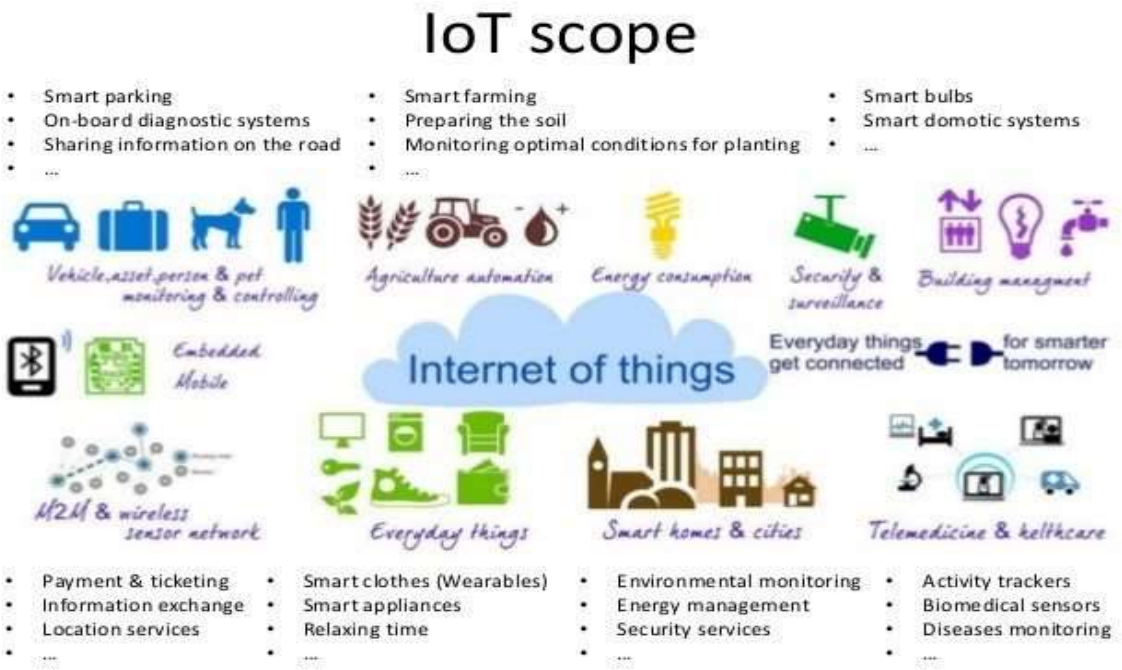


FUTURE SCOPE OF IoT
The future of ioT is bright,with many emerging trends and applications set to transform industries and improve our daily lives.
The future possibilities of ioT are limitless.
There are some Applications and the future scope of IoT in various sectors.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

*Healthcare: IoT in healthcare helps to provide advanced healthcare facilities to patients, doctors, and researchers.
*These facilities include smart diagnosis, wearable devices for tracking health, and patient management.
*The healthcare devices can directly send the patient's data health to doctors over a safe network.
*There is a decrease in manual errors in diagnosing patients .thus, patients can get proper treatment on time.
*The treatment of patients in the physical absence of doctors has become possible.
*The scope of IoT is helping the healthcare sector give proper treatment to the needy.
*Agriculture: one of the basic human needs is food. To fulfill the need for food, we do farming.
The agriculture industry is facing many challenges. To meet the rising demand for food, the industry has hence adopted technology to increase productivity.
There are three Applications:
*Precision farming: the technology uses sensors to calculate the moisture of soil, humidity, and temperature.
*precision farming helps farmers monitor their fields and boost productivity.
*Agricultural drones: Drones used for agriculture and farming are one of the best applications of IoT.
*They are used to enhance agricultural processes.
*With the help of drones, it becomes easier to evaluate the health of crops.
*Audio bridge: commonly referred to as the wireless HiFi system it connects wireless speakers to the audio bridge. This home automation system is also capable of playing the same songs in each room. this can be controlled by any digital device from your phone to your smartwatch.it also brings in simplicity as you can play music sitting in any area of your house.
*Edge Computing: one of the most significant trends in IoT is the move toward edge Computing.
*It involves processing data on the device itself, rather than sending it to the cloud for analysis.
*It helps to reduce latency, improve reliability and enhance privacy and security.

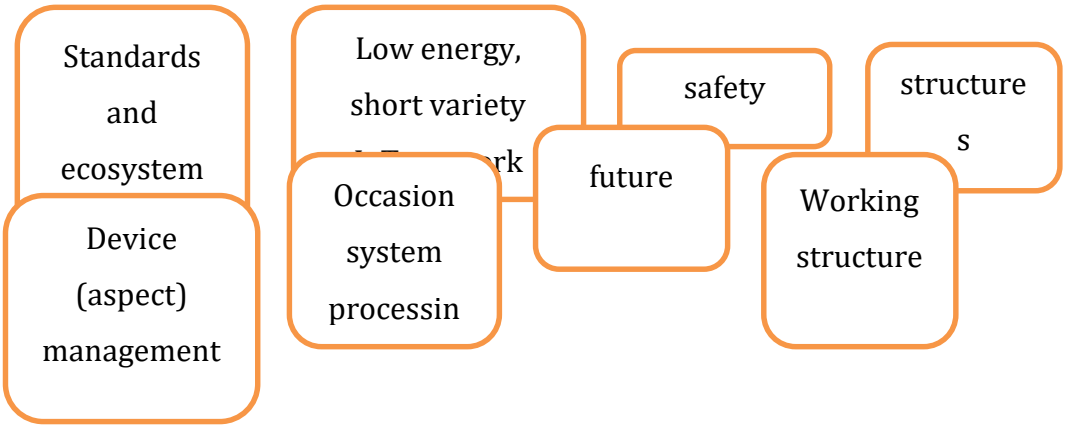
Internet of Things (IoT)



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.7 July - August – 2023
DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

FUTURE OF IoT

IoT contains the flaws and weaknesses of outdated network designs since it uses the standard network architecture to interact amongst numerous devices. To a significant part address performance and safety-related issues, the current network design must be enhanced, or a new lightweight, efficient, and safe network architecture must be built. The issues and safety layers on each network tier will be addressed in a future article, the authors anticipate. This paper examines security and privacy issues related to IoT devices from a number of angles. It also provides defenses against attacks on IoT systems. There are various efficient alternatives available for protecting IoT systems and sensitive user data. However, the attackers want to make their assault methods more potent and successful. Stronger IoT system protection solutions must be offered as a result of this. Based on the data and information offered in this survey report, a practical solution for safeguarding IoT systems may emerge in the future. a solution that reduces risk and makes it possible for IoT systems to remove the majority of dangers. an answer tailored to the nature and architecture of IoT systems.



It is clear from the literature reviews mentioned above that there are many components of IoT protection and that there are various countermeasures needed to improve it. Because of how important these issues are, many research projects have focused on them. This portion of the study demonstrated how researchers offered several significant elements and various IoT security issues.
To a significant part address performance and safety-related issues, the current network design must be upgraded, or a new lightweight, efficient, and safe network architecture must be built. The issues and safety layers on each network tier will be addressed in a future article, the authors anticipate. This paper examines security and privacy issues related to IoT devices from a number of angles. It also provides defenses against attacks on IoT systems. There are various efficient alternatives available for protecting IoT systems and sensitive user data. However, the attackers want to make their assault methods more potent and successful. Stronger IoT system protection solutions must be offered as a result of this. Based on the data and information offered in this survey report, a practical solution could be available for safeguarding IoT devices in the future. a procedure that reduces risk and makes it possible for IoT systems to get rid of the majority of dangers. a solution that takes the nature and design of IoT systems into account

CONCLUSION

In order to inform consumers of the dangers involved with using these devices, this study highlights the main security issues with IoT systems. IoT hazards have been divided into many groups for easier understanding. Additionally, a thorough comparison of each class is included. Network attacks are those that involve malicious nodes being injected into a network to steal information packets and slow the network down. Attackers use side-channel assaults to concurrently attack security and privacy. Attackers who use cryptanalysis get access to the decryption key to transform encrypted text into plaintext. Attackers use the restricted resources available in access-level assaults

DOI:10.46647/ijetms.2023.v07i04.065 ISSN: 2581-4621

to steal or modify the data. Attackers read and alter message packets during active attacks, whereas they can read messages during passive assaults but can not alter them. Attackers use a variety of tactics during assaults at the strategic level to insert malicious malware into IoT devices. Physical assaults are those that involve physical contact and harm hardware; they are also known as that. Logical attacks are those that may be carried out remotely. IoT assaults are divided into internal and external attacks based on the location of the adversary. An attacker might be an insider with knowledge of the targeted IoT system or an outsider with no knowledge of the system. In assaults when the hardware has been hacked, the attacker tampers with it to take data. Software assaults include the deliberate introduction of harmful applications onto the system to allow unauthorized access. Hackers can access these IoT web apps, databases, or servers because of bad coding. Firmware assaults are those launched as a result of outdated firmware not being present.

Additionally, we divided these areas into subcategories. In order to assist manufacturers in protecting IoT systems, this systematic literature analysis discusses more than 75 IoT security vulnerabilities. In the present day, cutting-edge technologies like cloud computing, fog technology, artificial intelligence, and machine learning are combined with IoT technology to address security and privacy issues. IoT security challenges may be resolved more effectively and affordably by using these new technologies, particularly blockchain technology. We conclude our review article by outlining a few areas for additional IoT security research that we believe need more investigation.

REFERENCES

1. S. Chaudhary, "Privacy and security issues in the Internet of Things," vol. 3, pp. 2433-2436, 2017

2. Reben Mohammed Saleem Kurda, 2 Umran Abdullah Haje, 3 Mohammed Hussein Abdulla, 4 Zhwan Mohammed Khalid “A review on privacy and security of internet of things” (Vol.10, No.4, 2021

3. N. C. Winget, A. R. Sadeghi, and Y. Jin, “Invited: can IoT be secured: emerging challenges in connecting the unconnected,” in Proceedings of the 53rd Annual Design Automation Conference, pp. 1–6, New York, USA, 2016.

4. A. S. Genadiarto, A. Noertjahyana, and V. Kabzar, “Introduction of Internet of Thing technology based on prototype, vol. 14, no. 1, pp. 47–52, 2018.

5. K. Hamid, M. W. Iqbal, A. U. R. Virk et al., “K-Banhatti Sombor invariants of certain computer networks,” Computers Materials & Continua, vol. 73, no. 1, pp. 15–31, 2022

6. A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Generation Computer Systems, vol. 108, pp. 909–920, 2020.