IOT IN PERSONAL DATA SECURITY

S.V.Sakthivel[1],K.Niranjana[2],B.Amrita[3]

[1]Student, Department of IT, Coimbatore Institute Technology, Coimbatore (India)
[2] Student, Department of CSE, SNS College of Technology, Coimbatore (India)
[3]Student, Department of Robotics and Automation, College of Technology, Coimbatore(India)

ABSTRACT - *This paper gives a detailed analysis of personal data and security on Internet of Things (IoT).The Internet of Things (IoT) has a vision in which the internet extends into the real world, which incorporates everyday objects. This explains how the internet of things is focused on safeguarding connected devices and network.Privacy and security are among the numerous challenges of the web of Things (IoT). Improper device updates, lack of economical and strong security protocols, user unknowingness, and famous active device watching are among the challenges that IoT is facing. During this work, we have a tendency to explore the background of IoT systems and security measures, and distinguishing (i) totally different security and privacy problems, (ii) approaches want to secure the parts of IoT-based environments and systems, (iii) existing security solutions, and (iv) the simplest privacy models necessary and appropriate for various layers of IoT driven applications.*

Keywords: Internet of things, Privacy, Applications,Devices,Security,VPN

1. INTRODUCTION

We live in an exceedingly new era of computing, info, and communication technology. As several areas unit oral communication, it pushes forward seamless interaction between humans, nature, and physical objects and is captured among the ecosystems of IOT. It is outlined because the interconnection via the web of computing devices embedded in everyday objects, facultative them to receive and send knowledge.The main motive of the web of things is to create the objects or things to be connected through the web , wireless detector network and sensible phones, in order that they'll share info mechanically.

IOT Security may be understood as a security strategy and protection mechanism that specially safeguards from the chance of cyberattacks on IOT devices that are unit connected to the network and advisedly engineered for a set of functionalities.

2. EXISTING SYSTEM

The IoT framework aspires to attach anyone with anything far and wide.It allows devices to act, collaborate and learn from each other’s experiences a lot like humans do. IoT usually features a 3 layers design which consists of Network,Perception and application layers. A variety of security principles ought to be implemented at every layer to attain a secure IoT realization.Of the 21.7 billion active connected devices and users worldwide, 54% are IoT device connections at the top of 2020;by 2025, it's expected that there will be at least thirty billion IoT connections, there will be a minimum of four IoT devices per person on an average.Being one amongst the foremost promising technologies the long run of IoT framework will solely be ensured if the protection problems related to its field is addressed and resolved.Government agencies including the “Federal Trade Commission” are apprehensive about the problems like knowledge security, mobile privacy, and massive knowledge. The progress of IoT means firms preserve privacy. Among other conditions, this involves adopting privacy and information security practices, only collecting and holding information with specific consumers consent, and providing them with access to their information.

2.1 Significant real-time IoT applications include

1)Wearables:
Wearable technology is an evident structure of IoT applications and probably is one of the earliest technologies to have deployed. We witness Fitbits, heart rate monitors and smartwatches everywhere having various merits.

2)Home applications:
The most common applications of home automation include light controls, HVAC(Heating, ventilation, and air conditioning), outdoor lawn irrigation system, kitchen appliances and security systems.It also includes gardening,security, air quality, water-sprinkler monitoring, voice assistants, switch boards and locks.

3)Health care:
IoT also improves the current devices in precision,efficiency and compatibility. It focuses on creating systems and implementing them rather than just equipment.IoT opens ways to an large environment of important data through analysis, real-time field data, and testing.

4)Industrial automation:
Industrial automation is one of the prominent fields where both faster developments and quality of products are the critical factors for a higher return on investment. With the applications of IoT, one could re-model products to deliver a better performance in both price and customer satisfaction.

5)Smart Speakers:
A smart speaker is much like a normal speaker including a microphone.It is basically an audio chipset powered with voice assistants such as Google Assistant, Amazon's Alexa, Microsoft's Cortana or third party voice assistants.

6)Agricultural statistics:
IoT in agriculture utilises robots, drones, remote sensors and computer imaging combined with progressive machine learning techniques and analytical tools for examining crops, surveying and scheduling the fields and providing useful information to farmers for efficient farm management to utilize time and money productively.

Most of the applications have encountered a minimum number of security breaches and should be resolved to attain its most efficient state.Some of the security challenges in IoT include Insufficient testing and updating,IoT malware and ransomware,IoT botnets aiming at cryptocurrency,Brute forcing,issues of default password and remote vehicle access.

2.2 Implementationof Existing Security Solutions into IOT

Encryption

As major IoT enabled devices will be battery operated, keeping this constraint along with the use of low processing power algorithms, encryption can be done for data integrity throughout transporting of data.

Virtual Private Network

Virtual Private Network (VPN) is networks that can be accessed from outside formed by a close group of partners. Only partners will be able to access the system and they can promise to make personal data confidential and data integrity is maintained. Virtual private networks do not provide the facility of dynamic global information exchange and you are bound to a limited area which makes this privacy enhancing technique effective but not plausible.

Text Dependent and Text Independent Voice Verification

Voice biometrics is the concept of using a person’s voice as a uniquely identifying characteristic. This technology can be implemented in smart speakers (such as homepods, Alexa), to improve the security system by having the device answer authenticated voices preventing the device from giving out information to strangers.

3. PROPOSED SYSTEM

IoT devices have scarce resources thus we have a tendency to cannot use complete security suites. We've got to style a special security framework or make a choice from existing solutions. we've got to appear towards light-weight security solutions to form IoT secure as a result of this may place a burden on device resources. To do so, we have a tendency to use good|a sensible| a wise} home IoT design that permits users to act with it through varied devices that support smart house management, and that we analyse completely different situations to spot doable security and privacy problems for users.

3.1 Investigating New Technological Approaches Towards Security

Using RFID for authentication:

RFID (Radio Frequency Identification) plays a main part in the identification of objects. It uses electromagnetic induction and propagation of electromagnetic waves to identify objects. From a security point of view, RFID can also be used against reproduction, combined encryption, and secure data on document, certificate, and other elements for the purpose of anti-counterfeiting and their control and management.

Security analytics and threat prediction using AI:

Not only must security-related data be monitored and controlled, it must also be used to predict and analyse future threats. They have to complement traditional approaches that look for activities that fall outside of an established policy. Prediction will require new algorithms and the application of artificial intelligence (AI) in the IoT to access non-traditional attack strategies.

Implementing hardware security among IoT devices:

Although many techniques have been developed to detect Hardware Trojans during pre-silicon and post-silicon tests, it is very difficult to trigger and detect all types of Trojans. Runtime monitoring monitors the chip’s behaviour or operating conditions to detect hardware Trojans during the chip’s run-time. On detecting abnormalities during run-time, they can disable the chip, or trigger other security measures to reduce the effects of HTs and provide a reliable operation.

4. CONCLUSION

The Internet of Things (IoT) referring to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human interventioncan connect various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities.Amidst all the substantial services,it also has minimal muddles and security setbacks;which when resolved can reach its most progressive and potent state in the near future.

5. REFERENCE

[1] Aqeel-ur-Rehman1, Sadiq Ur Rehman2, Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan [2016] International Journal of Communication Networks and Information Security (IJCNIS) Security and Privacy Issues in IoT.

[2]Chacko, Anil, Hayajneh, Thaier[2018] Security and Privacy Issues with IoT in Healthcare, EAIEndorsed Transactions on Pervasive Health and Technology.

[3] Trojans, Simranjeet Sidhu, Bassam J. Mohd and ThaierHayajneh[2017] . Journal of *Sensor and Actuator Networks,* Hardware Security in IoT Devices with Emphasis on Hardware.

[4] https://epic.org/privacy/internet/iot/

[5] https://www.edureka.co/blog/iot-applications/

[6]https://www.researchgate.net/publication/300413927_Internet_of_things_IoT_security_Current_status_challenges_and_prospective_measures

[7] https://www.emnify.com/en/resources/iot-security

[8] https://www.peerbits.com/blog/biggest-iot-security-challenges.html