International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Future of IOT and Biometrics

Assistant, Prof. Ms. Kalpana N Rode (ME Electronics)*, Ms. Aditi Amol Chiparge**, Ms. Sakshi Jitendra Khot, Ms. Sneha Anil Patil*******

*(Electronics and Telecommunication, Sharad Institute Of Technology College Of Engineering, Yadrav-Ichalkaranji Email: knrode_sit@rediffmail.com)

**(Electronics and Telecommunication, Sharad Institute Of Technology College Of Engineering, Yadrav-Ichalkaranji Email: khotsakshijitendra@gmail.com)

ABSTRACT

The human- to -machine and human -to- human communications are transforming to machine-to-machine communications by which several decision - making systems can be built. When different internet enabled smart devices interact with each other to achieve a goal (application depended), then a network is formed in which different sophisticated technologies will integrate to each other to formInternet of Things . It encompasses The vast amount of diverse smart devicee ,which collaborat with each other to achieve different smart applications like smart cities,connected cars , automated agriculture,and so on . Through radio-frequency identification (RFID) , wireless,mobile and sensor technologies make lot feasible ,but it suffers from many challenges like scalability, security is one of the primary concerns in loT. Without proper security and privacy,the buisness model of loT will not succeed.This chapter discusses the secure solutions for loT using blometric features of users as well as end users .The chapter will demonstrate thet biometric security is most feasible, reliable and efficient with respect to other existing security arrangements.

INTRODUCTION –

The internet of things (loT) is the interconnection of different devices of our daily life like cars, refrigerator, Mobile phones,smart doors ,devices for patient monitoring or any other monitoring devices .These devices are attached with smart sensor RFID tag ,actuator ,and network connectivity,which enable the devices to exchange or collect and send data to a server. This type of technology is called internet of things . loT is basically the combination of different fundamental types of technology and has different layer of communication level (ssc fig.19.1). Different level demands require different degrees of security arrangements.

TYPES –

LoT security is the domain ,which worries researchers and users due to the vulnerable attach on things or connected devices and network. The maximum connection in LoT is derived from the devices, embedded sensor system employed in industrial communication, building computerization system ,Vehicle communication and wearable gadgets. Therefore, devices which are connected in this giant network also raise the scope of potencila attack for hackers and other cyber criminals . There are five types of attack that occur in LoT internet working system.

•Botnet is network of system,which take control remotely. Command and control server is used to regulate the system and used by criminals for stealing private information. , exploiting online banking data and phishing emails .

•Man-in-the middle attack in the notion where the invider or hacker interrupts and breaks communication link between two discrete system. The invader covertly interrupt and sends fake messages but the sender and receiver believe that they are commenicating via authentic message with each other .

•Data and identity theft occurs in the case of careless handling the internet connected devices such as mobile phones ,Kindle ,smart watches,etc. The goal of identity theft is accumulation of data ,which can say a lot about a person . The information accessible on the internet ancluding social media and smart device.

ROLE –

Biometrics provide a secure way to transfer data as well as identify data ports and devices and ensure that they remain secure and their data intact. Biometrics are an optimal security measure, and their continued development will be a key component to creating difficult to breach security protocols. Since the characteristics identified by biometric scanners do not change and are unique to each individual, they make a very secure means of communicating data and creating identifiers for sharing secured data.Stronger than encryptions or password protections–both of which can be breached with practice and patience– biometric characteristics are extremely difficult to duplicate or fake. This feature alone makes them worthy of consideration in any security system.The growth of the biometrics industry will continue at a fast pace, and biometrics will continue to penetrate all levels of technology. With a need to keep data secure and the ease of integration into a variety of systems, the technology will continue to expand and will help develop seamless data transfer that is as secure as possible. Making the connections that are important to the IoT and the recommendations that end users have come to rely on, the role of biometrics will grow and evolve as the IoT continues to grow and evolve. The unique nature of biometrics and the myriad of ways that they can be used is likely to play a pivotal role in the growth of the IoT.

BENEFITS –

One of the most essential pieces of security is consent and validation of individuals – which is why so many companies are using biometric input devices. Biometric security systems are becoming a key element to multifactor authentication and used for a wide variety of purposes - such as attendance, tracking the authentication process, and even the metering time limits. A growing number of Iarge companies' entry and exit system are now based on biometrics. As there are various ways of conducting biometric verification - incIuding facial and iris recognition, vascular pattern recognition and even fingerprints - biometrics is a complex issue. Lets us look at some of the key benefits associated with this growing component of multifactor authentication:

Quick and Accurate Identification and Authentication

Using passwords and codes for security access is pretty straightforward but generic. Anyone with a card or pass can gain access. But biometric security technology refers to the biological passcodes that cannot be forged - meaning accurate identification and authentication of the specific individual. Iris or facial recognition is more often becoming integrated as part of the security process, as scanning is a quick and easy process.

Accountability at its Best

When there's accurate information about entry and exit, it exceeds the responsibility of the firm. In the event of any unfortunate events, there is a better proof of confirmation backed by data. The data is also easy to configure, analyzed and reported as necessary.

Highly Efficient

Every company demands highly efficient security systems. Biometric verification systems not only enhance security, but make it is easier and more efficient to manage key functions such as attendance tracking for payroII. It is even helpful for employees as they don't need to carry cards everywhere.

Convenience is Key

One key advantage of a biometric verification system is convenience. There's just no need to reset the passwords. Once the biometric test is activated, all fingerprints, iris and facial recognition are done –

APPLICATIONS –

There are several domains where IOT is being successfully implemented. The potentialities of IOT can still be exploited to develop new applications for the benefit for society. It can boost the role of information and communications technology (ICT) so that the quality of our lives can be improved. In the application environment of IOT , smart objects can communicate with each other and represent a context perceived from the environment. The potentially of IOT can be exploited in many domains like healthcare, transportation systems, environmental monitoring, personal and social, smart city, industrial control, and many more. In this section, we discuss few promising application domains and pointed out their short comings.Smart environment (homes, buildings, office, and plant):Sensors and actuators deployed or attached with household-equipment like refrigerator, lighting, and air conditioners can monitor the environment inside a house, plant, or office. The lightning system of a house can change according to the time of the day, like in the evening most of the lights will be on, while they will be off late at night. Based on the reading of a temperature or a smoke detector sensor, a fire alarm can be set off automatically. Such type of application is very helpful for clderly people staying alone at home. Based on the movement of occupants in home, some appliances like doors in room can be opened, lights can be turned on at current room, and water taps/faucets will be open at kitchen. Air conditioners, refrigerators, and washing machines will now be IOT – enabled and controlled over the Internet to save energy. In the near future, a smart malfunctioning refrigerator will send a message to a service man automatically without user's intervention. Industrial automation is improved by deploying RFID tags with products. Production process is controlled to ensure quality of product by getting different parameter values from sensors. IBM has launched Smart Home solution, better known as"Stratccast," to provide service to users allowing scamless communication among various smart devices in the house, like medical devices, computers, mobiles, TV'S, lighting, security, and sound system. IBM is collabrating with Verizon as a communication service provider (CSP) and Philips as a device vendor to implement the architecture. Siemens, Cisco, Xerox, Microsoft, MIT, and many others are working in to this domain. They have set nearly 20 home labs using more than 30 home appliances. 5 network protocols, and 3 artificial intelligence (AI) techniques. The intel smart home platformsupports recognition of family members by voice or face and personalizes the home. Intel provides IOT solutions for smarter building to support personalization by controlling over the office/living environment, mobility by enabling managers to monitor property remotely, and sustainability and efficiency in terms of saving energy, water, and other building resources.

CONCLUSION –

Along with an exponential growth in connected devices, each thing in IoT communicates packets of data that require reliable connectivity, storage, and security. With IoT, an organization is challenged with managing, monitoring, and securing immense volumes of data and connections from dispersed devices. But this challenge doesn't have to be a roadblock in a cloud-based environment. In addition to scaling and growing a solution in one location, cloud computing enables IoT solutions to scale globally and across different physical locations while lowering communication latency and allowing for better responsiveness from devices in the field. AWS offers a suite of IoT services with complete security, including services to operate and secure endpoints, gateways, platforms, and applications as well as the traffic traversing across these layers. This integration simplifies secure use and management of devices and data that continually interact with each other, allowing organizations to benefit from the innovation and efficiencies IoT can offer while maintaining security as a priority. AWS offers customers a defense in depth approach with multiple security services and an easier, faster and more cost-effective path towards comprehensive, continuous and scalable IoT security, compliance and governance solutions.

REFERENCE-

[1] P. Aufner, “The IoT security gap: a look down into the valley between threat models and their implementation,” *International Journal of Information Security*, vol. 19, no. 1, pp. 3–14, 2019.View at: Publisher Site | Google Scholar

[2] Gartner, “Gartner Says the Internet of Things Will Transform the Data Center, (2014http://www.gartner.com/newsroom/id/2684616.

[3] IoT. Analytics, “Why the Internet of Things Is Called Internet of Things: Definition, History, Disambiguation,” (2014) https://iot-analytics.com/internetof-things-definition.

[4] D. Ferraris and C. Fernandez-Gago, “TrUStAPIS: a trust requirements elicitation method for IoT,” *International Journal of Information Security*, vol. 19, 2019.View at: Publisher Site | Google Scholar.

[5] M. Trik, S. Pour Mozafari, and A. M. Bidgoli, “An adaptive routing strategy to reduce energy consumption in network on chip,” *Journal of Advances in Computer Research*, vol. 12, no. 3, pp. 1–12, 2021.View at: Publisher Site |