ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

Identity theft and protection using IoT

Krittika Irkal[1], Sameeksha Irkal[2]

U.G. Student, KLE BCA, P.C.Jabin Science College, Vidyanagar, Hubli, India[1]

Assistant Professor, KLE BCA, P.C.Jabin Science College, Vidyanagar, Hubli, India[2]

ABSTRACT:The Internet of Things (IoT) is a new revolution of the Internet. Internet of Things (IoT) can be said as the expansion of internet services. It provides a platform for communication between objects where objects can organize and manage themselves. It makes objects themselves recognizable. The internet of things allows everyone to be connected anytime and anywhere. Objects can be communicated between each other by using radio frequency identification (RFID), wireless sensor network (WSN), Zigbee etc. Radio Frequency identification assigns a unique identification to the objects. RFID technology is used as more secure identification and for tracking/locating objects, things, vehicles. The purpose of this paper is to describe the basic concept of Internet of Things, its architecture, its working, and its applications. It emphasises on identity theft in IoT and steps for its protection.Furthermore this paper proposes a terminology for Identity protection in Internet of Things.

KEYWORDS: Internet of things(IoT), Architecture of IoT, Working of IoT, Identity Theft, Identity Protection

I. INTRODUCTION

Internet of things (IoT) is a term coined by Kevin Ashton in 1999.It is the inter-connection of devices and systems that are inter-related via real-world sensors and actuators to the internet and have ability to transfer data over a network. Internet of things allows the users to achieve deeper automation, analysis and integration within a system. The Internet of Things revolves around increased machine-to-machine communication. The IoT utilizes existing and emerging technology for sensing, networking and robotics. The IoT is built on cloud computing and networks of data-gathering sensors; it's virtual, and instantaneous connection; it's the future and it's going to make the future "smarter". The Internet of Things is exploding. It is considered as an integral part of the future internet. Open and integrated IoT environments will boost competitiveness and make people's daily life easier. The IoT will change the way we live, work and communicate.

II. ARCHITECTURE OF INTERNET OF THINGS

Internet of things consists main three parts; they are sensors, network connectivity and data storage applications. The same is shown in figure 1.1

Figure 1.1 IOT Structure

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

- A sensor communicates directly with the central server for data or communicates indirectly via gateway devices. Sensors measure and it evaluates data.
- Sensors are used in different IoT devices as per their use such as to sense temperature, heat, humidity etc.
- Gateways handle the various wireless standard devices. One gateway can handle multiple technologies and multiple sensors.
- Some of the examples for typical wireless technologies are Zigbee, Zwave, and RFID etc.
- Cloud-based applications are the key to using leveraged data. The Internet of Things doesn't function without cloud-based applications to interpret and transmit the data coming from all these sensors.
- The cloud is what enables the applications to go to work for you anytime, anywhere.
- Gateway interfaces with cloud using backbone wireless or wired technologies are Wi-Fi, Mobile, DSL or fibre. IoT supports IPv4 and IPv6 protocols.
- Due to the support of these protocols, any natural or man-made object can be assigned an IP address and provided with the ability to transfer data.
- IOT service providers offer various QoS with different pricing and design need for memory, CPU and battery consumption.

III. **WORKING OF IOT**

The IoT works in the following cycle:

- An event occurs.
- The sensors record the results of the event and the data is collected.
- The collected data is uploaded in the network and analysed.
- The appropriate action for the analysed data is specified.
- The user is then reported about the action.

Figure 2.1

Any IoT device will have a radio that can send and receive wireless communications.Iot wireless protocols are designed to achieve some basic services: operate on low power, use low bandwidth and work on a mesh network. The devices in the mesh network are directly connected with one another and they pass signals to each other. Mesh networks have the ability to connect thousands of sensors over a wide area such as a city.RFID and sensor technology enable the computers to observe , identify, understand the real-world entities, without the limitations of human-entered data. The RFID (Radio Frequency Identification) is an automated data collector that uses radio-frequency to transfer data between scanner and the movable item. It is very fast and doesn't need contact between the scanner and the movable item. It attempts to provide unique identification and backend integration for wide range of applications.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

IV. APPLICATIONS FOR IOT

IoT has applications across all industries and markets. It spans user groups to reduce energy use in their home to large organizations who want to streamline their operations. It proves to be useful and we have moved towards advanced automation. Some of fields where IOT is been applied are:

- Engineering and Industry
  Ex: In an industry when the requirements are over, the IoT device notifies the manager about it.
- Government and Safety
  Ex: CCTV cameras installed all over the city helps in identifying the criminals and the IoT device gets the whole information about the criminal.
- Farming
  Ex: An IoT device that will give detailed information about a plant when it's scanned.
- Home and Office
  Ex: when you enter your office, and it recognizes your face and it automatically adjust the lighting and temperature to her preference
- Health and Medicine
  Ex: when in a hospital a call comes for a wounded man, the IoT device recognizes the patient and pulls out the patients record
- Media and Marketing
  Ex: An IoT device that will analyse and respond to the needs and interest of each customer.
- Transportation
  Ex: Think you want to travel in a bus from your home town and your mobile phone alerts you the exactly time you should get out of your home.
- Education
  Ex: Smart classes that will help the students to learn and understand the subjects better.
- Defence

Ex: Warfare techniques will be highly mechanized including unmanned fighter jets and precision specific defence systems with the power to locate hostile actions using artificially intelligent algorithms.

V. IOT-IDENTITY THEFT

Cyberspace and real life are merging. With the Internet of Things (IoT), individuals and devices are increasingly connected to the Internet and physical objects are continuously integrated into information networks. Machines and robots are able to sense and analyse data, enabling control of the physical world. The IoT will bring about many major changes. But these big changes make way for new challenges, particularly with respect to security. The stored data contains highly detailed information about an individual, and that gives a clear picture of the individual-that includes details about our financial circumstances, our health, our religious preferences, and our family and friends; giving the criminals all the information they need to take advantage of someone.People may also not be aware of the level of privacy; for example, entertainment devices may gather audio and video data, and share intimate information. When the IoT systems fail or malfunction, they can cause substantial damage; private data may get leaked.

The smart phones that we carry everywhere with us are connected to a no. of devices. We take them to busy places, public places and use them naturally in front of strangers, for any purpose. It's not hard for someone to watch someone type in their device's pin code or password and it's all easy to memorize a security code and steal the device. If the thief is using your Smartphone and your device's data and act as you on your behalf and impersonates the identify which may lead to the loss of much bigger things-General data available on the internet, combined with social media information, plus data from smart watches, fitness trackers and if available smart meters, smart fridges and many more give a great all-round idea of your identity. Any time that you establish an account with a username, password, and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

other identifiable information, you're leaving that digital trail about you.Identity theft can therefore be counted as one of the biggest risks in the IoT.Security is essential for IoT, especially with respect to identity. Therefore, security should be designed into IoT systems from the beginning, not tacked on later.

VI. IOT-IDENTITY PROTECTION

Identity of an individual must be protected in IoT; it is must to confidentially hold the personal details of any consumer. Various steps need to be taken to secure identity theft in IoT.some of them are:

- Have strong and unique passwords.
- Do not over share personal information
- Safeguarding your information, whether it's related to your credit card or your thermostat, should be a constant priority.
- For connectivity via Wi-Fi, it is better to use a VPN like PRIVATE Wi-Fi for mobile devices connecting to IOT devices.
- It is always wise to share as little information as possible when using services, and never select "remember my details" such as for personal banking or corporate networks.
- Ensure that your data is encrypted and only authorized people have access to the data.
- Smartphone for proper authentication on IoT devices.
- Multi-factor authentication requires a combination of objects to gain access – usually two or more of something you know (e.g. a password), something you have (e.g. your phone) and something you are (e.g. a fingerprint). This improves your security.
- Use a different password for every device and always change the default password.
- Give IoT sensors and devices their own digital identities**.** You can do this by converting select bits of information about each one into a digital record.
- Cryptographic authentication is the best approach to IoT device identity. IoT devices are fully capable of establishing, maintaining, and employing long cryptographic keys. There is no reason to employ passwords for device identity.
- Installing smart chips in each sensor.
- Monitor the systems and devices periodically.
- Ensure IoT users awareness; make the users know what details to share, how to keep their password strong and secured.

VII. CONCLUSION

In the Internet of Things, strong identity for users and devices is required. Without strong identity, attackers can cross the cyber-physical boundary and easily hack devices and get access to personal details of an individual. Because of the many applications of IoT technology, the impact of cyber-attacks is not restricted to the smart home or connected car, but extends to industrial automation, health care, and many other domains. When designing IoT systems and other systems that link cyberspace and the physical world, strong identity implemented with secure hardware and software should be a requirement. Only in this manner can safety be protected.

REFERENCES

[1] For IOT Architecture:http://www.rfwireless-world.com/IoT/IoT-architecture.html
[2] For IoT Identity theft and protection:https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf
[3] https://www.globalsign.com/en/blog/identity-theft-in-the-iot