Security and Privacy of Internet of Things in Medical Domain Using Biometrics and Key Management

Dr. S.Prem Kumar[1], Shaik Shaika Iffath[2], Eskala Raaga Veena[3]
[1]Professor, Dept of CSE
[2, 3]Dept of CSE
[1, 2, 3] GPCET(affiliated to JNTUA , Anantapur), Kurnool, India

Abstract- *The Internet of things has many opportunities in software, wearable devices, home appliances etc., which can share and communicate information on the Internet. The main issue is that the data which is stored in the Internet is of large amount and contain lots of information which is private, such information is to be preserved and high security is to be provided. In this paper we focus on the information security challenges that are encountered by IOT by using biometrics, key management.*

Keywords- Internet of things, Security, Privacy, Authentication, Identification, Access Control

I. INTRODUCTION

The Internet of things encompasses large amount of concepts like wireless sensor networks, machine to machine communication and technologies such as radio frequency identification. In future if any object possessing computing and sensor capabilities can be able to communicate with other devices with the help of Internet, due to this there is a chance of employment of large amount of sensing and actuator devices.

As Internet communication evolves to sensing objects, many mechanisms will be required to secure communication with such devices in context to the future IoT applications like home automation, smart cities etc.,

The majority of IoT devices- from medical devices connected vehicles and even smart cities-come with their own applications. After a number of research contributions in the recent past, targeting low energy wireless sensing applications and communications isolated from outside world, a shift towards its integration with the Internet has taken place which is also reflected in the efforts conducted by standardization bodies such as The Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF), towards the design of communication and security technologies for the IOT. Such technologies currently form a much necessary wireless communications protocol stack for the IOT that, together with the various communication technologies, is analysed in detail in [1] and discussed later in the article.

II. THE EVOLUTION OF IoT

The idea of connecting things to the internet extends much further back than the use of the term "INTERNET OF THINGS". In the early 1980s, Carnegie Memlon University students have fitted internet connected photo sensors to a soft drink vending machine that counted how many drinks had been dispensed and thus how many were remaining [1]. The first use of the term Internet of Things came much later, and is widely attributed to Ashton[2], when he used it as the title of a presentation at Procter and Gamble in1999.

III. THE GROWTH OF IOT

There has been a rapid growth in the number of devices connected to the internet. A survey by Cisco and Ericcson has predicted that there will be 50 million devices connected to the internet by 2020. One reason that it is difficult to predict the growth is that there are not even consistent figures for the number of devices connected to the internet today. Gartner research has estimated that the total number of M2M connections will grow from 5 billion in 2014 to 27 billion in 2024[3].

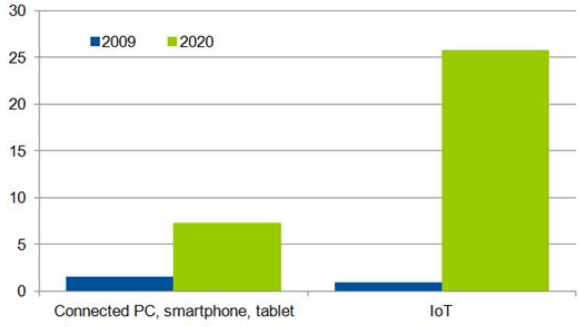

Fig.1. Growth of IoT

IV. APPLICATIONS OF IOT

The Iot is having a significant impact in number of domains and a number of researchers have analysed its

applications. The applications of sensors in the automotive sector have been one of the largest growth areas[4], there are a number of sensors with vehicles used for everything.

The use of sensors is an integral part of emerging medical and healthcare technologies [5]. The IoT has the potential to be integrated into numerous healthcare services and applications.

One of the biggest impacts globally of the IoT is expected to come through the advent of the Fourth Industrial Revolution, in which IoT technologies are to be incorporated into each phase of the manufacturing process[6]. With large numbers of shipments and increased inventory, IoT technologies can support logistics dynamically by enabling the service provider to increase operational efficiency whilst also increasing automation and decreasing manual processes[7].

In recent years there has been a dramatic increase in investment in smart grid research and development, pushing the UK into the lead in the European deployment of a wide range of viable smart grid solutions. Smart Grid is an intelligent power system which incorporates information and communication with existing transmission and distribution systems[8].

Smart technology is also being developed in the agricultural sector. Field information is traditionally obtained through manual reporting mechanisms, which can lead to inaccuracies in data. To maximise and streamline the production of agricultural commodities by systematically increasing efficiency and decreasing manual labour, IoT sensors and technologies can contribute to scientific cultivation with increased quality[9].

V. SECURITY CHALLENGES WITH THE IOT

As the IoT expands and becomes more interwoven into the fabric of our everyday lives, as well as becoming an increasingly important component of our critical national infrastructure, securing its systems becomes vital.

A. PHYSICAL LIMITATIONS OF DEVICES AND COMMUNICATIONS

In any application area, IoT devices are usually embedded with low power and low area processors, and it has been recognized that ‘the Internet Protocol could and should be applied even to the smallest devices’[10]. Constraints on IoT devices limit the ability to process information at speed – there is a limited CPU, memory, and energy budget. This means that challenging forms of security are required which satisfy the competing goals of strong performance and minimal resource consumption.

For security through digital signatures, a public key infrastructure is required, and this is a significant challenge to IoT systems. Public key infrastructure can protect against both loss of confidentiality and loss of integrity. However, even the encryption process with the public key requires computational and memory resources that are beyond many wireless sensor systems, especially when frequent data transmission is required.

Many components of the iot, particularly in the health and transport and logistics domains are also mobile. This presents a challenge in ensuring that security solutions adapt to the mobile environment, interacting with many different components and systems, each potentially offering different settings, protocols, and standards.

B. AUTHENTICATION AND IDENTTY MANAGEMENT

Identity management concerns the unique identification of objects, and authentication then validates the identity relationship between two parties.

Authentication within the IoT is difficult, since without appropriate authentication the integrity, confidentiality and availability of systems can be compromised. The authentication and Identification of users in the IOT remains a significant challenge. Currently username/password pairs are the most common form of authentication and identification of users in electronic systems, though other forms like digital certificates, shared keys or biometric credentials may be used[11].

It is just not the identification and authentication of users that requires consideration. It is also necessary to identify and validate service and devices in IoT systems. It can be challenging to perform a strong authentication of devices in the Iot because of the nature of the device or the context in which hit is being used[12]. Without adequate authentication processes, it is not be possible to assure the data originated from the intended device, or was received by the intended device. If the devices are appropriately authenticated, there is still a requirement to authenticate the service, since certain services will have access to certain data.

C. AUTHORISATION AND ACCESS CONTROL

Access control requires communication between entities (often restricted to software entities rather than human,

since users impact on the system through the software entities that they control) to request and grant access. There are various models for access control such as Discretionary Access Control (DAC – where an administrator determines who can access resources); role-based access control (RBAC – allowing access based on the role that the requester holds); and attribute-based access control (ABAC – where rights are granted through policies which evaluate the attributes of the user, resource requested and the environment from which the request is made)[13].

VII. SECURITY ISSUES

The connected and autonomous vehicles area is complex and involves many different sensors, actuators, infrastructure, communications protocols, and services. These services vary from small, simple services running on only a few components, through to global services involving significant parts of the critical national infrastructure. This work cannot encompass all of the types of system and potential and implemented attacks. However, it is possible to highlight some of the most significant attacks.

Recently, there have been an increasing number of attacks where the victims have been hospitalsed. There have been a myriad of potential and actual attacks on individual connected devices, including drug delivery systems, electronic health implants, insulin pumps, and pacemakers. Medical data can be used for identity theft or fraud, as well as to discover drug prescriptions, enabling hackers to order medication online. Hackers might also consider extortion and blackmail of people with certain illnesses that they would not want disclosed. Similar attacks on the confidentiality, integrity, and availability of IoT-enabled well-being, such as fitness trackers, also exist, though the impact from breaches on availability and potentially integrity is less severe[14]. This is not the case regarding confidentiality of information.

The IoT appears to offer significant efficiency and business opportunity in logistics. There are various application scenarios, which inevitably creates a large attack surface. One recognized attack is the manipulation of embedded data, either by malicious substitution of tags or by modification of tag information

There is a vast range of devices for the smart home promising intelligent resource efficiency through remote and instant access and control. Whilst such devices and services offer economic and functional benefits, they do increase security risks. The key risks that such devices represent are to confidentiality and privacy. Some issues, such as how energy consumption can provide inferences for profiling, have been discussed previously. As well as attacking the devices in smart homes and offices, hackers will target the building automation and control systems. Probably the most significant attack utilising access to internet-connected building control systems was the attack on Target. The attack originated by compromising the heating, ventilation, and air conditioning Company supplying Target.

VIII. PRIVACY CHALLENGES IN IOT

Privacy is seen as a major concern in the IoT [15]-[19]. The IoT has made an enormous quantity of data available, belonging not only to consumers such as is the case with the World Wide Web, but to citizens in general, groups, and organizations. This can be used to establish what we are interested in, where we go, and our intentions. Whilst this can provide great opportunities for improved services, it must be weighed against our desire for privacy. It is vital that consumers trust the services they engage with to respect their privacy.

Sensors, including those embedded in mobile devices; collect a variety of data about the lives of citizens. This data will be aggregated, analysed, processed, fused, and mined in order to extract useful information for enabling intelligent and ubiquitous services. Trust refers to the determining of when and to whom information should be released or disclosed.

IX. CONCLUSION

Libsecurity is a comprehensive package that offers application developers a complete, small and provably correct security toolkit for endpoints and gateway/hubs. This includes a lightweight and correct implementation of various security-related modules, including secure storage, user and password management, permissions and more. Authentication and identification in IoT systems is fundamental for security and privacy. Obviously, systems based upon biometric identification, possibly combined with a token, may prove advantageous compared to existing systems, but care must be taken to ensure that the system is secure yet frictionless. The IoT presents an opportunity to revolutionize the way we live and work. However, there remain a number of significant challenges to ensure that its potential can be realized without catastrophic consequences. There are numerous guidelines and best practices for security in the IoT available to individuals and organizations.

REFERENCES

[1] Vetter, R. J. 1995. "Internet Kiosk-Computer-Controlled Devices Reach the Internet." *Computer* 28 (12): 66–67.

[2] Ashton, Kevin. 2009. "That "Internet of Things" Thing." *RFiD Journal*, 97–114

[3] Machina Research. 2015. "Global M2M Market to Grow to 27 Billion Devices, Generating USD1.6 Trillion Revenue in 2024." Accessed July 4, 2017.

[4] Meola, Andrew. 2016. "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles – Business Insider." Accessed July 4, 2017.

[5] Dohr, Angelika,Robert Modre Opsrian, Mario Drobics,DieterHayn,and Günter Schreier. 2010. "The Internet of Things for Ambient Assisted Living." Seventh International Conference on Information Technology: New Generations (ITNG), Las Vegas, USA, April 12–14, 804–809, IEEE.

[6] Thoben, Klaus-Dieter, StefanWiesner, and Thorsten Wuest. 2017. "'Industrie 4.0' and Smart Manufacturing – A Review of Research Issues and Application Examples." *International Journal of Automation Technology* 11 (1): 4–16.

[7] Macaulay, James, Lauren Buckalew, and Gina Chung. 2015. "Internet of Things in Logistics." *DHL Trend Research* 1 (1): 1–27.

[8] DECC (Department of Energy & Climate Change). 2014. "Smart Grid Vision and Routemap Smart Grid Forum." *Smart Grid Forum*, February. doi:URN 14D/056.

[9] Chen, Xian-Yi, and Jin Zhi-Gang. 2012. "Research on Key Technology and Applications for Internet of Things." *Physics Procedia* 33: 561–566.

[10] Mulligan, Geoff. 2007. "The 6LoWPAN Architecture." EmNets '07 proceedings of the 4th workshop on Embedded Networked Sensors, Cork, Ireland, June 25–26, 78–82.

[11] Gessner, Dennis, AlexisOlivereau, Alexander SalinasSegura, and AlexandruSerbanati. 2012. "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things." IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, England, June 25–27, 998–1003.

[12] Sarma, Amardeo C., and JoãoGirão. 2009. "Identities in the Future Internet of Things." *Wireless Personal Communications* 49 (3): 353–363.

[13] Gusmeroli, Sergio, SalvatorePiccione, and DomenicoRotondi. 2013. "A Capability-Based Security Approach to Manage Access Control in the Internet of Things." *Mathematical and ComputerModelling* 58 (5–6): 1189–1205.

[14] Storm, Darlene. 2015. "MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks." *Computerworld*, June 8.

[15] Misra, Sridipta, MuthucumaruMaheswaran, and SalmanHashmi. 2016. *Security Challenges and Approaches in Internet of Things*. Springer Briefs in Electrical and Computer Engineering. Cham: Springer.

[16] Sicari, Sabrina, AlessandraRizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks* 76: 146–164.

[17] Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and KlausWehrle. 2014. "Privacy in the Internet of Things: Threats and Challenges." *Security and Communication Networks* 7 (12): 2728–2742.

[18] Roman, Rodrigo, Pablo Najera, and Javier Lopez. 2011. "'Securing the Internet of Things (IoT)'." *IEEE Computer* 44: 51–58. doi:10.1109/MC.2011.291.

[19] Gessner, Dennis, AlexisOlivereau, Alexander SalinasSegura, and AlexandruSerbanati. 2012. "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things." IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, England, June 25–27, 998–1003.