IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 75-79

A review paper on Security Integration & Privacy in the IOT

Chandan Kumar Sethi[1],
[1](*Mechanical Engineering, Gandhi Institute for Education and Technology / BPUT Rourkela, India)*

Abstract: *The internet of things (IoT) is a technology that has the capacity to revolutionize the way that we live, in sectors ranging from transport to health, from entertainment to our interactions with government. This fantastic opportunity also presents a number of significant challenges. The growth in the number of devices and the speed of that growth presents challenges to our security and freedoms as we battle to develop policies, standards, and governance that shape this development without stifling innovation. This paper discusses the evolution of the IOT, its various definitions, and some of its key application areas. Security and privacy considerations and challenges that lie ahead are discussed both generally and in the context of these applications. Mobile Cloud Computing is a new technology which refers to an infrastructure where both data storage and data processing operate outside of the mobile device.*

Keywords: *Internet of things, security, privacy, trust*

I. Introduction

The internet of things (IoT) is heralded as a development that can deliver dramatic changes in the way we live. It is recognized as an enabler that will increase efficiency in a number of areas, including transport and logistics, health, and manufacturing. The IoT will assist in the optimization of processes through advanced data analytics, and be the catalyst for new market segments by capitalizing on its cyber-physical characteristics, giving rise to cross-cutting applications and services. Internet of Things is a new technology which is growing rapidly in the field of telecommunications. More specifically, IoT related with wireless telecommunications. The main goal of the interaction and cooperation between things and objects which sent through the wireless networks is to fulfill the objective set to them as a combined entity. In addition, there is a rapid development of both technologies, Cloud Computing and Internet of Things, regard the field of wireless communications. In this paper, we present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, we combine the two aforementioned technologies (i.e Cloud Computing and IoT) in order to examine the common features, and in order to discover the benefits of their integration. Concluding, we present the contribution of Cloud Computing to the IoT technology. Thus, it shows how the Cloud Computing technology improves the function of the IoT. Finally, we survey the security challenges of the integration of IoT and Cloud Computing.

II.The evolution of the 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 students at Carnegie Melon University fitted internet-connected photosensors to a soft drinks vending machine, which allowed them to count the number of cans that were being dispensed. This enabled anyone with access to the internet to determine how many drinks had been dispensed, and thus how many were remaining Even before the first webpage was created, John Romkey and Simon Hackett introduced a toaster that was connected to the internet in 1990. Romkey's presentation at the 1990 Interop Conference featured an internet-connected Sunbeam Deluxe Automatic Radiant Control toaster, and arose as the result of a challenge at the previous year's conference from Dan Lynch, President of Interop, to Romkey. Lynch had promised Romkey centre stage at the event if he succeeded. The toaster was connected using TCP/IP and had a Simple Networking Management Protocol Management Information Base (SNMP MIB) controller; its one function was to turn the power on or off. The first use of the term 'Internet of Things' came much later, and is widely attributed to Ashton.

III.The growth of the IoT

There has been rapid growth in the number of devices connected to the internet. A number of analysts, notably Cisco and Ericcson (Dave Evans and Hans Vestburg, respectively), have predicted that there will be 50 billion devices connected to the internet by 2020. Of course, these estimates are difficult to assert with confidence, and both have now revised their estimates down. Evans, now at Stringify, predicts 30 million whist Ericcson estimates 28 billion by 2021. One reason that it is difficult to predict growth is that there are not even consistent figures for the number of devices connected to the internet today. Not only is there a significant difference in figures using the same definitions, but the issue concerning the varying interpretations of the IoT also has an impact. Some figures clearly state the difference between machine-to-machine (M2M) and IoT

devices, such as those of the GSMA, whose analysis of M2M 'focuses on cellular M2M connectivity and excludes computing devices in consumer electronics such as smartphones, e- readers, tablets, as well as other types of M2M connection technologies that support the wider universe of the Internet of Things (IoT)' . A 2015 report by Machine Research predicted that the total number of M2M connections will grow from 5 billion in 2014 to 27 billion in 2024 (Machina 2015Machina Research. 2015. Observed that, in 2016, Gartner estimated that there were 6.4 billion devices (excluding smartphones, tablets, and computers), the International Data Corporation estimated 9 billion (with the same exclusions) and HIS estimated 17.6 billion (including smartphones, tablets, and computers). A similar study by Juniper Research estimated that there were 16 billion devices. Whilst there are not consistent figures for the number of connected IoT devices, it can be seen that the number of devices is enormous, and growth has been, and is predicted to be, rapid.

Defining the IoT

When writing about his first use of the term IoT, Ashton remarked that the term 'is still often misunderstood'. Indeed, today there exist many definitions and interpretations of the IoT. Describes the IoT as 'a network of items – each embedded with sensors – which are connected to the Internet'. On the other hand another august, expert organisation, the Internet Engineering Task Force (IETF), states that 'in the vision of the IoT, "things" are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc.

IV. Applications of the IoT

The IoT is having a significant impact in a number of domains, and a number of researchers have provided insights and analyses into its applications. When presenting applications of the IoT, researchers have their own classification of domains and applications. Each taxonomy has its own merits, and depends not only upon the objective to be achieved but also the definition and context of the IoT under consideration. The reader is referred to the references presented in Table 2(further information on the applications of the IoT). The application of sensors in the automotive sector has been one of the largest growth areas.

Health, well-being, and recreation

The use of sensors is an integral part of emerging medical and healthcare technologies. The IoT has the potential to be integrated into numerous healthcare services and applications The healthcare services that will benefit most significantly include ambient assisted living (a significant area of application involving the use of smart homes to allow patient monitoring and care in independent environments); the internet of mobile health (integrating medical sensors into mobile technologies); semantic medical access (utilising semantics, IoT healthcare applications can use medical rule engines to analyse large quantities of sensor data); and adverse drug reaction (by labelling drugs and examining a medical database, any potential adverse reaction such as allergy, or reaction with other drugs, can be avoided). Healthcare applications that have already been developed, or are set to be developed include blood pressure and diabetes monitoring, body temperature and rehabilitation monitoring, oxygen saturation monitoring, and wheelchair management The Impact of the Internet of Things on Implanted Medical Devices Including Pacemakers, and ICDs.

Industry 4.0

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. This will involve a shift from automated to intelligent manufacturing processes (Thoben, Wiesner, and Wuest 2017 Thoben, Klaus-Dieter, StefanWiesner, and Thorsten Wuest. 2017. "'Industrie 4.0' and Smart Manufacturing. The IoT can be employed throughout the development lifecycle through the introduction of smart connected machines with proactive maintenance, enabling a smarter manufacturing process delivered through intelligent logistics, allowing rapid, flexible, and lean manufacturing. Optimised decision-making and innovative planning methods, combined with smart grid technology, will mean the energy efficiency of plants can be maximised.

V. Security challenges within 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. The securing of systems can be based upon a number of principles, from the CIA of information security (confidentiality, integrity, and availability), to the five pillars of information assurance (confidentiality, integrity, availability, authenticity, and non- repudiation) and the Parkerian Hexad (confidentiality, integrity, availability, authenticity, possession, and utilty). It is certainly worth considering all of these components of security, especially in complex cyber-physical systems such as the IoT. However, for this piece we use the three

broadest categories of the CIA, understanding that the compromises may be of physical as well as information assets. We discuss some of the most significant challenges, highlighting which principles are under threat of compromise. However, it must be recognised that this is not an exhaustive list of the security challenges.

Authentication and identity management

Identity management concerns the unique identification of objects, and authentication then validates the identity relationship between two parties recognises that further research is needed in the 'development, convergence and interoperability of technologies for identification and authentication that can operate at a global scale'.

Authentication within the IoT is critical, since without appropriate authentication the confidentiality, integrity, and availability of systems can be compromised. This is because if an adversary can authenticate as a legitimate user, they will have access to any data that the user has, and can see (compromising confidentiality), modify (compromising integrity), and delete or restrict availability (compromising availability) in the same way that the user can.

Authorisation and access control

It has been recognised that there is a need to 'exercise access control over [the Internet of Things] at the edge of the network in the device or, at least, a local access controller for the device'. There is an important role in establishing whether the user, once identified and validated, has permission to access the requested resources (Abomhara and Køien 2014Abomhara, Mohamed, and Geir M. Køien. 2014. "Security and Privacy in the Internet of Things. 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).

Implementation, updating, responsibility, and accountability

It is vital, though often overlooked in discussion, that the implementation and updating of security protection must be both manageable and low cost. IoT systems can be geographically remote and involve sensors and actuators in extreme and challenging environments. To protect the cyber security of the system it is vital that any vulnerabilities are addressed as soon as they are discovered. As such, there is a need for remote access to allow these system updates. The latest software patches could be installed dynamically, and the process managed through cloud-assisted frameworks; however, designing a secure mechanism for dynamic installation is a challenging task . It must also be recognised that updates can change the functionality of devices, and these changes may not always be aligned with user expectations

Security issues in connected and autonomous vehicles

The connected and autonomous vehicles (CAV) 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.

Modern vehicles have between 70 and 100 integrated electronic control units (ECUs) for applications such as braking, steering, transmission, suspension, and engine control. The sensors providing information into these ECUs include the Tyre Pressure Monitoring System Infotainment system, Camera, LIDAR, RADAR, and brake and engine sensors. Communication to ECUs is through a range of network types including CAN (Controller Area Networks), FlexRay, MOST (Media Oriented System Transport), and LIN (Local Interconnect Network). Different manufacturers employ different networks, but modern vehicles will feature a number of these network types. However, these protocols were designed prioritising efficiency and safety rather than security. Although the likelihood of a cyber-attack on a connected vehicle is currently thought to be low, the increasing importance of these vehicles, and the rise of technologies such as ransomware, make this a significant emerging risk to the integrity and availability of connected and autonomous vehicular systems. As well as financial motivations, we are likely to see attempts to compromise these systems by terrorists, nation states, and hacktivists.

Many applications in CAV involve a combination of personal and vehicular (that can be linked to individuals) data that is sent externally. This type of data can have its confidentiality and privacy breached in a number of ways, including through the use of 'sniffing stations'. It is also possible to undertake man in the

middle attacks on the wireless communications entering a vehicle, thereby compromise the integrity of that data. Such a man in the middle attack was the basis of the remote exploit of the Jeep by Miller and Valasek.
As connected vehicles interact with and become dependent upon infrastructures such as Cloud and Edge-cloud, the risk and impact of attacks on the availability of systems will increase.

VI. Privacy challenges in the IoT

Privacy is seen as a major concern in the IoT .'Securing the Internet of Things (IoT)', Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of . 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 organisations. 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. Trust is a fundamental element in the forming of any relationship, and is a vital factor in the adoption of new technology .IBM Watson Foundation 2015IBM Watson Foundations. 2015. "Maximize Insight, Ensure Trust and Improve IT Economics – United States", and this is particularly true in complex systems such as the IoT.

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

Giving users more control over the collection and use of their personal information has been seen as an essential aspect of ensuring trust in distributed systems. Previous projects, such as the Platform for Privacy Preferences Project (P3P) have been designed to give users control when using web browsers. The P3P protocol, an initiative of the World Wide Web Consortium (W3C) initiated in 2002, allows websites to declare the intended use of data collected through web browsers. It was built upon the idea of translating website privacy policies into standardised machine-readable information to aid transparency and enable user choice. Unfortunately, the project ended prematurely, and there have been very few implementations. A variety of privacy enhancing technologies have been developed for ensuring privacy, including Virtual Private Networks, Transport Layer Security, DNS Security Extension, Onion Routing, and Private Information Retrieval (Weber 2010Weber, R. H. 2010. "Internet of Things – New Security and Privacy Challenges."

VII. Conclusions and further work

In this article we have discussed the origins of the IoT and how this has posed a major challenge to standardisation and a single overall vision. This, in turn, has given rise to challenges for security and assurance in the IoT.

Arguably the most significant challenge, but also the most fundamental, is to encourage standardisation and coordination in the IoT. This is not only difficult in terms of process and technology, but also politics. There needs to be consideration of all stakeholders and their conflicting views on the IoT. The P3P project shows the difficulties involved in gaining consensus and trust between parties that have different visions and interests.

The P3P project was laudable but faced considerable difficulties. An analogous system for the IoT would certainly be beneficial, but it is challenging to ensure that the outcomes are relevant and acceptable to all. If there is to be a protocol, analogous to P3P, to *communicate* how data are captured, processed, stored, and transmitted, and offer users a way to have *choice and control* regarding their data, it is important that lessons are learned from the P3P project. It is important that, for any standard to be successful, the project should be mindful of the politics involved. Privacy advocates may see the development as industrial subterfuge, a criticism that was levelled at the P3P project; the protocol should not allow services to create an illusion of privacy whilst gathering personal data. It should be recognised that any standard is likely to be only part of a solution, and as such, implementing the standard alone may not provide adequate protection. Therefore it is recommended that the standard should be used together with other privacy enhancing tools. Any standard should be developed in line with legal and regulatory compliance. If there is no compliance requirement or financial implication to not implementing the protocol, the business case for the protocol will fail. To maximise the probability of industry adoption and user acceptance, any protocol for managing consent in the IoT should be:

- developed around firmly agreed principles, to ensure there is no mission creep and that the objectives are clear;
- simple, economically efficient, and implementable;
- mindful of any impact on current and future business models;
- co-developed with industry bodies (service and infrastructure providers) and user representative groups;

- developed in line with legal and regulatory compliance. If there is no compliance requirement or financial implication to not implementing the protocol, the business case for the protocol will fail.

VIII. References

[1]. ABI Research. 2017. "What Is the Internet of Things?" Accessed July 4, 2017.

[2]. Abomhara, Mohamed, and Geir M. Køien. 2014. "Security and Privacy in the Internet of Things: Current Status and Open Issues." International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, May 11–14, 1–8.

[3]. Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and MoussaAyyash. 2015. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." *IEEE Communications Surveys & Tutorials* 17 (4): 2347–2376.

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

[5]. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. 2010. "The Internet of Things: A Survey." *Computer Networks* 54 (15): 2787–2805. doi:10.1016/j.comnet.2010.05.010.

[6]. Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. 2014. "A Security Evaluation of AIS Automated Identification System." Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, December 8–12, 436–445.

[7]. Bandyopadhyay, Debasis, and Jaydip Sen. 2011. "Internet of Things: Applications and Challenges in Technology and Standardization." *Wireless Personal Communications* 58 (1): 49–69. doi:10.1007/s11277-011-0288-5.