Security, Privacy and Trust for Smart Mobile devicesin Internet of Things – A Literature Study

RafidhaRehiman K A, *Research Scholar, Karpagam University, Coimbatore- 641021* and

Dr. S.Veni,Head , Department of Computer Science, *Karpagam University, Coimbatore- 641021*

***Abstract*—Earlier Internet connects places, then people and now in this era it connects things and arise a new concept Internet of Things (IoT).IoT penetrates all aspects of human life and handles huge volume of data (big data), so security and privacy concepts including access control, authentication and confidentiality plays a major role in IoT to enforce trust in dynamic environment. The user acceptance of IoT is enormously high and is always collecting sensitive information so privacy preservation and security in Trust Management in IoT is a big challenge in its research area. Since the current researches lack a comprehensive study on the enhancement of security in IoT, in this paper we investigate the main research challenges in this field and identify the unsolved problems. It also proposes a unique trust management framework for mobile devices by considering security related issues.**

***Index Terms*—Access Control, Internet of Things, Privacy Preservation, Security, Trust Management.**

I. INTRODUCTION

IOT IS a new revolution on the Internet and enable self-awareness in things including people, objects, information and places to be connected at any time, at any place. IoT provides access to information and services through wired or wireless connections, all things connected has unique IP and can be tracked. Now IoTis a reality and provide a world with real, virtual and digital converging to create the smart intelligent environment. This is the main difference between the Internet and Internet of Things. The things in IoT refer tothe active participants that autonomously interact and communicate in network.[1]

IOT is an interconnected collection of communication devices, computational power and technology, all types of data about social life and environmental information. It is a technological improvement of smart devices which improve the personal and professional life. The three components of IOT are the producer, the consumer and the objects. The producer publishes the information and acts as the source of information, the consumer consumes the information published and the object is a platform on which sensor data is shared. Wireless or wired sensors collect the information and are sometimes stored on data centers under the control of management centers and the website provide an interface to the user to communicate with IOT.

Now the number of internet connected deviceshave surpassed the number of people in the planet and according to the industry analyst firm IDC it is expected to be in between 26 to 50 billion in the year 2020 and approximately six devices will be used by a single person in the world.From the technology perspective the increase in density ofIoT is by Moore’s law because the data in IoT isgenerated by machines.

The fundamental characteristics of IoT include Interconnectivity, Things related to services, Heterogeneity, dynamic changes in enormous scale. IoT include advanced technology like embedded sensors, near field communication, global positioning systems etc. An outlined view of the concept is depicted in the figure 1. In IoT, things of the real world integrate into virtual world and enable any time anywhere connectivity.

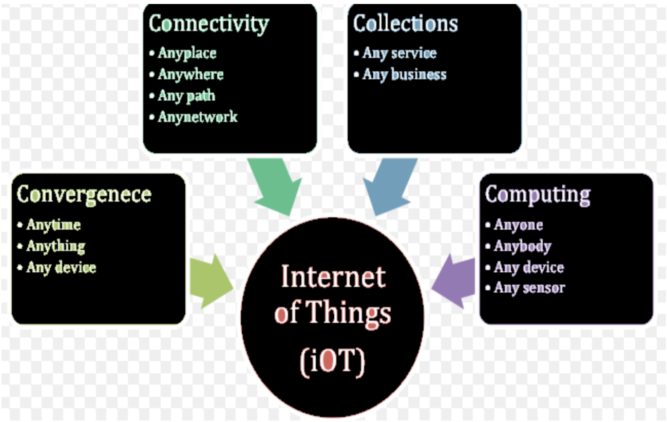

Figure 1: Outlined view of Internet of Things

IoT brings many opportunities to business, industry, and technology to increase theperformance and at the same time add complexities to information technology. Now people are surrounded by intelligent interfaces embedded in all kinds of objects. So it is capable to recognize other people and share data with other users. IoT is attractive and create new future to technology but the main issue faced by it is privacy and security. The devices in IoT are not immune against cyber threats. For example Symantec discovered a new worm named Linux.Darlloz targeting small IoT devices and computers in November 2013 and later it was updated to focusing money through coin mining. Smartphones and Tablets are also targets of attacks. The other vulnerabilities present in mobile IoT devices include Heart bleed, DoS, Weak password, Cross Site scripting etc. So we need to take measures to protect these devices.

II. RESEARCH CHALLENGES IN IOT

In IoT data is generated by the smart devices and in unconditional and unstructured format, it also collects the data directly from human life through sensor network, social networks, social data, call detail record, medical records, RFID etc. By sensors and actuators in smart devices a person is always tracked. This is a violation against the right to be let alone. Almost all information collected by the sensors is private and confidential. The collection and analysis of this big data introduce the all the problems with big data and serious issues in privacy. So the big data and security related challenges need to be addressed by the research community.[2]

In IoT we need to consider the different trust related aspects like communication, authentication, security, access control, integrity and reliability. There is no centralized agency to control the counterfeiting in the network, so we are required to take necessary care for server authentication.

The light weight, low cost and high performance solutions are required in smart devices because they are constrained with limited memory and battery power. So the common solutions for preserving privacy and security are not suitable for IoT environment.

A main concern IoT has to address is privacy. Since IoT uses smart devices which include sensors and actuators to collect the personal data (the movements, habits, preferences, payment information etc),we require entirely different methods to support the anonymity and restrictions for personal information. We need context based, access control,authorization and attack detection mechanisms. Moreover discrimination from sensor output is a big problem and the privacy law is still unprepared for IoT.

III. SECURITY CHALLENGES ON SMART DEVICES

In IoT environment, there is no prior knowledge about each other so identifying an intruder is a big challenge. An intruder can change the firmware or software on a device in IoT and it will affect the operational behavior of the device. Another possible attack is privacy threat and misuse. Also an untrustworthy manufacturer can install back doors to launch later attacks.

IoT include heterogeneous objects. Thereforefor real time analysis and applications it requires cloud services. Now it is widely used in distributed mobile environment and more vulnerable to security threats. In IoTthere is no central control to provide security, so for tracking the objects through insecure channel in a secure way is required. Also secret extraction and tampering of nodes are serious issues in IoT.[18]

IV. IOT SECURITY REQUIREMENTS

Current researches in IoT do not deeply investigate trust, security and privacy requirements. Recent research literatures only address the challenges faced by the research community to address the problems.

In this paper we study two major properties of trust, security and privacy to propose the objectives of trust management through security and privacy. For trust enhancement we analyze the security requirements- access control, authentication and confidentiality. Also we analyze different algorithms and methodology used by the literature for privacy preservation including personal data, location and information about the user.

For implementing security goals in IoT environment we need to consider its ad-hoc nature and limitations (size, low processing power and memory). There are restrictions in implementing chipset or Operating System level security in these devices because of hardware.

V. Literature review

A number of studies by the eminent researchers are done in literature to improve the security and privacy in IoT. We analyzed more relevant and recent available solutions for security, privacy and hence improve trust in IoT.

A. Privacy Preservation in IoT

Privacy means information about identifiable people in communication. Increasing amount of data, users and communication in IoT lead to the need of privacy preservation. Regarding privacy preservation a number of studies are aimed to improve the identity trust in IoT.

Jaydeepsen proposed privacy preservation technologies based on secure multi party computations by considering ubiquitous applications. By this a user in IoT environment is able to locate the things in vicinity without providing his location and preferences. With this algorithm we can provide solutions to privacy leakage but most of the multiparty computations are inefficient because of increased computational and communicational overhead. The method does not provide a solution that accommodate IoT devices.[3]

In “Internet of Things and Privacy Preserving Technologies” Vladimir Oleshchuk introduced the idea of using secure multi party computations for privacy preservation in IoT by considering different approaches. With examples they proved that Secure Multi party computations are well suitable for privacy preservation, but at the same time explained the drawbacks of the SMC protocol, its inefficiency and requirement of high computational and communicational resources.[4]

In 2012 Xin Huang et al suggested a user interactive privacy preserved access control mechanism and designed a content aware k- anonymity privacy policy and filter. By this a user can control his personal data from being collected. The major issue associated with this design is a user need to pay attention to ensure privacy and not practical because majority of users in IoT environment are from business field.[5]

Yi Lu et al in “Trust based Privacy preservation for peer to peer data sharing” tried to hide the relationship between the identity of data requester and the data. They developed a buddy system like a firewall to separate the identity and data. The buddy system knows the identity of the requester and reliability of the system depends on the buddy. If the details and data are encrypted we can offer more privacy based on this approach. But in case of IoT this was not a practical solution for privacy preservation because sometimes we require remembering some information. For example, the location ofcurrent user is required to calculate the distance between the user and another location.[6]

B. Security in IoT

Since IoT formed by the smart objects with autonomous facility in real time and spread the services all over the world, it will require suitable solutions for ensuring the security goals- Confidentiality, integrity and availability. To ensure the availability to right people we require strong access control and authentication systems with footprint supported by smart devices.

In 2013 A Alcaide et al presented a fully decentralized anonymous authentication protocol for confidentiality of both private information and data in IoT. In this scenario the data users must authenticate users and things from which information is collected. Also the repositories provide data only to the specific target. One of the issues associated in this context is its performance and temporal constraints. The system requires more computations than traditional data base management systems.[7]

In 2013 itself Xi Jun Lin and Lin Sun proved that the protocol is insecure. By this protocol an adversary can impersonate to be as the legitimate user and can cheat the users because their protocol does not rely on any central organization. They point out the drawbacks through cryptanalysis on the algorithm.[8]

In DTLS based security and two-way authentication for IoT, Thomas Kothmayr introduced a 2 way authentication security scheme for IoT based on Datagram Transport Layer Security infrastructure. The system existing on fully authenticated engineering technique so enables an easy security uptake. The method uses RSA public key cryptography and ensures X.509 certificate standard, but the system limited the inclusion of more constrained nodes.[9]

In 2014 Rahul Godha, SnehaPrateek and NikhitaKataria proposed an access control algorithm to identify and connect many physical sensors into a secure system. For implementing their approach they maintained a matrix on server side similar to the access control matrix with capability to provide access to the system. But the method is limited to home automation and the sensors are unaware of the access.[10]

The devices with sensors communicate without human interaction like RFIDs require strong authorization mechanisms. Jun Ya Lee enhanced existing RFIDs with encryption method based on XOR operation. The resulting system overcomes the flaws present in original RFID but the hardware implementation in this approach is an overhead.[11]

Rene Hummen et al proposed a delegation architecture which separates the DTLS connection setup after initial connection establishment for protecting the application data and hence reducing the computational and memory overhead. Also they argue that symmetric key cryptography reduce the memory and computation requirement when compared with public key cryptography. Hence they provide a solution for authentication, authorization and data protection.[12]

C. Trust Management

A system is said to be trustable, if the risk of using thesystem was analyzed and solved then Security and privacy problems associated with that system is settled .Trust is regard to the users' belief, confidence, and expectation on the reliability of the services provided by the system. Trust is a term highly related to security and privacy

Zheng Yan et al in his survey on trust management for IoT presented the properties of trust and its objectives, and then provided clear distinction between trust, security and privacy. They identified the problems faced by the research community including the lack of common frame work; secondly there is no light weight frame work to support small devices offering confidentiality. They proposed future research trends for holistic trust management with a diagrammatic model. Also the survey presented different methods for privacy preservation. Finally in the discussions they give the open issues faced and need to be addressed in the IoT environment.[13]

Most recently in March 2015,S Sicari et al presented a survey paper "Security Privacy and Trust in Internet of Things" which discussed the main research challenges and existing solutions in the area of IoT. They focused the security challenges faced by IoT including access control, authentication, confidentiality, privacy, policy enhancement etc. They summarized the survey by giving the research directions in the field. They explained the need of suitable solutions guaranteeing access control, confidentiality and privacy which is independent of exploited platform [14].Finally they pointed out the security of widespread smart mobile devices.

VI. Proposal

Based on the survey conducted we are proposing a light weight power efficient trust management system for smart mobile devices in IoT.[16] Smart Mobile devices that contain sensors , Compass, Accelerometer, Light monitor, Proximity sensor, GPS and Gyroscope and sensor based IoT devices are prone to security flaws. These products are manufactured by consumer goods makers and lack the data security in many cases. So necessary care need to be taken to build such a frame work.

Location is an important characteristic with the introduction of Global Positioning System, Near Field Communicators and Radio Frequency Identifiers. Sometimes the users need to hide their location from services based on the service they avail. Hiding the location every time is not a practical solution. So we propose a context based filter to preserve the privacy based on the situation. When in movement from one location to another, cryptography based protocols are required for preserving the location.

For protecting the identity and to ensure strong authentication and access control within the available footprint,we plan to design a novel algorithm based on Zero Knowledge Protocol. This will help to advance the privacy preservation and hence trust in IoT.

Afterprivacy preservation, access control and authorization, for both user and system next challenge is to protect the data handled. Refusing to share the data with anybody in IoT is not possible and against principles ofIoT. Only solution is to develop confidentiality enhancement to avoid or reduce the abuse of data. We plan to design a small server application in between the server and requester. The application will act like a personal firewall on the server side. To ensure the main goal of security confidentiality will plan to apply the private key cryptography.

Implementing security also introduces challenges in the area of IoT. Traditional cryptographic algorithms offer security but they are processed very slowly and require more power and memory, so we need to develop an algorithm suitable for IoT environment. Asymmetric key algorithms are more secure than private key algorithms but, additional cost and power will be required.So for IoT environment we choose symmetric key system.

For secure key exchange we plan to design a key distribution center for the servers. Also to preserve the integrity we want to make sure about the reliability of information received. Hashes can be used to measure the reliability and hence the trust.[17]

VII. CONCLUSIONS

In the survey we analyzed a series of methods used by previous researchers for security and privacy in IoT environment. These methods provided solutions with increased communication and computation overhead which are not suitable for smart environment. So we propose a new light weight method for trust management specific for smart mobile devices. The security goals- confidentiality, privacy and access control, proposed improves the trustworthiness of mobile devices in IoT[15]

REFERENCES

[1] OvidiuVermesan, Peter Friess, "Internet of Things – From research and Innovations to Market Deployment", River Publishers, 2015

[2] Scott R Peppet, "Regulating the Internet of Things: First step towards managing descrimination, Privacy , Security and Consent, Texas law reviews, 2014

[3] Jaydip Sen, "Privacy Preservation Technologies in Internet of Things ",

[4] Vladimir Oleshchunk, "Internet of Things and Privacy Preserving Technologies", Wireless VITAE'09, IEEE, 2009, p 336-340

[5] Xin Huang, et.al, "User interactive Internet of Things Privacy Preserved access control", the seventh International conference for Internet Technology and secured transaction ICITST, 2012.

[6] Yi Lu, Weichao Wang, Dongyan Xu, Bharat Bhargava, " Trust based Privacy Preservation for peer to peer data sharing",

[7] A Alcaide, E Palormar, J Montero – Castillo, A Ribagorda, "anonymous authentication for privacy preserving iot target driven applications", Computer security 37(2013), 111-123

[8] Xi- Jun Lin and Lin Sun, "Insecurity of an autonomous authentication for privacy preserving IoT target driven applications", November 28 2013.

[9] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig, Georg Carle, "DTLS based security and two way authentication for the internet of things", Elsevier Journal of AdHoc Networks, may 2013.

[10] Rahul Gogha, SnehPrateek, NikhitaKataria, "Home Automation: Access Control for IoT devices", International journal of Scientific and Research Publications, volume 4, issue 10, October 2014.

[11] Jun Ya Lee, Wei- Cheng Lin, Yu- Hung Huang, "A Lightweight Authentication Protocol for Internet of Things", IEEE 2014.

[12] Rene Hummen, Hossein Shafagh, Shahid Raza, Thiemo Voigt, Klaus Wehrle, "Delegation based Authentication and Authorization for the IP based Internet of Things", IEEE 2014

[13] Zheng Yan, Peng Zhang, Athanasios V Vasilakos, "A survey on Trust Management for Internet of Things", Journal of Network and Computer Applications Elsevier 42, 2014, p 120- 134

[14] S.Sicari, A Rizzardi, L.A Grieco, A Coen-Porisini, "Security, Privacy and Trust in Internet of Things : The road ahead" , Science Direct Computer Networks 76, 2015, p 146- 164

[15] Developing solutions for the Internet of Things, Intel products, solutions and services are enabling secure and seamless solutions for the Internet of Things.

[16] Scott R Peppet, "Regulating the Internet of Things: First step towards managing descrimination, Privacy , Security and Consent, Texas law reviews, 2014

[17] JaapHenkHoepman, "In Things we trust ? Towards trustability in the Internet of Things",2011.

[18] TapalinaBhattasali, RituparnaChaki, NabenduChaki, "Study of Security Issues in Pervasive Environment of Next Generation internet of Things" Computer science networking and Internet architecture, Cornell university, June 2014.