A SURVEY ON IoT: IDENTITY MANAGEMENT IN INTERNET OF THINGS

Subiya Siraj[1], Ms. Janhavi V[2]
[1]PG Scholar, [2]Associate Professor,
Department of CSE, VidyaVardhaka, College of Engineering, Mysuru, India

ABSTRACT: Internet of Things (IoT) devices are rapidly becoming ubiquitous while IoT services are becoming pervasive. The success of IoT has been noticed and the number of threats and attacks against IoT devices and services are on the increase as well. security has automatically become one main concern in the IoT deployment. Lack of security measures will result in decreased adoption among users which makes it one of the driving factors in the failure of the IoT. A lot of important questions regarding security has been solved but some remain opened. One of the importantl unresolved issue is the identity management of IoT devices. This paper presents a survey on common identity management frameworks, as well as technologies.

Keywords: Internet of Things(IoT); Public Key Infrastructures (PKIs); Pretty Good Privacy (PGP); Mobile Ad-hoc Network (MANET) ; security.

I. INTRODUCTION

The Internet has undergone severe changes since its first launch in the late 1960's as an outcome of the ARPANET with number of users about 20% of the world population. "7 trillion wireless devices serving 7 billion people in 2017". This vision reflects the increasing trend of introducing micro devices and tools in future i.e. IoT [1]. The Internet of Things (IoT) is the internetworking of physical devices, vehicles (also referred to as connected devices"), buildings and other items embedded with electronics, software, sensors, actuators and network connectivity that enables these objects to collect and exchange data. having a number of nodes.IoT has gradually permeated all aspects of moderrn human life, such as education, healthcare, and business, involving the storage of sensitive information about individuals and companies, financial data transactions, product development and marketing. The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide. Security is a process to protect an object against physical and software damage, unauthorized access, theft or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed [2, 11], without strong security infrastructure, attacks and impairments in the IoT, will outweigh any of its benefits. Talking about security infrastructure in IoT identity management is one of the strong security foundations. It's important to pay close consideration to the most appropriate security measures and best practices in terms of identity management systems.

Identity management has two principle components: management "of" the identity and management "by" the identity. Management of the identity is the process of delivering and using digital identities and credentials (such as usernames and passwords) for authentication. Management by the identity combines the proven identity of the user with their authentication, in order to grant access to resources. This paper is structured as follows: Section 2 focuses on identity management frameworks. Section 3 talks about technologies. Section 4 concludes the paper.

II. IDENTITY MANAGEMENT FRAMEWORKS

A lot of work has been done to offer better and more secure identity management frameworks. Several Factors are involved in the management process. The issues of trust and security are very important for many communications Environments and thus it is important to find efficient framework that can address them. The authors in [1] focuses on Identity Certificate Frameworks for identity management that are based on identity certificates, which are certificates that bind a public key to an identity. Identity certificate frameworks include Public Key Infrastructures (PKIs),. and Pretty Good Privacy (PGP). public key infrastructure, is a frame of services for services that provide for the generation, distribution, regulation and accounting of public key certificates. This public key system ensures secure user authentication, network traffic, encryption. Pretty Good Privacy (PGP) is a encryption program ,it's establishing itself as a provider of globally trusted identities for not only its own applications, but other high value applications and transactions. In the paper Identity and Mobility in a Digital World Ali M. Al-Khouri et al in 2012 [3] talks about identity management in digital world through smart cards. UAE issues the smart identity card to all of it's citizens and residents. The digital identity provided by the UAE is composed of a set of credentials delivered in the form of a smart card, which includes a unique national identification number, biometric data (fingerprints), and a pair of PKI digital certificates, one for authentication and another for signature Digital credentials in the Smart identity cards are provided to facilitate government and public sector service delivery transactions, from across manned counters to transactions on the web. The digital ID profile consists of: 1) A unique national identity number (IDN); 2) Biometrics (fingerprints); 3) A pair of digital certificates issued from the population certification authority (CA) of the public key infrastructure set up for this purpose. In [4] the authors aims to come out with a new Mobile Ad-hoc Network (MANET) framework that will support the IDM of the forthcoming IoT

and proposes an IDM framework. A mobile ad hoc network (MANET) also known as wireless ad hoc network is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. The identity management framework consists of 3 modules The identity module: The identity module consists of Device ID, IP, and Use ID. The User ID is further branched to consist of Device ID and user type. It is of predominant importance to point out that in the IoT, there is a possibility of sharing a device with other IoT applications, it is also important to allow the usage of existing devices to be incorporated within the IoT domain. Therefore, a MANET provides a suitable platform and provides the means for flawless interaction of such Things. However, due to the nature of the sensitive information used with e-Health applications in the IoT, it is vital to create a separation of individual data within the shared device. This functionality is provided by 'sandbox' modules. These create a virtual 'wall' between the individual users of a shared device and provide a mechanism that segments the device and users' information cannot be shared or accessed by other users. This also provides an extra mechanism to help protect against ID theft and information misuse. The context module: will play a crucial role in the IoT. It helps to provide a personalized service to Things that will facilitate the functionality of the framework. This is done by providing a means of tracking the identity of Things and users in a more dynamic way and will help in restricting the usability of Things based on the context in which it is intended to be used The privacy management module: provides an extra means of creating dynamic privacy policies that will enhance IDM security. The functionality of the contextual modules, the privacy module and the sandbox of the identity module is used to provide a personalized user interface to help in accessing and managing Ids in the IDM of the IoT. Personalized user interface and information access rights will be generated in the framework for individual users who are identified within the framework. The author Parikshit Narendra Mahalle in 2013[5] proposed a secure cross layer collaborative Identity Management (IdM) framework to cater to the requirements coming from IoT. The framework ties the IdM of the service layer together with the security, and access control needed for interactions between the things. When talking about functionality of this framework in the middle of both IoT devices and services , IdM middleware layer securely manages the relationships between devices/things and services. This framework is an integration of the solutions for set of operations which are required for achieving IdM of the devices. Identities and identifier formats for IdM, the objects in IoT are associated with resource constrained embedded devices. Forming an ad-hoc network, interactions between these nomadic devices to provide seamless service extend the need of new identities to the devices for IdM. This contribution presents clustering of devices, and hierarchical addressing with a new identifier format. This contribution has proposed new concepts of identity, identification, and identifier format. It also proposes context-aware clustering with hierarchical addressing for nomadic devices in IoT, and clustering of ubiquitous devices to achieve lifetime, and scalability results into better performance in terms of end-to-end delay, throughput, and energy expenditure of IoT network. In the framework IdM layer includes identity binding and mapping with the proposed identifier format. In [6] the authors proposes a framework that creates trusted environment of devices around centralized identity store. It allows not only authentication, but also complete device identity management. The framework also allows response fast enough to prevent any further damages in case of an attack targeting devices. Framework contains not only unique identifiers for devices but also supports the Role-Based Access Control by storing the roles internally. All machines and applications in the network can use those roles for their authorization rules. Such trusted central identity provider can provide environment, in which both participants can verify identity of the second partner and also they can determine if the partner is allowed to perform the given action.

Figure 1 demonstrates the work-flow of devices authentication and authorization. It can be described in the following steps:

Administrator creates an account for a device and set up its roles.

The device is configured with credentials provided by the administrator and requests a token from the store.

For any confidential communication the device uses the token to authenticate itself.

Application/device receiving the communication verifies the identity and roles by given token at the central store.

Administrator can disable or remove a device from the dentity store and therefore effectively disable it for any cooperation. Using the central identity element in IoT promotes a trusted environment RFID will not be the only technology used in the IoT to identify objects and link them to the Internet, but , it's the technology that's emanating as the most likely standard.

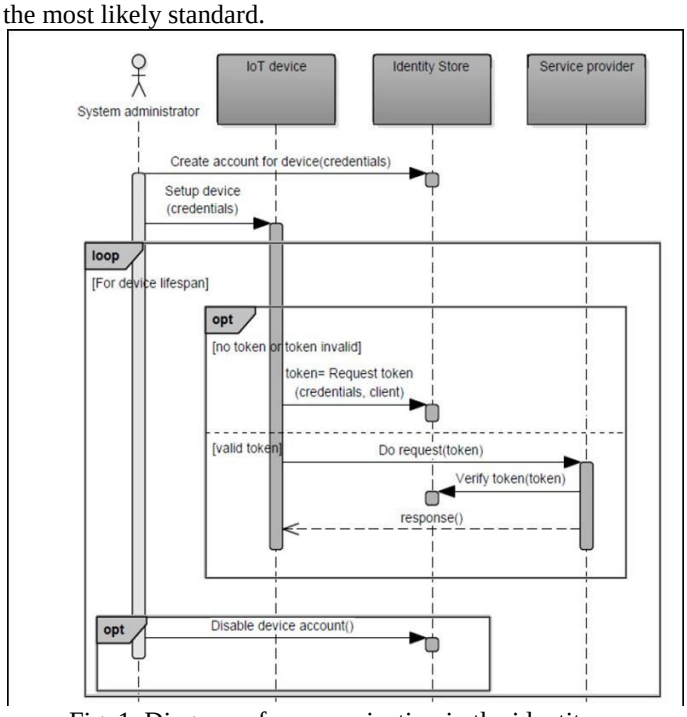

Fig. 1. Diagram of communication in the identity management framework

III. TYPES OF TECHNOLOGIES

The Internet of Things (IoT) enabled users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like NFC, RFID and 2D barcode which allowed physical objects to be identified and referred over the internet [7]. IoT, which is integrated with Sensor Technology and Radio Frequency Technology, is the ubiquitous network based on the omnipresent hardware resources of Internet, is the Internet contents objects together.

1. Radio Frequency Identification (RFID)

The Internet of Things (IoT) require a few necessary technologies to enable communication between IoT devices. These IoT objects need to be augmented using an Auto-ID technology, typically what is called an RFID tag, in order to uniquely identify the object. Also, the IoT device can wirelessly communicate certain types of information using an RFID tag.

2. Internet Protocol (IP).

The responsibility of delivering packets from the source host to the destination host is single-handedly based on the IP addresses in the packet headers in Internet Protocol(IP). For this reason, packet structures that encapsulates the data to be delivered is defined by IP. It also describes addressing methods that are used to label the datagram with source and destination information. The two versions of Internet Protocol (IP) are in use: IPv4 and IPv6. Each version of IP defines an IP address differently. Traditional IP address are used in IoT things when it comes to devices being servers switches firewalls but not necessarily in devices like refrigerators ,light bulbs, thermostats etc.

3. Electronic Product Code (EPC) cloud.

Electronic Product Code (EPC) is a 64 bit or 98 bit code which is electronically recorded on an RFID tag and expected to design an improvement in the EPC barcode system. EPC code can store information about the type of EPC, unique serial number of product, its specifications, manufacturer information etc. EPC cloud synoptic standardized IoT infrastructures. EPC address every steps from encoding unique number on RFID tag.

4. Barcode and QR codes.

Barcode is just a different way of encoding numbers and letters by using combination of bars and spaces of varying width. Behind Bars [8] serves its original intent to be descriptive but is not critical. QR code is the trademark for a type of matrix barcode(or two-dimensional barcode) designed for the automotive industry in japan. combining the use of RFID tags with both barcode and QR codes allows the consumer to connect to the IoT with the simple scan of a smartphone or tablet. Having all object marked with a QR code pr barcode means improving the retail environment for consumers because they will be more educated about the item before purchasing and they will be able to check for an item's availability.

5. Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. The integration of Wi-Fi into notebooks, handhelds and Consumer Electronics (CE) devices has accelerated the adoption of Wi-Fi to the point where it is nearly a default in these devices [9]. a new IEEE Wi-Fi standard 802.11ah using the 900MHz band has been in works and will solve the need of connectivity for a large number of things over long distances. A typical 802.11ah access point could associate more than 8,000 devices within a range of 1 km, making it ideal for areas with a high concentration of things. The Wi-Fi Alliance is committed to getting this standard ratified soon. With this, Wi-Fi has the potential to become a ubiquitous standard for IoT.

6. Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances, using short wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz from fixed and mobile devices. The new Bluetooth Low-Energy (BLE) or Bluetooth Smart, as it is now branded is a significant protocol for IoT applications. Importantly, while it offers similar range to Bluetooth it has been designed to offer significantly reduced power consumption. Bluetooth won't support every IoT need, but the sheer number of Bluetooth-enabled devices on the market and the ease of programming Bluetooth compatible applications makes it an important technology to familiarize yourself with as your business implements IoT solutions.

7. ZigBee

ZigBee technology is created by the ZigBee Alliance which is founded in the year 2001. It is a low power wireless network protocol based on the IEEE 802.15.4 standard [10]. ZigBee has some significant advantages in complex systems offering low-power operation, high security, robustness and high scalability with high node counts and is well positioned to take advantage of wireless control and sensor networks in IoT applications.

IV. CONCLUSION

This paper talks about common identity management frameworks and technologies, specifies framework for particular technology. Here the key observation is that, there is no standard framework . IoT framework standard is required which's accepted universally at architectural level. Technologies vary with changing customer requirements and so will frameworks. We need to build standard framework and protocols for identity management. Let's hope better IoT future.

REFERENCES

[1] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), 2010.
[2] J. M. Kizza, Guide to Computer Network Security. Springer, 2013.
[3] Ali M. Al-Khouri, Identity and Mobility in a Digital

World, 2012.

[4] Caroline Chibelushi, Alan Eardley and Abdullahi Arabo, Identity Management in the Internet of Things: the Role of MANETs for Healthcare Applications, 2013.

[5] Parikshit Narendra Mahalle, Identity management framework for internet of things, 2013.

[6] Michal Trnka and Tomas Cerny, Identity management of devices in Internet of Things environment, 2016.

[7] Razzak F, Spamming the Internet of Things: A Possibility and its probable Solution, 2012.

[8] Grieco A., Occhipinti, E. and Colombini, D, Work Postures and Musculo-Skeletal Disorder in VDT Operators, 1989.

[9] Pahlavan, K., Krishnamurthy, P., Hatami, A., Ylianttila, M., Makela, J.P., Pichna, R. and Vallstron, J, Handoff in Hybrid Mobile Data Networks. Mobile and Wireless Communication Summit, 7,2007.

[10] Chen, X.-Y. and Jin, Z.-G, Research on Key Technology and Applications for the Internet of Things, 2012.

[11] G. M. Koien and V. A. Oleshchuk, Aspects of Personal Privacy in Communications Problems, 2013.

