An Identity Management Framework for Internet of Things

Prachi V. Kale[1], Dr. G. D. Dalvi[2]

[1]*Assistant Professor, Department of CSE, P.R.Pote (Patil) college of Engineering and Management, Amravati, (MS) India*

[2]*Assistant Professor, Department of EXTC, P.R.Pote (Patil) college of Engineering and Management, Amravati, (MS) India*

***ABSTRACT*:** With the increasing population in most of the industrialized countries imposes a necessity for developing advanced and practical services and at the same time the availability of internet has been increased tremendously i.e. the reason the Internet of Things (IoT) has come in existence. It is more like a buzzword. Gradually from Internet of Things (IoT) it is becoming Internet of Everything (IoE).When the things are growing rapidly surely the issue of Security will arise. As the success has been noticed , the number of threats and attacks against IoT and its services are on the increase as well. In this case security has automatically become one of the main concern in the IoT deployment. Because of lack of security measures it result in decreased adoption among users. Many questions regarding security has been solved but some are yet to be solved. One of the important 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); Internet of Everything (IoE) ;Mobile Ad-hoc Network (MANET) ; security.*

I. INTRODUCTION

The Internet has changed very fast since its first launch in the late 1960"s as an outcome of the Advanced Research Projects Agency Network (ARPANET), which was the world's first operational packet switching network and the core network of a set that came to compose the global. Internet users are nearly about 20% of the world population but now the rise increases in a shocking way from "7 trillion wireless devices serving 7 billion people in 2017". As a result of this vision reflects the increasing trend of introducing micro devices and tools in future i.e. IoT [1].

A. IoT World

Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts. According to Wikipedia, IoT refers to the interconnection of uniquely identifiable embedded computing-like devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid.Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, bio-chip transponders on farm animals, automobiles with built- in sensors, or field operation devices that assist fire- fighters in search and rescue. Current market examples include smart thermostat systems and washer/dryers that utilize WiFi for remote monitoring.

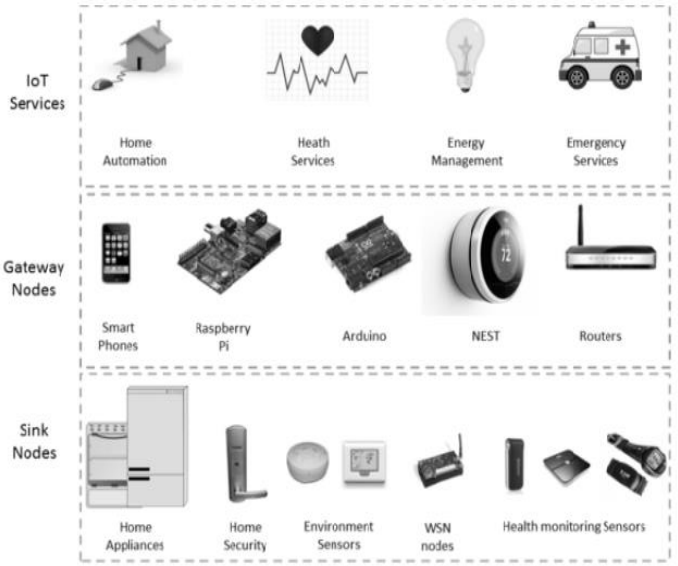

Fig. 1 IoT world

To form a IoT world we need sink nodes , gateway nodes and IoT services. The Internet of Things (IoT) is the communication network between physical devices, vehicles, buildings and other items embedded with electronics, software, sensors and network connectivity that enables these objects to collect and exchange data having a number of nodes. Anything which can be connected to internet should have the three capabilities i.e sensing, computing and communication. For Internet of Things (IoT) all these three things are necessary, if any one of these is missing then it won't be accepted for IoT. Now IoT has gradually entering into all aspects of modern human life, such as healthcare, education and business, which stores the sensitive

information about individuals and companies, financial data transactions, product development and marketing. Now a days security becomes a major concern if the sensitive data is in role , which create enormous demand for vigorous security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide. Security protect an object against physical and software damage, unauthorized access, theft or loss of data , by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed [2] without strong security infrastructure, attacks in the IoT. When we talk about security infrastructure in IoT identity management is one of the strong security foundations. It is very important to pay close attention to the most accurate security measures and best practices in terms of identity management system. Identity management has two main components to be considered i.e 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 organized as follows: Section 2 describes identity management frameworks. Section 3 discusses about technologies. Section 4 concludes the paper.

II. IDENTITY MANAGEMENT FRAMEWORK

For providing the security to identity management a lot of work has been done to offer better and more secure frameworks. Few factors are involved in the management process. In this fastest growing world the trust and security are very important factors for many communications environments thus it is very important to find efficient framework which can address them. Sachin Babar et.al. in [1] focuses on Identity Certificate Frameworks for identity management that are based on identity certificates. These are the certificates that bind a public key to an identity. This 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. World Ali M. Al-Khouri et al in 2012 in the paper Identity and Mobility in a Digital World [3] describes 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 oc Network (MANET) framework. It 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.

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.

III. TYPES OF TECHNOLOGIES

There are various technologies that can be used for Identity Information Framework such as ZigBee, Wi-Fi, and RFID are developments in exchange of data transformations within the IoT. ZigBee is a short-run remote exchange of data convention, which depends on IEEE 802.15.4 standard PHY layer and MAC sublayer along with the APS layer, ZOD, ZDP, AF, NWK, and ZigBee security layer [15]. The ZigBee system is not highly practical but rather it gives adequate execution to send messages in conjunction with sensors and it has a leeway of associating different smart devices. In any case, it is difficult to apply this security framework in light of the fact that the amount of transmittable data is restricted [13]. There are two security advances for ZigBee system (i.e., Standard Security Mode (SSM) and High-Security Mode (HSM)). SSM gives a low-security level and HSM bolsters a high security level. Wi-Fi is a remote LAN innovation in view of IEEE 802.11 standard. Wi-Fi is especially helpless against threats for security since it imparts remotely [14].

A. Radio Frequency Identification (RFID)

If we have to connect any physical thing to the world through The Internet of Things (IoT) we need a tagging. That tagging will actually connect users to bring physical objects into the sphere of cyber world. This was made possible by different tagging technologies like RFID , NFS and 2D barcode which allowed physical objects to be identified and referred over the internet [7]. IoT is the integration of Sensor Technology and Radio Frequency Technology.

Radio frequency identification (RFID) is a "wireless automatic identification and data capture (AIDC)" technology that allows end-to-end supply chain item level tracking and tracing[12] The technology is considered by scholars and practitioners as at the core of the so-called "Internet of Things", which refers to the "possibility of discovering information about a tagged object by browsing an Internet address or database entry that corresponds to a particular RFID". Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects .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.

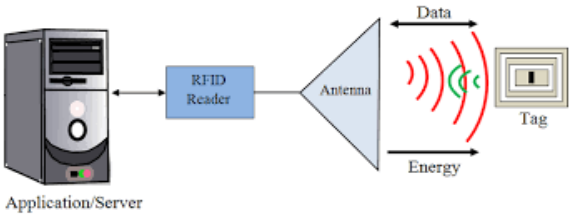

Fig. 2 RFID system

B. Internet Protocol (IP)

To deliver a packet from the source host to the destination host is solely handed based on the IP addresses which is present in the packet headers in Internet Protocol(IP). The basic packet structures that contains 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. IPv4 and IPv6 are the two versions of Internet Protocol (IP) in use. Each of this 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.

C. Electronic Product Code (EPC) cloud.

It gives a unique identity to individual physical objects such as items ,cases, pallets ,locations , loads , assests 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.

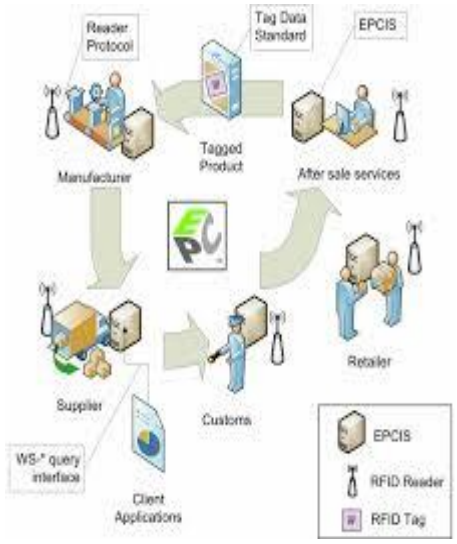

Fig 3. EPC cloud

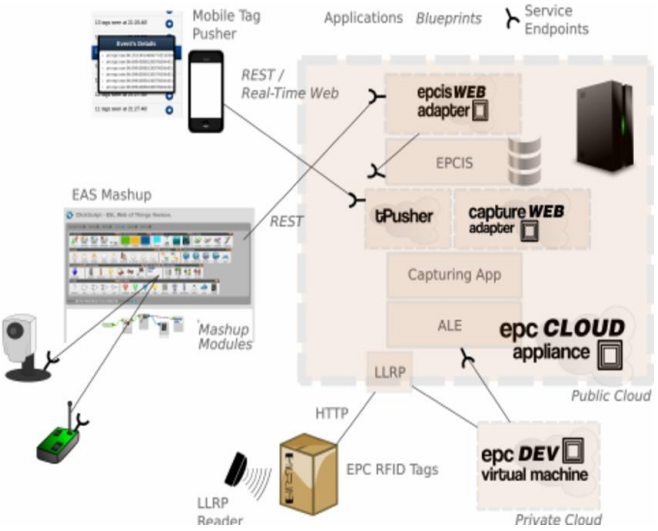

Fig. 4 Architecture of EPC cloud components

D. 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 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.

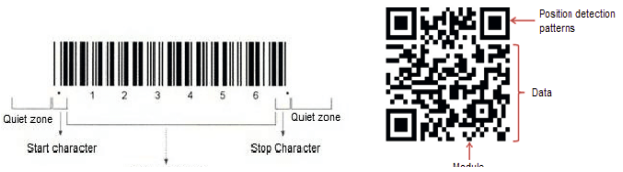

Fig. 5 Barcode and QR code

E. Wireless Fidelity (Wi-Fi)

Wireless Fidelity (Wi-Fi) is a networking technology that allows computers and other devices to communicate over a wireless signal. WiFi, wireless modems, and wireless mesh networks are the most common ways IoT devices are connected to the internet. 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 [7].

A new IEEE Wi-Fi standard 802.11 ah 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 get this standard ratified soon. With this, Wi-Fi has the potential to become a ubiquitous standard for IoT

Fig. 6 Wifi

F. Bluetooth

A Bluetooth technology is a high speed low powered wireless technology link that is designed to connect phones or other portable equipment together. It is a specification (IEEE 802.15.1) for the use of low power radio communications to link phones, computers and other network devices over short distance without wires. Wireless signals transmitted with Bluetooth cover short distances. It is achieved by embedded low cost transceivers into the devices. It supports on the frequency band of 2.45GHz from fixed and mobile devices It is a wireless technology standard for exchanging. 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.[5]

G. Zigbee

ZigBee is the most popular industry wireless mesh networking standard for connecting sensors, instrumentation and control systems. ZigBee, a specification for communication in a wireless personal area network (WPAN), has been called the "Internet of things.". It is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. ZigBee and IEEE 802.15.4 are low data rate wireless networking standards that can eliminate the costly and damage prone wiring in industrial control applications. The ZigBee RF4CE standard enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application profiles that can be used to create interoperable multi-vendor consumer electronic solutions. This communication system is less expensive and simpler than the other proprietary short-range wireless sensor networks as Bluetooth and Wi-Fi.[8]

Fig. 7 ZigBee Technology

IV. CONCLUSION

This paper discuses about the common identity management frameworks and technologies, specifies framework for particular technology. From the observation it can be said 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 will have to build standard framework and protocols for identity management.

V. 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]. Subiya Siraj1, Ms. Janhavi V "A Survey On Iot: Identity Management In Internet Of Things" International Journal For Technological Research In Engineering Volume 4, Issue 9, May-2017,pp 1678-1681
[6]. Michal Trnka and Tomas Cerny, Identity management of devices in Internet of Things environment, 2016.

[7]. 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
[8]. Ankur Tomar–Introduction to Zibgbee Technology Global Technology Centre Volume 1, July 2011
[9]. Razzak F, Spamming the Internet of Things: A Possibility and its probable Solution, 2012.
[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
[12]. Samuel Fosso Wambaa,b, *, Abhijith Anandb , Lemuria Carter "RFID Applications, Issues, Methods and Theory: a Review of the AIS Basket of TOP journals "Samuel Fosso Wamba et al. Procedia Technology 9 (2013) 421 – 430
[13]. Majeed. A, Bhana. R, Haq. A, Kyaruzi. I, Williams. M, "Devising Secure Architecture of Internet of Everything (IoE) to Avoid the Data Exploitation in Cross Culture Communications" International Journal of Advanced Computer Science and Applications,7(4), 2016.
[14]. Park, J.; Shin, S.; Kang, N. Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things. J. Korea Inf. Commun. Soc. 2013, 38, 707–714.
[15]. Park, N. Implementation of Terminal Middleware Platform for Mobile RFID Computing. Int. J. Ad Hoc Ubiquitous Compute. 2011, 8, 205–21