IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Security Survey on Internet of Things

A.A. Kulkarni[1*], P.K. Mishra[2], B.K. Tripathy[3], Manoranjan Panda[4]

[1] School of Computer Science and Engineering, VIT University, Vellore, India
[2] College of Engineering and Technology, Bhubaneswar, India
[3] School of Computer Science and Engineering, VIT University, Vellore, India
[4] College of Engineering and Technology, Bhubaneswar, India

[*]Corresponding Author: avinash.dhawandkar@gmail.com, Tel.: +91-9960278307

Available online at: www.ijcseonline.org

Accepted: 15/Jun/2018, Published: 30/Jun/2018

Abstract**—** The Internet of Things (IoT) brings together a multitude of technologies, with a vision of creating an interconnected world. This will benefit both corporations as well as the end users. However, a plethora of security and privacy challenges need to be addressed for the IoT to be fully realized. In this paper, we identify and discuss the properties that constitute the uniqueness of the IoT in terms of the upcoming security and privacy challenges. Furthermore, we construct requirements induced by the aforementioned properties. We survey the four most dominant IoT architectures and analyse their security and privacy components with respect to the requirements. Our analysis shows a mediocre coverage of security and privacy requirements. Finally, through our survey, we identify a number of research gaps that constitute the steps ahead for future research.

Keywords**—**Internet of Things, IoT Architecture, IoT Applications, Security, Privacy, Future Trends.

I. INTRODUCTION

Through rapidly advancing technologies, society is moving towards an "always connected" model. Wired and wireless networks are everywhere, open standards are defined and allowed for particularly addressing procedure. Concepts associated with the "Future Internet" are being researched [1], developed and continuously adapted in daily life. One new concept associated with the "Future Internet" is called "Internet of Things" (IoT). The IoT has become a vision where real-world objects are part of the internet: every object is uniquely identified, and accessible to the network, its position and status are known [1], where numerous services and intelligence are added to effectively expand an Internet, seamlessly combining between the digital and physical world, eventually affecting on personal and social environment.

This paper presents an overview of the Internet of Things, generic architecture and protocols, applications, security and privacy concerns, implementation and its future trends. It is positioned as an introductory paper beneficial to a wide audience ranging such as networks researchers, chief information officers (CIO), information technology specialists, consultants, decision makers in the business firms and so on. The main motivation of this paper is in three folds. They are as follows:

1. To provide an overall discussion about IoT architectures and different associated protocols;
2. To provide an overview of security threats on IoT applications;
3. To discuss and identify future trends in IoT domain.

The rest of the paper is organized as follows. Section 2 presents the reasoning for and the evolution of the Internet of Things. Section 3 describes briefly the generic architecture and protocols of IoT. Section 4 gives real-life applications of IoTs and Security and Privacy concerns in IoT are discussed in Section 5. Section 6 presents an implementation and Future trends of IoT. Finally, Section 7 concludes survey study with references at the end.

II. ARCHITECTURE

Internet, things, Internet of things, Internet of Everything! These are some of the buzzwords you may have been hearing, reading and very likely talking about endlessly. These are more than just keywords; IoT (Internet of Things) is a technology concept and/or an architecture which is an aggregation of already available technologies. Similar to the way in which Internet has changed the way we work and communicate by connecting us (humans) through World Wide Web, IoT aims to take this connectivity to next level by connecting various devices to the internet – facilitating human-machine, machine-machine interactions also.

The visionaries have also realized that this IoT ecosystem has business applications in areas of Home Automation, Automotive, Factory/assembly line automation, Retail, Medical/Preventive healthcare and more. Now that we all understand the IoT concept, it would be worthwhile to deep dive in order to get familiar with the building blocks of IoT

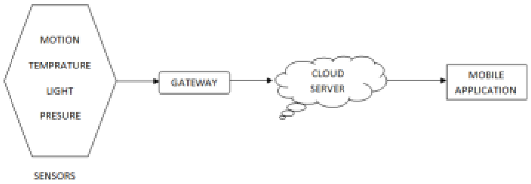

Figure 1. General IoT Framework

A. Sensors and Sensor technology

They will sniff a wide variety of information ranging from Location, Weather/Environment conditions, Grid parameters, Movement on assembly lines, Jet engine maintenance data to Health essentials of a patient.

B. IoT Gateways

IoT Gateways, as the name rightly suggests, are the gateways to the internet for all the things/devices that we want to interact with. Gateways help to bridge the internal network of sensor nodes with the external Internet or World Wide Web. They do this by collecting the data from sensor nodes and transmitting it to the internet infrastructure.

IoT Gateway development defines the success of an IoT implementation. The Gateway design can be a customized or a turnkey solution depending on the application.

C. Cloud/server infrastructure and Big Data

The data transmitted through the gateway is stored and processed securely within the cloud infrastructure using Big Data analytics engine. This processed data is then used to perform intelligent actions that make all our devices 'Smart Devices'!

D. End-user Mobile apps

The intuitive mobile apps will help end users to control and monitor their devices (ranging from room thermostat to jet engines and assembly lines) from remote locations. These apps push the important information on your hand-held devices and help to send commands to your Smart Devices.

III. POSSIBLE ATTACKS

Over the course of several decades, the progression of technology paved the way for the computerization and interconnectedness of the world around us, consisting of not only networks of high-power personal computers and servers, but also a connected web of peripheral-like devices. The Internet of Things (IoT) (also referred to as the Internet of Everything and the Internet with Things) describes a network comprised of physical objects or ”things” embedded with electronics, software, sensors and connectivity to achieve greater value and service by exchanging data with manufacturers, users and/or other connected devices. However, it is often the case that some of these devices are constrained by limited processing power, memory and power consumption. These limitations may enable adverse effects as the IoT becomes pervasive, reaching into infrastructure, buildings and homes. The current trend shows IoT technologies growing rapidly, will security for these environments grow in tandem? Researchers have deduced that IoT-based companies with no experience in security are diving into the space rapidly by adding connectivity mechanisms to their devices. As reported by Hewlett-Packard in a 2015 report on IoT research:

- Six out of 10 device user interfaces (UI) were vulnerable (such as XSS and weak credentials)
- 80% of devices (with cloud and mobile app components) failed to require passwords of sufficient complexity
- 70% of devices (with cloud and mobile app components) enabled an attacker to identify valid user accounts through enumeration
- 70% of devices used unencrypted network services
- 90% of devices collected at least one piece of personally identifiable information (via device, cloud or mobile app)

The web user interfaces that are deployed to interact with, monitor or control IoT devices have also come under scrutiny. The Open Web Application Security Project (OWASP) has enumerated the following list of the top 10 IoT vulnerabilities:

1 Insecure web interface
2 Insufficient Network service
3 Lack of transport
4 Privacy concerns
5 Insecure cloud interface
6 Insecure mobile interface
7 Insufficient security configuration
8 Insecure Software and Firmware
9 Poor Physical Security
10 Insufficient Authentication/Authorization

Current approaches to secure IoT (if at all) have attempted to leverage communication protocol-based mechanisms, such as encryption for data-at-rest or in-transit. But this may not be sufficient if the constrained endpoints themselves are susceptible to modification either by local access or remote connections. Can researchers leverage emerging computer and network security frameworks to incorporate security into this burgeoning domain? Gartner predicts that by 2020 more than 25\% of identified attacks in an Enterprise will be against IoT devices or systems, even though IoT will only account for less than 10\% of IT security budgets. Since most of the vendor provided platforms and solutions often rely on cloud infrastructure to provide data storage and management portals to consumers, the same inherent risks and vulnerabilities with cloud services reveal themselves in these predicaments [1].

IV. CURRENT THREATS

Security threats to IoT can be generally divided into two categories. In the first category, the threats are similar to those in conventional network ecosystems and revolve around confidentiality, integrity, and availability. But as mentioned, the complexity and severity of the security threats is much greater. The other category of threats arises from the type of data being carried in the IoT. IoT objects often take sensitive readings that pertain to humans; thus, for certain applications, the data in the IoT ecosystem is personal and dynamic. The data readings about device owners (or persons inadvertently monitored) may provide information leakage about persons' geological locations, health, and living habits enabling attackers to extract and disclose personal data. Thus, in this context, security starts at the device. At the device level, attack surfaces may be categorized into:

1 Device hardware security vulnerabilities
2 Firmware based vulnerabilities
3 Mobile and web app security issues
4 Radio and network communication-based vulnerabilities

To date, hackers have recorded success on such Things as Nest, WiFi Kettle and Coffee Maker, Belkin Smart Plug, Cayla Doll, LG refrigerator, Lifx light bulbs, and Smart TVs. According to [16], an experienced attacker can run code injection on a Fitbit device in less than 10 seconds, which could later plug into a personal computing device and distribute malware across a network. At the network level, each device must be equipped with a unique ID or address to enable communications over a data network. The unique attribute allows the device to be targeted.

Vulnerabilities caused by using simple passwords or relying on default passwords on embedded systems can be easily exploitable. Furthermore, such devices are often never powered down; persistent network connectivity effectively shortens the attack time against vulnerabilities of largely unsecured endpoint devices. The lack of basic security features has allowed researchers to discover new vulnerabilities and attack vectors against IoT systems, such as allowing remote ignition of a car's engine or getting root access on a home automation connectivity hub. As a threat in the wild, one of the first botnets of IoT devices was identified in 2013. Furthermore, over a quarter of identified botnets are formed by devices other than computers, such as electrical appliances, smart TVs, sensors and other household utilities.

Disrupting service is also a threat in IoT. DoS/DDOS attacks are already well documented for the Internet and enterprises; IoT is also susceptible to such attacks but will require specific techniques and mechanisms for resilience to ensure that transportation, energy and city infrastructures are not disabled or subverted. Devices with limited and constrained resources may not be capable of averting flood or fuzz attacks. Other threat scenarios include the deletion of service encryption keys stored in the memory of embedded devices to distributing malicious or corrupted software in the M2M core service provider network or corrupted firmware to endpoints. From the device to the Cloud, interesting vulnerabilities may exist. As mentioned above in [1], security software was often developed with the notion that a user would be physically present at the endpoint, to act as a decision-maker in the data security event (either configuration or attack). With IoT, the device may no longer have a user present to intervene. The problem manifests itself in risks of non-browser SSL certificate verification, and the extent to which widely deployed and relied-upon libraries and software may fail to properly validate certificates.

The authors of [1] provide an extensive and exhaustive list of the threats that exist against the IoT. Each threat may exploit one or more vulnerabilities and result in the final risk for an entire IoT system. The list has been updated from the original scenarios to broadly capture the threats that exist today.

1 Denial of service attack
2 Spoofing of credentials
3 Large-scale unauthorized data mining
4 Man in the middle attack
5 Unauthorized access
6 Side channel attack
7 Jamming
8 Fake/rogue scanner/collector
9 Worms, Viruses and malicious code
10 Procedures not followed
11 Function creep
12 Profiling
13 Exclusion of subject from data processing process

A survey conducted by the SANS Institute asked 391 individuals from a broad range of industries what they perceived as the greatest IoT threat vectors. 31% felt the IoT and the high level of embedded operating systems and applications would be left vulnerable due to poor patch management practices. Another familiar issue - malware - was the next most highly cited at 26%, with the concern being IoT devices would end up spreading malware into the enterprise. Denial of service (13%) and sabotage and destruction of connected Things (12%) were also concerns; 10% saw user error as the greatest threat vector [1]. Apart from that IoT applications are also victim to the attacks that are capable of disrupting cloud services. As mentioned in [15] , the attacks on cloud infrastructures require attention for running IoT application as well.

V. WIRELESS COMMUNICATION TECHNOLOGY

Wireless communication technologies are the backbone of IoT systems which enables connectivity between different machines as well as with different application.

A. NFC (Near field communication)

Near Field Communication (NFC) is a short-range, high-frequency (13.56MHz) RFID technology that allows the user to exchange data and information between two NFC enabled devices. In future NFC can be one of the most used communication technology due to some of the following reasons. NFC provides easy network access and data sharing, without much lengthy process of handshaking. NFC can be configured with user intent and provide much better access to the device. It also provides data security at multiple levels which is really one of the crucial points for IoT. One of the biggest disadvantages of NFC is distance. Texas Instruments recently announced that they are also working on NFC sensor transponder for Industrial, medical, wearable and many other IoT applications [9, 11].

B. RFID (Radio Freq Identification)

Radio Frequency Identification is a technology where information stored on a microchip can be read remotely, without physical contact using energy. In RF there are several frequency ranges used including Low Frequency (LF, 125 kHz), High Frequency (HF, 13.56 MHz), Ultra High Frequency (UHF, 433 MHz, 860-960 MHz) and Microwave (2.45 GHz, 5.8 GHz). These bands, in general, do not require a license if the transmitted power is limited. Some bands can be used globally (HF) while others are specific to certain regions (UHF in US, EU, and Japan) [10, 11].

C. Bluetooth

Bluetooth is based on the IEEE 802.15.1 standard. It is a low power, low-cost wireless communication technology suitable for data transmission between mobile devices over a short range (8–10 m). The Bluetooth standard defines a personal area network (PAN) communication. It operates in 2.4 GHz band. The data rate in various versions of the Bluetooth ranges from 1 Mb/s to 24 Mb/s. The ultra-low power, low-cost version of this standard is named as Bluetooth Low Energy (BLE or Bluetooth Smart). Earlier, in 2010 BLE was merged with Bluetooth standard v4.0 [11].

D. WiMax

IEEE 802.16 is a collection of wireless broadband standards. WiMAX (Worldwide Interoperability for Microwave Access) standards provide data rates from 1.5 Mb/s to 1 Gb/s. The recent update (802.16 m) provides a data rate of 100 Mb/s for mobile stations and 1 Gb/s for fixed stations [11].

E. Wifi

IEEE 802.11 is a collection of Wireless Local Area Network (WLAN) communication standards. For example, 802.11a operates in the 5 GHz band, 802.11b and 802.11 g operate in the 2.4 GHz band, 802.11n operates in the 2.4/5 GHz bands, 802.11ac operates in the 5 GHz band and 802.11ad operates in the 60 GHz band. These standards provide data rates from 1 Mb/s to 6.75 Gb/s. WiFi provides communication range in the order of 20 m (indoor) to 100 m (outdoor) [11].

F. ZigBee

The ZigBee Alliance has developed a very low-cost, very low-power consumption, an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create PAN with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth two-way, wireless communications standard. The ZigBee network layer (NWK) supports star, tree, and mesh topologies. Its low power consumption limits transmission distances to 10–100 meters line-of-sight, a defined rate of 250 Kbit/s, which is best suited for intermittent data transmissions from a sensor or input device [11, 12].

G. LOW Pan

The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. IPv4 and IPv6 are the workhorses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain. The inherent natures of the two networks though are different. IEEE 802.15.4 nodes can operate in either secure mode or non-secure mode. Two security modes are defined in the specification in order to achieve different security objectives: Access Control List (ACL) and secure mode [11, 14].

H. Mobile Communication

There are different generations of mobile communication standards including second generation (2G including GSM and CDMA), third generation (3Gincluding UMTS and CDMA2000) and fourth generation (4Gincluding LTE). IoT devices based on these standards can communicate over cellular networks. Data rates for these standards range from 9.6 Kb/s (2G) to 100 Mb/s (4G) and are available from the 3GPP websites [11].

VI. IOT APPLICATIONS

According to survey done by the IoT-I project in 2010 [3] indicated IoT's circumstance applications could be grouped in 14 domain viz; Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory, Supply chain, Emergency, User Interaction, Healthcare, Culture and Tourism, Environment and Energy. This survey was based on 270 responses from 31 countries demonstrated the most interesting circumstance applications were: smart home, smart city, transportation and healthcare. In this paper, our focus will be briefly on the IoT applications in transportation, healthcare, smart city or home, personal and social.

A. Assisted Driving

Today's different type of transportation such as cars, trains and buses along with the road and the rails equipped with sensors, actuators and powerful processors may provide beneficial information to the driver and/or passengers (i.e. accidents, temporary and/or permanent road closures, traffic congestion) to provide better navigation and safety [14]. Numerous profit and non-profit organizations would benefit from the gathered road traffic patterns information such as governmental authorities using this information for construction/ planning purpose, freight companies using this information to perform more route optimization which allows energy saving, and so on.

B. Mobile Ticketing

Electronic posters or billboards providing information in regard to transportation services can be equipped with the NFC tag. The user can get information from the web by either hovering their mobile phone over the NFC tag or pointing the mobile phone to the visual markers [14]. The mobile phone automatically retrieves and combines information from the related web services (stations, number of passengers, costs, available seats, departure and arrival time, and type of services) and provides the suggestion about tickets which is suitable for each user.

C. Sensing

Sensor device enabling multifunction focused on both inpatient and outpatient treatment and especially on diagnosing patient conditions providing real-time information on patient health indicators. Heterogeneous wireless access- based remote patient monitoring system can be deployed to reach the patient everywhere with multiple wireless technologies integrated to support continuous biosignal monitoring in presence of patient mobility [14].

D. Identification and Authentication

Identification and authentication are two terms that described the preliminary phases of the security process in computer systems which could apply to healthcare, for instance, patient identification to reduce harmful incidents to the patient, current electronic medical record maintenance and infant identification in hospitals to prevent mismatching. An identification and authentication procedure is most frequently used to manage, grant access and improve medical staff morale by addressing patient safety issues [14-16]. In addition, identification and authentication are essential parts to meet the requirements of security schemes and prevent thefts or losses of precious instruments and products.

E. Comfortable Homes and Offices

Sensors and actuators distributed deployment in houses and offices could make our life easier in several aspects, for instance, room heating can be adapted as per predefined preferences and the weather; the room lighting can automatically change according to the time of day; hazardous incidents can be prevented with appropriate alarm and monitoring system [14] and energy cost could be drastically reduced by automatically switching off the electrical equipment such as television, air condition, kettle, fridge, light bulb and so on, when not used.

F. Social Networking

This application is involved to automatically update information and location about our social activities in social networking websites. We probably think of RFIDs which generate events about people and places to assist users with real-time updates in their social networks. The mobile/web application user interfaces would display a feed of events that their friends have preliminary defined and the users not only manage their friend lists but also grant permission for each friend who is privileged to reach the information or events.

G. Thefts

An application informs the user to know if precious objects are moved from a restricted area, which indicates that the object is being stolen [14]. In this case, the event has to be notified promptly to the owner and/or security guards through SMS, call, e-mail, etc.

H. Losses

A search engine for things is an instrument that helps in finding objects that have been lost for a long time. The web-based application is one of the best approaches to finding lost objects that provide a latest recorded location for tagged objects or retrieve for a particular object's location. Furthermore, this application allows user-defined events to notify the owner when the most recent recorded object location matches predefined conditions [14].

VII. CONCLUSION AND FUTURE WORK

We presented an overview of security and privacy issues for IoT networks. As we are engulfed by the so-called IoT devices in different aspects of our life, it is indeed crucial to verify the integrity of these devices. On one hand this article will provide different communication protocols used by IoT networks along with different IoT application scenarios and on the other hand, it also highlights different security and Privacy concerns.

As part of our future works we would like to explore different attacks on IoT applications and provide suitable countermeasures for the same. We would also like to simulate different IoT architectures and present an comparative studies based on their outcomes along with lightweight security protocols especially designed for IoT framework.

ACKNOWLEDGMENT

We would like to thank Dr. B. K. Tripathy and Manoranjan Panda for their continuous support and guidance. We would continue to work on our future work under their guidance.

REFERENCES

[1] William M.S Stout, Vincent E "*Challenges to securing the IOT*" , 2016, Sandia National Laboratories Albuquerque, New Mexico, IEEE.

[2] Mangal Sain, Young J K, Hoon J Lee *"Survey on Security in IoT of things: State of the art and Challenges"*, 2017, ICACT.

[3] Surapon K, Panwit T, Kind Monngkut's,*"A survey on IOT Architecture, Protocol, Applications, Security, Privacy, Real world implementation and future trends"*,Institute of Technology Ladkrabang, Bankok, Thailand.

[4] Imen B I, Abderrazak Jemai, Adlen Loukil,*"A survey on security of IoT in the context ode Health and clouds"*, 2016, 11'th International Design and Test Symposium.

[5] Ivor D Addo, Sheikh I Ahamed, Stephen S Y, Arun Buduru *"A reference Architecture for Improving Security and Privacy in Internet of Things Applications"*, 2014, IEEE International Conference on Mobile Services.

[6] Krishna Kanth Gupta, Sapna Shukla *"Internet of Things: Security Challenges for Next Generation Networks"*, 2016, 1'st International Conference on Innovation and challenges in Cyber security.

[7] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang and Wei Zho *"A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications"*, 2017, IEEE Internet of Things Journal.

[8] Minela G, Drazen P, Srdan P, Vladimir K,*"Provided security measures of enabling technologies in Internet of Things (IoT): A survey"*, 2016, IEEE.

[9] Shain Armstrong RFID Basics: How RFID Tags Work last accessed from http://blog.atlasrfidstore.com/rfid-tag-basics on November 24, 2011.

[10] *"A survey on Internet of things architectures",* Journal of King Saud University – Computer and Information Sciences, 8 October 2016.

[11] ZigBee: Brief Introduction. Noor Ul Mushtaq. Retrieved 2016.

[12] Wireless Devices in Process Manufacturing last accessed from http://www.arcweb.com/market-studies/pages/wireless-devices-for-process-industries.aspx

[13] Prak,S.; Kim, K:, Haddad, W.; Chalrabarti, S; Laganier, . IPv6 over Low Power WPAN Security Analysis. IETF. I-D deaft-daniel-6lowpan-security-analysis-05. Retrieved 10 May 2016.

[14] Atzori L., Iera A. and Morabito G. "*The Internet of Things: A Survey"*. Computer Networks Journal, June 2010, 2787-2805. (1999). Rule learning by seven-month-old infants. Science, 283(5398), 77-80.

[15] R. V. Dharmadhikari 1,S. S. Turambekar,S. C. Dolli,P K Akulwar "Cloud Computing: Data Storage Protocols and Security Techniques", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.2, pp.113-118, April (2018).

[16] Oluigbo Ikenna V, Nwokonkwo Obi C., Ezeh Gloria N., Ndukwe Ngoziobasi G. "Revolutionizing the Healthcare Industry in Nigeria: The Role of Internet of Things and Big Data Analytics", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.6, pp.1-12, December (2017)

Authors Profile

A A Kulkarni pursued Bachelor of Science from SRTM University, India in 2011 and Master of Science from VIT University in the year 2013. He worked as "Teaching Associate" at the University of Pune, India. From last two years, he is working as "Software Engineer" at iSynergy Techsys Pvt. Ltd., Pune, India. He is interested in Object-oriented programming application, Cloud computing & IoT application security.

P. K Mishra pursued Bachelor of Technology in Computer Science and Engineering from College of Engineering and Technology, India in 2015. He is interested in IoT application security and Artificial Intelligence.

B. K. Tripathy, a triple gold medalist, is a senior professor in VIT. He has supervised 29 Ph.D. s, 13 M. Phil s and 04 M.S degrees, a senior member of IEEE, ACM, ACEEE and CSI. and is associated with over 70 international journals, published around 500 articles, 5 edited volumes, two books and two monographs.He is working on Rough sets, Fuzzy sets, Social networks, Data mining, Soft Computing, Granular computing, MCDM, Neighbourhood systems, SIoT , Big Data Analytics, Deep Neural Networks and Soft Sets.

Manoranjan Panda is a senior faculty member in CET. He pursued his BE from Utkal University in 2001 and M. Tech from FM university in 2010. He is currently pursuing his Ph.D. from Utkal University. His main research area is in IOT, WSN and Computer Networking.