A Review on Securityand Privacy Challenges in IoT

Parag K. Shelke
Computer Science & Engineering
Mauli Group of Institutions College of Engineering & Technology, Shegaon
Dist- Buldhana(MH), India
e-mail:pshelke21.engg@gmail.com

Kshitij R. Mawale
Computer Science & Engineering
Mauli Group of Institutions College of Engineering & Technology, Shegaon
Dist- Buldhana(MH), India
e-mail: krm.mawale@gmail.com

Prabodh S. Nimat
Computer Science & Engineering
Mauli Group of Institutions College of Engineering & Technology, Shegaon
Dist- Buldhana(MH), India
e-mail:psnimat@gmail.com

Sagar R. Deshmukh
Computer Science & Engineering
Mauli Group of Institutions College of Engineering & Technology, Shegaon
Dist- Buldhana(MH), India
e-mail: srdeshmukh04@gmail.com

Ashwini G. Sharma
Computer Science & Engineering
Mauli Group of Institutions College of Engineering & Technology, Shegaon
Dist- Buldhana(MH), India
e-mail:ashwini.unnati@gmail.com

Abstract—Today, we can say that the internet is everywhere, it's becoming more and more ubiquitous day by day. This is because of the existence of a massive network of interconnected wired/wireless physical objects/things/sensors/devices, which can interact through a worldwide communication and information infrastructure and provide value added services. This introduces a new concept called Internet of Things, IoT, a proposed development of the Internet in which everyday objects are connected with network , to allow them to send and receive data. The Vision of such an IoT system has the potential to mark an evolution that will have a great impact on our environments and our lives. But this ubiquitous IoT also have a number of challenges where security is on high priority. That means if one thing can prevent the Internet of things from its purpose, it will be a breakdown in security.The Globally interconnected physical objects inevitably result in security attacks that can be easily exploited if without adequate protection. With so many inter-connected devices around, it can be a reason for large number of threats posing to strike in near future.

Keywords- *IoT, data security, privacy, access control, information assurance, network and security.*

*****

I. INTRODUCTION

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data[1]. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure[2], creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit[3][4][5][6][7][8]; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

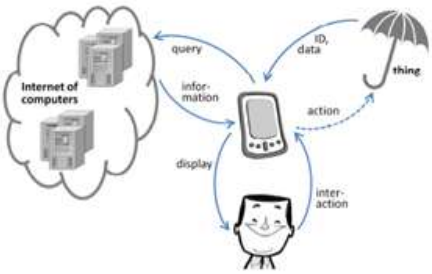

Figure1:The Smartphone as a mediator between people things and Internet.

In the Internet of Things vision, every physical object has a virtual component that can produce and consume services. Such extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use.

In the Internet of Things (IoT), everything real becomes virtual, which means that each person and thing has a locatable, addressable, and readable counterpart on the Internet. These virtual entities can produce and consume services and collaborate toward a common goal. The user's phone knows about his physical and mental state through a network of devices that surround his body, so it can act on his behalf. The embedded system in a swimming pool can share its state with other virtual entities. With these characteristics, the IoT promises to extend "anywhere, anyhow, anytime" computing to "anything, anyone, any service"[9].

From a technical point of view, the Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

- Communication and cooperation:

Objects have the ability to network with Internet resources or even with each other, to make use of data and services and update their state. Wireless technologies such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and various other wireless networking standards currently under development,

particularly those relating to Wireless Personal Area Networks (WPANs), are of primary relevance here.

- Addressability:

Within an Internet of Things, objects can be located and addressed via discovery, look-up or name services, and hence remotely interrogated or configured.

- Identification:

Objects are uniquely identifiable. RFID, NFC (Near Field Communication) and optically readable bar codes are examples of technologies with which even passive objects which do not have built-in energy resources can be identified (with the aid of a "mediator" such as an RFID reader or mobile phone). Identification enables objects to be linked to information associated with the particular object and that can be retrieved from a server, provided the mediator is connected to the network (see Figure 1).

- Sensing:

Objects collect information about their surroundings with sensors, record it, forward it or react directly to it.

- Actuation:

Objects contain actuators to manipulate their environment (for example by converting electrical signals into mechanical movement). Such actuators can be used to remotely control real-world processes via the Internet.

- Embedded information processing:

Smart objects feature a processor or microcontroller, plus storage capacity. These resources can be used, for example, to process and interpret sensor information, or to give products a "memory" of how they have been used.

- Localization:

Smart things are aware of their physical location, or can be located. GPS or the mobile phone network are suitable technologies to achieve this, as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known coordinates) and optical technologies.

- User interfaces:

Smart objects can communicate with people in an appropriate manner (either directly or indirectly, for example via a smartphone). Innovative interaction paradigms are relevant here, such as tangible user interfaces, flexible polymer-based displays and voice, image or gesture recognition methods. Most specific applications only need a subset of these capabilities, particularly since implementing all of them is often expensive and requires significant technical effort [20].

II. THE INTERNET OF THINGS (IOT)

A. A step towards a Smarter Internet

Visualize a world where billions of objects can sense, converse and share information, all interrelatedor connected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, examined and used to initiate action, and which are used for intelligent planning, management and decision making. This is the world of the Internet of Things (IOT).

Since then, many visionaries have clutched the phrase "Internet of Things" to refer to the general idea of things, especially everyday objects that are readable, recognizable, locatable, addressable, and/or controllable via the Internet, irrespective of the communication means. Everyday objects include not only the electronic devices we come across or the products of higher technological development such as vehicles and equipment but things that we do not ordinarily think of as electronic at all - such as food and clothing[21]. Examples of "things" include:

- People
- Location (of objects)
- Time Information (of objects)
- Condition (of objects)

These "things" of the real world shall seamlessly integrate into the virtual world, enabling anytime, anywhere connectivity. In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Cisco forecasts that this figure is expected to double to 25 billion in 2015 as the number of more smart devices per person increases, and to a further 50 billion by 2020[21].

With more physical objects and smart devices connected in the IOT landscape, the impact and value that IOT brings to our daily lives become more prevalent. People make better decisions such as taking the best routes to work or choosing their favorite restaurant. New services can emerge to address society challenges such as remote health monitoring for elderly patients and pay-as-you-use services. For government, the convergence of data sources on shared networks improves nationwide planning, promotes better coordination between agencies and facilitates quicker responsiveness to emergencies and disasters. For enterprises, IOT brings about tangible business benefits from improved management and tracking of assets and products, new business models and cost savings achieved through the optimization of equipment and resource usage[21].

III. PRIVACY

A. Data and privacy

Privacy is one of the most sensitive subjects in any discussion of IoT protection. The data availability explosion has created Big Brother-like entities that ile and track users without their consent. The IoT's anywhere, anything, anytime nature could easily turn such practices into a dystopia. Users would have access to an unprecedented number of personalized services, all of which would generate considerable data, and the environment itself would be able to acquire information about users automatically.

Although a dystopia is the worst-case scenario, the IoT could certainly exacerbate a range of undesirable situations. Facebook accounts already affect a user's employability and personal interactions. Imagine exponentially more such exposure opportunities [9][22].

- Privacy by design:-

One viable solution is privacy by design, in which users would have the tools they need to manage their own data. The solution is not too far from current reality. Whenever users produce a data fragment, they can already use dynamic consent tools that permit certain services to access as little or

as much of that data as desired. Taking that idea a step further, a user in Central Park could provide a location-based service with the information that he's in New York City, but not that he's in a specific park[9][22].

- Transparency:-

Transparency is also essential, since users should know which entities are managing their data and how and when those entities are using it. Stakeholders such as service providers must be part of this equation, which might make take-it-or-leave-it license agreements obsolete. Businesses will adjust their services according to the amount of personal data the user provides[9][22].

- Data management:-

A huge issue is deciding who manages the secrets. Technically, cryptographic mechanisms and protocols protect data throughout the service's life cycle, but some entities might lack the resources to manage such apparatuses. In other words, one data management policy will not fit all situations. Consequently, there must be policies on how to manage various kinds of data as well as some policy-enforcement mechanism. Developing such data management policies and enforcing them is not trivial. It requires interpreting, translating, and optimally reconciling a series of rules, each of which might be in a different language. And any policies must align with lawmaking on data protection, which itself could change[9] [22].

B. Privacy challenges:-

Some privacy challenges are identified which are faced by all stakeholders in IoT domain, from the manufacturers and app developers to the consumers themselves, and examined the responsibility of each party in order to ensure user privacy at all times. Problems highlighted[11] include:

- User approval – somehow, users need to be able to give informed consent to data collection. Users, however, have limited time and technical knowledge.
- Freedom of choice – both privacy protections and underlying standards should promote freedom of choice.
- Obscurity – IoT platforms pay scant attention to user anonymity when transmitting data. Future platforms could, for example, use TOR (The Onion Router) or similar technologies so that users can't be too deeply iled based on the behaviors of their "things".

IV. SECURITY

A fundamental problem that is pervasive in the Internet today that must be solved is dealing with security attacks [12] [13]. Security attacks are problematic for the IoT because of the minimal capacity "things" (devices) being used, the physical accessibility to sensors, actuators and objects, and the openness of the systems, including the fact that most devices will communicate wirelessly. The security problem is further exacerbated because transient and permanent random failures are commonplace and failures are vulnerabilities that can be exploited by attackers. However, the considerable redundancy that is available creates potential for designing applications to continue to provide their specified services even in the face of failures. To meet realistic system requirements that derive from long lived and unattended operation, IoT applications must be able to continue to operate satisfactorily in the presence of, and to recover effectively from security attacks. Solutions may require downloading new code [14] and this itself is open to security attacks. The system must also be able to adapt to new attacks unanticipated when the system was first deployed. These problems are beginning to be addressed by work such as that found in [15]. In [15], the system operates with a base level of support including strong attack detection capabilities. Once an attack is detected then reaction to it occurs, by self-healing.

To heal from security attacks, a system needs to detect the attack, diagnose the attack, and deploy countermeasures and repairs, but perform all of this in a lightweight manner due to the types of low capacity devices involved. Most of today's mainframe security solutions require heavyweight computations and large memory requirements, so solutions for IoT are major research challenges. Ideally, for a quick response, given the real-time nature of many IoTs, the detection, countermeasures and repairs must run in real-time as part of a runtime self-healing architecture. Sometimes, healing requires re-programming, e.g., when an unanticipated attack occurs. In these cases, healing instructions need to be securely (with authentication and attestation) delivered to the appropriate nodes and then the node's running programs need to be amended by the runtime architecture. It is likely that significant hardware support will be necessary for providing encryption, authentication, attestation, and tamper proof keys. Even if new devices are security-aware, dealing with legacy devices will prove difficult[16].

A. Privacy and security

As the adoption of IOT becomes pervasive, data that is captured and stored becomes huge. One of the main concerns that the IOT has to address is privacy. The most important challenge in convincing users to adopt emerging technologies is the protection of data and privacy. Concerns over privacy and data protection are widespread, particularly as sensors and smart tags can track user movements, habits and ongoing preferences. Invisible and constant data exchange between things and people, and between things and other things, will take place, unknown to the owners and originators of such data. IOT implementations would need to decide who controls the data and for how long. The fact that in the IOT, a lot of data flows autonomously and without human knowledge makes it very important to have authorization protocols in place to avoid the misuse of data. Moreover, protecting privacy must not be limited to technical solutions, but must encompass regulatory, market-based and socio-ethical considerations. Another area of protecting data privacy is the rising phenomenon of the "Quantified Self"[17] where people exercise access control to their own personal data e.g. food consumed, distance travelled, personal preferences. These groups of people gather data from their daily lives and grant trusted third-party applications to access their data in exchange for benefits such as free data storage and analysis. The third-party applications or providers do not have access to the raw data or usually have commercial relationships with these consumers and hence cannot use their personal data for other purposes [18].

In the retail/consumer example, data collected from users can range from location data, user preferences, payment

information to security parameters. This data gives insight into the lives of the users and hence, appropriate privacy and security mechanisms have to be in place to protect the use and dissemination of the data.

With new IOT applications being developed from evolving data that has been processed and filtered, IOT systems must be able to resolve the privacy settings from this evolving data and also for corresponding applications.

Today, various encryption and authentication technologies such as Rivest Shamir Adleman (RSA) and message authentication code (MAC) protect the confidentiality and authenticity of transaction data as it "transits" between networks. Encryptions such as full disk encryption (FDE) is also performed for user data "at rest" to prevent unauthorized access and data tampering.

In future, new standards and technologies should address security and privacy features for users, network, data and applications. In areas of network protocol security, Internet Protocol Version 6 (IPv6) is the next generation protocol for the Internet; it contains addressing and security control information, i.e., IPSec to route packets through the Internet. In IPv4, IPSec is optional and connecting computers (peers) do not necessarily support IPsec. With IPv6, IPSec support is integrated into the protocol design and connections can be secured when communicating with other IPv6 devices. IPSec provides data confidentiality, data integrity and data authentication at the network layer, and offers various security services at the IP layer and above. These security services are, for example, access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Other IP-based security solutions such as Internet Key Exchange (IKEv2) and Host Identity Protocol (HIP) are also used to perform authenticated key exchanges over IPSec protocol for secure payload delivery. At the data link layer, Extensible Authentication Protocol (EAP) is an authentication framework used to support multiple authentication methods. It runs directly on the data link layer, and supports duplicate detection and re-transmission error. In order to enable network access authentication between clients and the network infrastructure, a Protocol for carrying Authentication for Network Access (PANA) forms the network-layer transport for EAP. In EAP terms, PANA is a User Datagram Protocol (UDP)-based EAP lower layer that runs between the EAP peer and the EAP authenticator [23].

For data privacy, policy approaches and technical implementations exist to ensure that sensitive data is removed or replaced with realistic data (not real data). Using policy approaches, Data Protection Acts are passed by various countries such as the USA and the European Union to safeguard an individual's personal data against misuse. For technical implementations, there are Privacy Enhancing Techniques (PETs) such as anonymization and obfuscation to de-sensitize personal data. PETs use a variety of techniques such as data substitution, data hashing and truncation to break the sensitive association of data, so that the data is no longer personally identifiable and safe to use. For example, European Network and Information Security Agency (ENISA) has proposed to approach data privacy by design [19], using a "data masking" platform which uses PETs to ensure data privacy.

With the IOT-distributed nature of embedded devices in public areas, threats coming from networks trying to spoof data access, collection and privacy controls to allow the sharing of real-time information, IOT security has to be implemented on a strong foundation built on a holistic view of security for all IOT elements at various interacting layers.

B. Protocol and network security

Heterogeneity greatly affects the protection of the network infrastructure. Highly constrained devices that use low-bandwidth standards must open a secure communication channel with more powerful devices—for example, sensor nodes scattered in a smart city communicate with smartphones or PDAs. Securing this channel requires optimal cryptography algorithms and adequate key management systems, as well as security protocols that connect all these devices through the Internet. Although it is not clear how many resources will be available to such constrained devices once the IoT truly takes off, it is safe to optimize security as much as possible to improve the provision of future services.

In a bottom-up approach, cryptography is the cornerstone for network infrastructure protection. Although it is possible to implement existing standards, such as AES, some IoT devices, such as passive RFID tags, might be extremely constrained. Cryptographic mechanisms must be smaller and faster but with little or no reduction in security level. Mechanisms could include symmetric algorithms, hash functions, and random number generators.

In this approach, cryptography is the bricks and the mortar is the key-management infrastructures that establish keying material, for example, shared secret keys. Making this mortar requires associating previously unrelated and sometimes highly constrained objects in an extremely dynamic environment. Manual configuration works only in small and personal environments, and traditional public-key infrastructures will almost certainly not scale to accommodate the IoT's amalgam of contexts and devices. There is also the issue of rekeying devices to keep information flow safe in the long run.

Further up the network infrastructure are the communication layers. Clearly, the IoT must extensively use Internet standards for communication and service provision. Still, some devices, such as sensors that check the state of runway lights, will lack the resources to implement the Internet security mechanisms that normally protect these kinds of interactions. Therefore, security protocols require some forward-looking adaptation [10].

V. THE BEST WAYS TO PREVENT IOT THREATS

Whenever a product is purchased the security settings of that product must be checked thoroughly. Disable the remote accessible facility of the product if necessary. Default passwords should be changed and common passwords must be ignored[18].

Keep a regular check on the manufacturer's website for updates on the device's software, because if there's a security threat the manufacturer would patch the software and update it.

Since many of the devices are connected to home network and hence connected to the internet, it's better to equip the device with a firewall and ensure that it is properly configured and active.

CONCLUSION

Though the IoTs are energy-preservation equipment built for the human assistance, they also possess threat. It is our sincere attempt to review IoT threats, few safety measures and the IoT will work effectively for human's betterment. Security protocols also require some forward-looking adaptation. These Adaptations should fulfill the IoT's security performance requirements.

REFERENCES

[1] "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
[2] "Internet of Things Global Standards Initiative". ITU. Retrieved 1 June 2016.
[3] https://hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf
[4] http://www.internet-of-things research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf
[5] http://www.cisco.com/web/solutions/trends/iot/introduction_to_IoT_november.pdf
[6] http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-internet-revolution.pdf
[7] http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf
[8] http://www.cognizant.com/InsightsWhitepapers/Reaping-theBenefits-of-the-Internet-of-Things.pdf
[9] R. Roman,P.Najera,andJ.Lopez, "SecuringtheInternetofThings", IEEE Computer, vol.44,pp.51-58,2011.
[10] O. Garcia-Morchon et al., "Security Considerations in the IP-Based Internet of Things," IETF, Mar. 2011.
[11] Perera, Charith; Ranjan, Rajiv; Wang, Lizhe; Khan, Samee; Zomaya, Albert (2015) "Privacy of Big Data in the Internet of Things Era". IEEE IT essional Magazine. PrePrint (Internet of Anything).Retrieved1 February 2015.
[12] S. Ravi, A. Raghunathan, S. Chakradhar. Tamper Resistance Mechanisms for Secure, Embedded Systems, Proc. of 17th International Conference on VLSI Design, 2004. p. 605.
[13] W. Xu, W. Trappe, Y. Zhang, T. Wood, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, Proc. of MobiHoc, 2005. pp. 46-57.
[14] J. Deng, R. Han, and S. Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, Proc. of ACM/IEEE IPSN, 2006. pp. 292-300
[15] A. Wood, L. Fang, J. Stankovic, and T. He, SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks, ACM Security of Ad Hoc and Sensor Networks, Best Paper Award, October 31, 2006.
[16] S. Ravi, A. Raghunathan, S. Chakradhar. Tamper Resistance Mechanisms for Secure, Embedded Systems, Proc. of 17th International Conference on VLSI Design, 2004. p. 605.
[17] https://connect.innovateuk.org/c/document_library/get_file?folderId=9447195&name=DLFE-102773.pdf [Accessed 9th July 2012].
[18] https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf
[19] European Network and Information Security Agency. Privacy, Accountability and Trust – Challenges and Opportunities. [Online] Available from http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study [Accessed 9th July 2012].
[20] From the Internet of Computersto the Internet of ThingsFriedemannMattern and Christian FloerkemeierDistributed Systems Group, Institute for Pervasive Computing, ETH Zurich{mattern,floerkem}@inf.ethz.ch
[21] https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf
[22] http://ijesta.com/upcomingissue/04.04.2015.pdf
[23] https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf