iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5388

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Privacy in Internet of Things

Mr. Khalil Ahmed M Mujawar[1], Ms. Savita Sangam[2]
[1, 2]*Computer Engineering,University of Mumbai*

Abstract: Internet of things (IoT) is quickly gaining popularity due to its necessity and effectiveness in the computer realm. The provision of wireless connectivity as well as the emergence of gadgets alleviates its practice essentially in governing systems in various fields. Nevertheless, these systems are universal, seamless and pervasive, an issue regarding consumers' privacy remains debatable. This is valid in almost all the sectors. In this paper, we discuss related concepts and methods for data privacy in IoT, and recognize research challenges that must be addressed by comprehensive solutions to data privacy.
Keywords: Internet, IoT, Privacy, Hacker, Attacks, Data, User, Trust.

I. INTRODUCTION

Today the Internet has become omnipresent, has touched almost every crook of the globe, and is affecting human life in incredible ways. However, the journey is far from over. We are now entering an era of even more universal connectivity where almost every appliance will be connected on web. For this intelligence and interconnection, IoT devices are equipped and embedded with transceivers, actuators, sensors, and processors. IoT cannot be referred to as a single technology, rather it is an accumulation of numerous technologies that work together in tandem.

Actuators and sensors are devices that help in communicating with the physical environment. The percepts received by the sensor has to be stored and processed intelligently in order to derive useful inferences from it. An actuator is a device that is used to effect a change in environment such as brakes which are used to slow down or stop a car.

After collecting the data from sensors it has to be processed. Once it gets to the cloud or is stored in repository/servers the software performs operations on the data by using various algorithms embedded by the developers this could be very simple calculations such as checking that the temperature reading is within an acceptable range or not . Or it could also be very complex, such as using machine learning or artificial intelligence.

After processing the established data, some action needs to be taken on the basis of the derived readings. The nature of actions can be diverse. We can directly alter the physical world through actuators. Or maybe we can use virtualization. For example, we can send some information to other internet connect IoT smart things. Compute servers, actuators, sensors, and the communication network form the core infrastructure of an IoT framework. However, there are many software characteristics that need to be considered.

Mostly all of the IoT applications nowadays consists of sensors that collect private information that are very personal to the users. However, when such data is released to third parties, there are high chances of malicious privacy breaches. Even if the released data is privacy protected by standard privacy preservation techniques like noise addition, suppression; user should be well are of the privacy contents of his sensor data.

The problem of data privacy is not new, researches address this problem dates back to the early 70's. Earlier the researches on statistical databases pioneered initial data privacy methodologies. However such early methods presumed data to be stored in controlled database systems only available through specialized interfaces supporting pre-defined statistical queries.

II. LITERATURE SURVEY

A. Janice and Anthony, "Using ML to secure IoT systems".

The authors of this paper have discussed several security challenges [14] which are diverse in system and number of devices gradually increasing day by day. In the paper, they have proposed the idea of using machine learning methodologies and testbed creation method to face the security challenges in an IoT framework.

B. Benjamin Khoo, "RFID as an Enabler of the IoT: Issues of Security and Privacy".

The authors of this paper [15] have discussed enabling RFID technology which has the potential of identifying gadgets, be aware of their position then exchange information and take precautions if necessary. They have discussed various challenges in the RFID system which are privacy related issues. They have proposed a technique which is a feasible solution by putting a tag to sleep state to face the security issues.

C. Jorge Granjal et al. "Security for the IoT: A Survey of Existing Protocols and Open Research issues".

The authors of this paper [16] have discussed the next generation internet where user, sensors and internet connectivity are associated with each other. In this paper, the authors have proposed the use of ipv6 for better connectivity and better security.

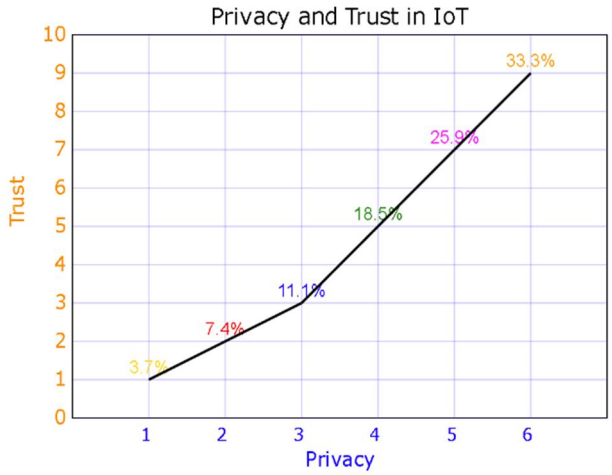
D. Kunal Kumar et al. "Integrating IoT with the power of Cloud Computing and the Intelligence of Big Data Analytics – A Three Layered Approach".

The authors of this paper [17] have discussed mixture of IoT with emerging technologies like cloud computing and big data analytics. They have also discussed sequence of lab observations done on discrete hardware products. In this paper, the authors have proposed that the random forest algorithm attained the highest success rate by performing on 18 different cyber-attacks. In this paper, the authors have challenged that no one has achieved such operation on hardware objects so far in the IoT intricate environment.

III. PRIVACY & TRUST

Internet privacy is the term concerned with the privacy and security level of personal data published via the internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect users sensitive, confidential data [5].

Trust is a amount of the value of a relationship between two people, groups of people or between a person and an organization. It is a very complicated concept that can be influenced by many measurable and non measurable properties.



IV. DIMENSIONS OF PRIVACY

A. Identity Privacy

Identity privacy refers to the need of privacy for information that can identify [5] an individual. Many approaches have been proposed to comply to this need by performing pseudonymization or anonymization.

B. Location Privacy

Location privacy refers to a form of footprint privacy. Location can reveal many things about an individual like points of interest and even religion given by the location of a church. Therefore approaches such as MIX zones and sharing of location slices have been proposed.

C. Footprint Privacy

Footprint privacy refers to the privacy of the information that gets leak unintentionally, such as operating system when browsing the internet and preferred languages. This type of data is also referred to as meta data and micro data. Approaches to fulfill this need exists but acting may leave a footprint without possibility of avoidance.

D. Query Privacy

Query privacy refers to the need for privacy regarding the information contained in a query e.g., Location and date required by the weather forecast. Methods for answering queries while respecting the need for privacy exists, however the fact that a query has been created is hard to ignore.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

V. DIMENSIONS OF TRUST

A. Device Trust

Device trust refers to the need to interact with dependable devices such as sensors and actuators. Common methods to meet this goal are trusted computing and trusted software.

B. Processing Trust

Processing trust [5] expresses the need to deal with rational and meaningful data. Trust is usually achieved by precise data gathering combined with appropriate data analytics. The result can be further improved by using data fusion.

C. Connection Trust

Connection trust refers to the requirement to exchange the correct data with right service providers exclusively. This is achieved by ensuring confidentiality, authenticity and non-repudiation.

D. System Trust

System trust discusses the desire to influence a dependable overall system. This kind of trust is achieved by being transparent about all the subjects involved like workflows, underlying technology, processes by passing respective certifications.

VI. TYPES OF ATTACKS AND RISKS

Researchers and IoT practitioners have discovered many attacks related to the security in IoT systems. Most of the attacks exploit users privacy and misuse them for illegal means. Some of the attacks related to privacy are:

A. Sinkhole Attack.

It is a kind of attack[1] in which the attacker makes the compromised node look attractive to the nearby nodes due to which all the traffic is diverted towards the attractive node resulting in the no. of packets drop i.e. all the traffic is relatively silent while the system is manipulated to believe that the data has been received on the other side. Moreover this attack results in more energy consumption which can cause Denial of service attack.

B. Clone attack.

In this attack[1] the attacker spies a particular node and extracts its credentials, cryptographic secrets, etc. He then goes on to create multiple copies of this node in the whole network due to which he can simply misguide the packets. These nodes look exactly like a certified participant so it is very difficult to detect a clone attack.

C. Malicious code injection.

This is a serious kind of attack[8] in which an attacker targets a node to inject harmful code into the system which could result in attacker getting full control of the network or in some cases complete shutdown of the network.

D. Spear-Phishing Attack.

Spear-Phishing attack is an email spoofing attack where the victim, probably a high-ranking person, is manipulated into opening the email through which the attacker gains access to the credentials of that victim and can then go on to get more sensitive information.

E. Sniffing Attack.

A Hacker[1] can force an attack into the system which could gain all the information present int the system resulting in corruption of the system.

F. Botnets.

A Botnet is a network of systems combined together with a sole purpose of remotely taking control over a system/network and distributing malware. They are used to steal private information, exploit online banking data, Distributed denial of service attacks or for spam and phishing emails with the help of command and control servers(C&C Server).

G. Man in the Middle.

Man in the Middle[8] is where an attacker interrupts and breaches communication between two separate systems or networks. It can be a critical attack since it is the one wherein the hacker secretly intercepts and transmits messages between two users when they are under belief that they are communicating safely/Privately with each other.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

H. Social Engineering.

Social Engineering[8] is an act of manipulating people so they give up private information. The types of information that criminals are seeking for are passwords, bank information etc. Or they cold try to access your system and secretly install malicious software's that will then give them access to personal information.

I. Pharming.

Pharming is a cyber-attack intended to redirect a legitimate website visitor to another fake site. It can be conducted either by altering the hosts file on a target's computer or by exploitation of a loophole/flaw in DNS server software.

J. Spyware.

Spyware is an offline application that obtains users private data without his/her consent. When the system comes online all the collected data is sent to the attackers.

VII. PREVENTIVE MEASURES

A. Common IOT Security Measures Include [13]

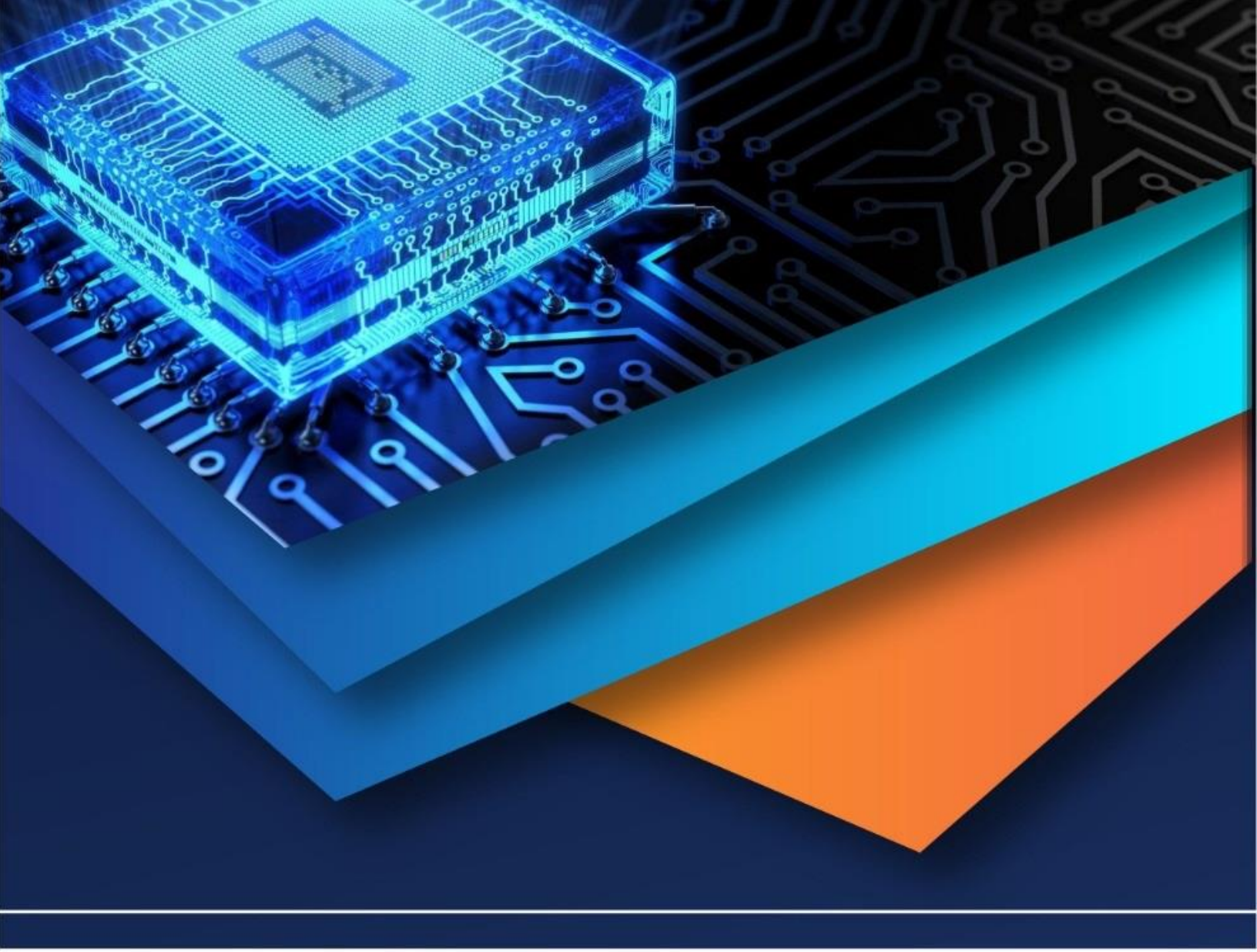
1) *Integrating security at the design stage.* IoT developers should include security at the start of any device development. Enabling security by default is serious, as well as providing the most recent operating systems and using secure hardware.
2) *Hardcoded credentials must never be part of the design procedure.* An additional measure developers can take is to require login data be updated by a user before the device functions. If a device comes with default login ids and password, users should update them using a robust password or multifactor authentication or biometrics where possible.
3) *Identity management.* Developer must provide each device with a unique identifier to understand what the device is and how it works.
4) *Hardware security.* This includes making devices tamper-proof or tamper-evident. This is particularly imperative when devices will be used in harsh surroundings or where they will not be supervised physically.
5) *Robust encryption is critical to fortifying communication between devices.* Data both at rest and in transit should be secured using cryptographic algorithms.
6) *Network security.* Defending an IoT network includes ensuring port security, deactivating port forwarding and never opening the ports unless and until it is needed, using antimalware, defenders, firewalls and interruption detection / prevention system, stalling unauthorized IP addresses; and ensuring systems are patched and updated with the latest updates.
7) *Network access control.* NAC can help recognize and register IoT devices connecting to a network. This will help in tracing and monitoring devices.
8) *Connection.* IoT devices that are directly connected to the internet must be categorized into their own networks and access to enterprise network must be restricted. Network segments should be monitoring for anomalous activity, where action can be taken when an issue is problem is detected.
9) *Security gateways.* These gateways are present between IoT devices and the network, security gateways have more memory, processing power and capabilities than the IoT devices themselves, which provides them the ability to implement features such as firewalls and other methods to guarantee that the hackers cannot access the IoT devices they connect.
10) *Patch constant software updates.* Giving methods for updating devices either over system associations or through computerization is basic. Having a planned divulgence of vulnerabilities is additionally critical to refreshing gadgets at the earliest opportunity. Consider end-of-life systems too.
11) *IoT and operational system security are fairly new to most of the existing security teams.* It is necessary to keep security team up to date with new or unfamiliar systems, teach them new architectures and programming languages and be ready for new security challenges. Cyber security teams should receive regular training to keep up with modern technology and the threats and security measures associated with it.
12) *Integrating teams.* Along with training, integrating skilled resources and new manpower can be beneficial example, having programing developers work with security specialists can help in ensuring that the proper controls are added to devices during the development phase.
13) *Consumer education.* Consumers must be made well aware of the risks of IoT systems and provided steps they can take to stay secure, such as updating default credentials (login data or the data already present which was entered by the manufacturer) and applying software updates. Consumers can advise manufacturers to create safe devices, and boycotting the use of devices that don't meet the security standards.

VIII.CONCLUSION

By analyzing, identifying, classifying various papers we have conducted a systematic study about privacy in IoT. This paper has discussed research directions in IoT data privacy. When we look at present state of the art technologies, we can easily predict how IoT will be implemented on a universal level in coming years. This report surveyed some of the most important aspects of data privacy in IoT. While the present technologies make the concept of IoT feasible, a large number of challenges still lie ahead for development of large scale IoT applications. We have studied that trust will play an important role for networking and communication research in industrial as well as academic laboratories.

REFERENCES

[1] Vaishnavi Seva, "Various Types of Attacks and Its Detection Algorithm in Internet of Things (IoT): Survey", Conference: International Conference on Advances in Science, Management and Engineering, doi December 2017.
[2] R. Beresford and F. Stajano, "Mix zones: User privacy in locationaware services," in 2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), 14-17 March 2004, Orlando, FL, USA. IEEE Computer Society, 2004, pp. 127–131.
[3] Z. Riaz, F. Durr, and K. Rothermel, "Optimized location update ¨ protocols for secure and efficient position sharing," in 2015 Conference on Networked Systems, NetSys 2015, Cottbus, Germany, March 9-12, 2015. IEEE, 2015, p. in print.
[4] R. Dingledine, N. Mathewson, and P. F. Syverson, "Tor: The secondgeneration onion router," in Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA, M. Blaze, Ed. USENIX, 2004, pp. 303–320.
[5] Jörg Daubert, Alexander Wiesmaier, Panagiotis Kikiras, "A view on privacy & trust in IoT," Conference: IEEE International Conference on Communication (ICC) 2015 Workshop Proceedings, At London, UK, DOI: 10.1109/ICCW.2015.7247581
[6] Iliev and S. Smith, "Protecting client privacy with trusted computing at the server," Security Privacy, IEEE, vol. 3, no. 2, March 2005, pp. 20–28.
[7] Ren, Z., Liu X. and Ye R. 2017. Security and Privacy on Internet of Things. In 7th IEEE International Conference on Electronic Information and Emergency Communication (ICEIEC), pp. 140-142.
[8] Hezam Akram Abdul-Ghani, Dimitri Konstantas, Mohammed Mahyoub, 'A Comprehensive IoT Attacks Survey based on a building-blocked Reference Model', (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 9, No. 3, 2018
[9] Ahmed, M. M., Shah, M.A. and Wahid, A. 2017. IoT Security: A Layered Approach for Attacks & Defenses. in IEEE International Conference on Communication Technologies (ComTech), pp. 104-110.
[10] Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z. and Bloodsworth, P.C, 2014. Semantic security against web application attacks. Information Sciences, vol. 254, pp. 19-38.
[11] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A. and Kikiras, P. 2015. On the Security and Privacy of Internet of Things Architectures and Systems. IEEE International Workshop on Secure Internet of Things (SIoT), pp. 49-57
[12] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J. and Qiu, D. November, 2014. Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20(8), pp. 2481-2501.
[13] https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
[14] Janice Canedo and Anthony Skjellum, "Using Machine Learning to Secure IoT Systems", Auburn University, doi:10.1109/PST.2016.7906930, pp.219-222, December 2016.
[15] Benjamin Khoo, "RFID as an Enabler of the Internet of things: Issues of Security and Privacy", doi: 10.1109/iThings/CPSCom.2011.83, pp.709-712, October 2011.
[16] Jorge Granjal, EdMundo Monteiro and Jorge Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues", doi: 10.1109/comst.2015.2388550, vol. 1553-877X(p), January 2015.
[17] MD Tanzim, Neeraj Anand Sharma, Kunal Kumar, A B M Shawkat Ali and Yang Xiang, "Integrating Internet-of-things with the power of cloud computing and the intelligence of big data analytics- A Three Layered Approach", doi: 10.1109/APWCCSE.2015.7476124, Deakin University, Australia, December 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY