Analysis of Security Vulnerability and Analytics of Internet of Things (IOT) Platform

16

Anteneh Girma

Abstract

The Internet of Things (IOT) has become an attractive and inviting technology that enables gathering information about all interconnected devices on real-time. These interconnected physical devices have a unique identifiers and the ability to communicate each other using its sensor technology and transfer data over a network. The collected information also provide significant opportunity for different businesses to have insight about these data by applying effective data analytics on them. Internet of Things have also revealed a huge security vulnerability that range from its authentication to its trust management, and a threat to its embedded devices. This research paper explores and discusses the challenges of Internet of things (IOT) that includes: its vulnerability, security and Privacy of IOT, current analytics of IOT, Imminent ownership threat, trust management, IOT Models, its road map, and make recommendation on how to resolve its security challenges.

Keywords

IOT · IOT security · IOT models · IOT category · IOT privacy

16.1 Introduction

Since its inception during 1991, the idea of interconnecting objects and sharing information has been advanced a great deal. Electronics devices with embedded smart technologies has become more appealing and being attractive for both business community and both home and business owners. Many different types of IOT platforms could be observed both in private and business sectors. IOT devices in smart home environment includes house appliances like dryer, washer, dish washer, TV, heating, and cooling, refrigerator. The business sectors include health care, transportation, digital city, vehicles, and agriculture.

Internet of things (IOT) is an interconnected environment of physical devices to exchange information among them and collect information from them and apply IOT analytics to take the right action. Internet of things also includes different communication such as Things to Things, Human to Things, and Human to Human interactions [1]. Information technology experts have already starting talking about nearly fifty billion smart devices would be available in 2020 and most of our household objects would be interconnected. An individual could also start managing at least ten devices. Some of these interconnected IoT devices are mobile devices and could lose connectivity due to vulnerability of wireless outages. Some of them could also run out of the battery life time to operate. The use of these heterogeneous interconnected devices in IoT platform could bring both security and interoperability issues [2].

The internet of things deployed on intranet environment for different purposes, and the information collected from these devices are monitored from the remote. The advancement in high speed connectivity has also brought certain progress in the deployment and performance of current IOT devices. The key indicators of the IOT system that is the way its different parts, including the devices and the services where the information are get analyzed, combine to generate new value or better performance.

A. Girma (✉)
Robert Morris University, Moon, PA, USA
e-mail: Girma@rmu.edu

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_16

16.2 Background Information

16.2.1 Security and Privacy of IOT

Internet of things could provide an interconnected easily managed computing environment by enabling the individual users to control their digital household items, and also the businesses to enhance the capacity, security, and other related functionalities of these interconnected items by gathering information and applying different IOT analytics operation. The security vulnerabilities of these devices has been the major and critical issue for the researchers around the globe. Because IOT is dealing with number of interconnected devices, any security vulnerability associated with each individual physical device could pose a security threat to the whole interconnected devices. Moreover, as we are also managing and controlling these devices from remote location, the other major security concern is the internet itself, which is always vulnerable and could cause another security threat. Internet is the most widely used data communication route and any access to the information which are carried out via Internet using many types of smart devices, could cause users' identity easily hacked. Other security related issues also include authentication, privacy, trust relationship among the interconnected devices, access control. Researchers reviewed thoroughly the existing authentication techniques used with IOT devices by discussing the existing limitation of those currently available authentication tools. By using their in-depth survey, they further detailed how cryptography could contribute in securing the IOT devices, and provided a well refined summary on the weakness and strength of the existing IOT security tool performances [3].

A cloud based identity framework for resolving some of the security issues associated with IOT has also been proposed [4]. This proposed frame work identified the major components like the physical environment that host the sensors and transmitters that interact with each other and the cloud services. This proposed framework also has two components: *service manager* that handles the authorization module that provides access to the sensors and receivers, and *identity manager* that handle the authentication module. Another researchers [5] also applied the two mostly popularly used keys [6, 7] with the wireless networks, by integrating them in IOT computing environment to mitigate and prevent the malicious attacks.

Other security threats related to privacy due to the involvements of those many number of interconnected devices have been identified [8]. Some middleware layers were recommended to enforce the security of the interconnected devices and the integrity of the data communicated among these devices.

16.2.2 Modelling of Internet of Things

The internet of things has been a huge interest of the business world provided that more billions of devices are expected to be interconnected through the internet in the next few years; and it brings people, data, and process to be more interconnected. The IoT is getting everywhere and its impact on the internetworking business is growing tremendously. Businesses are planning and investing much to have an adaptable and scalable infrastructure that could handle all what it takes to deploy what the IOT computing environment needs. The major capability requirements of modelling the internet of things include model construction, representation across scales, broad accommodation for multiple formalisms, integration and aggregation across models, model evolution, flexibility and modularity, scalability [9].

16.3 IOT Challenges

The number of interconnected devices at every household and every organization are getting too big, the amount of data communicating through the internet is also exploding, the number of smart devices used by every human is getting high in number, and the need for scalable and adaptable computer networking architecture is not only a much more needed but a must considered investment plan. Most importantly, the number of people who will join the computing world could make the internet traffic and the network connectivity more exploded. The interconnected devices with IOT computing environment are very different, the data generated by these different devices are also computed differently, and most importantly the location of this devices could be different. The security of this very complex interconnected network infrastructure is always a concern. The security of the communication and connectivity among these devices is the major threat and a paramount concern. Any attack aimed at one of the interconnected devices could be a security threat for all other devices. Networking systems must be built to reliably route information at rest and in motion. Security should be a major factor while designing the IOT environment. Most of currently available off the shelf IOT devices lacks security requirements and are vulnerable to get easily compromised. Moreover, IOT devices deployed on public network and accessed wirelessly are also subject to malicious attacks. The major security challenges of the IOT include Authentication, Trust, Privacy, Mobile Security, Confidentiality, Secure Middle ware, policy enforcement, and access control. Among the above mentioned security requirements, the three major three key security requirements are Authentication, confidentiality, and access control [9].

The trust level among the interconnected devices should be considered to enhance the IOT security. A dynamically trust management protocol among the interconnected physical devices have been proposed that could adapt and adjust its parameter setting for any real time changing environments. [10]. This protocol deals with physically connected devices that acts differently called malicious nodes and provide the required behavioral resolution by validating the changes in behavior and adapt on real time.

16.4 IOT Analytics

The changing and advancing nature of technology is bringing many changes in our daily life and working environments. Every household is getting smart by getting its major items interconnected. Every devices in the hospital is getting interconnected and provide any patient related information as required. Automobiles are also getting their devices interconnected with different sensors and are making driving easier and somehow safe. All these Interconnected IoT devices are handling the data analysis in a dynamic environment on real time. In most cases these analytics computations are done in cloud computing environment. The elasticity, ease of use, and scalability nature of cloud make it more attractive and convenient except the security issues associated with its service models, deployment models, and its' major characteristics.

Sensors and system logs are critical in order to collect data from each interconnected devices and execute the required data analytics. Among the requirement to analyze the data, the sensor life time and cost are the most critical elements. This is because of its major contribution in detecting and responding to inputs from the other interconnected device in the IOT platform it belongs to. The characteristics of different internet of things data types including streaming, high volume, semi structured, and non-structured data types have been discussed and mentioned that the vast majority of IOT data streams are not useful in broader context [11]. Moreover, it was noted and explained how streaming data analytics play a greater role in unlocking value from the interconnected devices, and present the main difference between IOT analytics and big data analytics.

As the number of interconnected devices is increasing, the amount of data collected and exchanged within the IoT platform is also increasing at the higher rate. Processing and analysis of big data has been a huge issue for researchers as it demand big investment requiring big memory, high level performing infrastructure, and high level of security. To resolve these issues, different analytical algorithms has been proposed to handle applying streaming and batch data feed approach. The existing big data analytics frameworks present the problem associated with big data analytics as a map reduce problem. Incremental algorithm approach using autoregression has been used to improve memory reduction by increasing and allowing each participating devices to handle the request at its node [12]. Even though the autoregression works well to handle the high level memory needs, the security and the performance issue are still continuing and remains to be resolved.

The other very challenging task in IoT is the non-existence of any form of standards that govern how the interconnected devices exchange information and operate at the cloud computing environment. The security of the cloud operation and the information exchange medium (Internet) are the most known unsecure and vulnerable cases while trying to implement the IoT Analytics. Some form of standards like Message Queue Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP) was proposed which only could handle lightweight message oriented middleware [13].

Some of those interconnected smart devices have different limitations that include sensor lifetime, bandwidth, battery life, etc. Moreover, the performance and availability of wireless infrastructure to support the required information handling and IoT analytics, is not reliable and remains to be a high level research project to be considered. These issues could result in a catastrophic consequences in Health-IoT infrastructures. For example, a Hadoop-based intelligent care system (HICS) [14] that demonstrates IoT-based collaborative contextual Big Data sharing among all of the devices in a healthcare system was proposed. This proposed system have shown a very positive and promising results in leveraging the capacity and performances of sensors, coordinators, and being flexible based on intelligent building that performs the collecting the IoT data from the interconnected devices and do the analytics. But the security of the proposed system has number of vulnerability mainly with its' confidentiality and user authentication.

16.5 Conclusion

The rapid and dynamic presence of IOT has brought a new direction of computing environment. The number of interconnected devices at every household is increasing at alarming rate, and the needs for having a more secured and powerful infrastructure to handle its data collection and analytics has been very critical. Hospitals, Cities, electrical grids and power systems, automobile systems, are among those already implementing the internet of things technology by deploying as many interconnected devices as needed. In addition to their performance issue during IOT analytics, currently existing IOT frameworks infrastructures and applications are exposed to high degree of security vulnerabilities and lacks the required security assurances. The insecurity

of cloud operation where part or all the information are stored, and the insecurity of internet media through which the information exchange is taking place, are the major and critical problems that required an immediate attentions. Security issues associated with the sensors, which are the main source of data about the interconnected devices that requires advance enhancement to leverage both its security vulnerability and performance issues is also another major areas of security problems.

The business communities is embracing the IoT success and are investing a lot. More and more other promising and enhanced IoT platform solutions are well ahead of us. Its' application is limitless. The performance issues are well getting covered. But the IoT-security issue remains to be a big challenge. Different cybersecurity attacks like DDoS, Data Integrity, Information theft, are among the major cyber-attacks that could be launched and result in severe damage in any IoT platform. In our research, we will present our detailed analysis with regard to IoT and its operation in cloud computing environment.

References

1. T. Heer, O. Murchony, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehlre, Security challenges in the IP-based internet of things. Wirel Pers Commun **61**(3), 527–542 (2011)
2. M. Babar, F. Arf, Smart urban planning using big data analytics based internet of tings, in *UBICOMP/ISWC, Ubicomp' 17 Proceeding of the the* 2017 *ACM International Joint Conference on Pervasive and Ubiqui Plannintous Cimputing, and Ubiquitous Computing and Preceeding of the* 2017 *ACM International on Wearable Computer, "International Conference on Future Internet of Things*", pp. 191–196
3. Y. Atwald, M. Hammoudeh, A survey on authentication techniques for the internet of things, in *Preceedings of ICFNDS'17*, Cambridge, United Kingdom, July 2017
4. S. Homow, A. Sardana, Identity management framework for cloud based internet of things, in *Secure IT'12*, ACM, Kollam, Kerale, India, August 2012
5. S. Silari, D. Morandi, A. Rizzardi, A. Coen-Porisini, Internet of things: security in the keys, in *Q2SWINET, Preceeding of 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Malta, Malta, November 2016, pp. 129–133
6. R. Di Pietro, L. Mancini, S. Jajodia, Providing secrecy in key management protocols for large wireless sensor networks. Ad Hoc Netw. **1**(4), 455–468 (2003)
7. G. Dini, L. Lopriore, Key propagation in wireless sensor networks. Comput Electr Eng **41**, 426–433 (2015)
8. S. Silari, L.A. Grieco, A. Coen Porisini, Security, privacy, and trust in internet of things: the road ahead. Comput Network **76**(15), 146–164 (2015)
9. S. Breiner, E. Subrahmanian, R.D. Sriram, *Modeling The Internet of Things, Foundational Approach* (ACM, Stuttgart, 2016)
10. F. Bao, R. Chen, Dynamic trust management for internet of things applications, in *Self-IoT'12, Preceeding of the 2012 International Workshop on Self-aware Internet of Things*, San Jose, California, USA., September 2012, pp. 1–6
11. J. Haight, H. Park, "IoT analytics and practice", Blue Hill Research, Analyst Insight, Report number A0173, September 2015, pp. 1–12
12. D. Mukerjee, S. Datta, Incremental time series algorithm for iot analytics: an example from autoregression, in *ICDCN'16, Proceedings of the 17th International Conference on Distributed Computing and Networking Article, Number 13*, Singapore, Singapore, January 2016
13. P. Wlodarczak, M. Ally, J. Soar, Data Mining in IoT Data analysis for a new paradigm on the Internet, in *WI'17 Proceedings of the International Conference on Web Intelligence*, Leipzig, Germany, August 2017, pp. 1100–1103
14. Hadoop-Based Intelligent Care System (HICS). Analytical Approach for Big Data in IoT in M. Mazhar Rathore and Anand Paul, Awais Ahmad, Marco Anisett, Gwanggil Jeon, ACM Transaction on Internet Technology (TOIT)", vol. 8, issue 1, New York, New York, November 2017