Indian Journal of Science and Technology, *Vol 10(11), 10.17485/ijst/2017/v10i11/107974, March 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure Communications on IoT and Big Data

Alex Roney Mathew* and Aayad Al Hajj

Department of Information Technology, College of Applied Sciences, Ministry of Higher Education, Sultanate of Oman, Oman; dr.alex.soh@cas.edu.om, aayad_hajj.soh@cas.edu.om

Abstract

Objective: Presently Internet of Things or "IoT" refers to the means of all possible communications. This paper presents a review of Internet of things and big data available on it. **Methods/Analysis:** The paper depicts the impacts and importance of these terminologies in the current scenario. Data Analytics is an emerging field which utilizes IoT and big data. Most of the organizations start cultivating big data available on IoT for their strategic decisions **Findings:** Though organizations finding it beneficial, also facing security challenges to protect their important data. Companies that fail to maintain reasonable security, it means for organizations is that if they fail to secure the life cycle of their big data environments, then they may face regulatory consequences, in addition to the significant brand damage that data breaches can cause. To protect various techniques likes cryptography, and encryption etc. are used. For secure communication in IoT-type systems currently requires many levels of configuration of security algorithms, which discourages users from implementing protection and often encourages functionality to be prioritized over security. This paper highlights new security enhancing techniques which are based on identification and authentication of the things in the IoT environment. Global Data is on the rise, by 2020, we would have manifold of the data we generate every day. This data would be generated through a wide array of sensors we are continuously incorporating in our lives. **Improvement:** So we have to implement standard approach to risk management which assumes that the trust boundary is already defined. What is missing in the risk-focused and techno-centric approach is everything related to the management of trust, i.e., the new functions and processes, and the new policies and structures required to expand the risk boundary.

Keywords: Big Data, Communication, Cryptography, Data Analytics, IOT, Security

1. Introduction

When taking into account the monetary value created from technology, as well as the potential for new market opportunities, it is estimated that the Internet of Things will generate $14.4 trillion in net profit for enterprises over the next two decades. Organizations across all industries have started to develop and implement their own IoT strategies with the motive toward seizing the opportunity this new era presents Internet of things (IOT) enables any device to be able to connect any other device using the internet. To highlight any device aspect the term internet of everything is also used. The Internet of Things is all about collecting data from various sources and making it useful in ways that enhance how we go about our business. The tremendous volume of data that will be coming in from devices presents a huge challenge for IoT solution providers. Big Data solutions will be overcoming this challenge by giving us the capacity to analyze data, and discover relevant trends and patterns.

Big data can be defined as a collections of data sets with sizes beyond the ability of commonly used software tools such as database management tools or traditional data processing applications to capture and

**Author for correspondence*

analyze within a stipulated time. Big data is characterized by '4 Vs': volume, variety, velocity and veracity. That is, big data comes in large amounts (volume), is a mixture of structured and unstructured information (variety) arrives at (often real-time) speed (velocity) and can be of uncertain provenance (veracity). Size of Big data is constantly increasing, ranging from a few dozen terabytes in 2012 to today many petabytes of data. To meet the demands of handling such huge quantities of data, new platforms of "big data" tools are being used and new developments are continuously done. Big data brings with it tangible benefits for any company willing to use it. The advantages of leveraging big data are real and oftentimes far-reaching, which is why so many organizations have adopted big data for their own operations.

For a long time, communication over the Internet has largely depended on the use of IP addresses to identify communicating parties. Some IoT uses cases will require a new technique of communication technologies that are able to provide greater security and more efficient communication. Pitfalls are still plentiful, and few represent as much of a problem as big data security. Businesses may be willing to use big data, but they must also be aware that security remains a top concern. This is in part because the technology is advancing so rapidly that the solutions to security problems often fall behind. If a business wants in on the enabling world of big data analytics, they'll need to be aware of some of the biggest security concerns first. IOT enabled devices would generate and transmit so much data that security issues[1] as well as managing the life cycle of those data are other dimensions that need to be addressed.

2. Impact of IoT on Big Data

IoT and big data basically are two fold which can be considered as sides of the same coin. Today the business world is facing the great challenge which is the management and extraction of valued information from the big data in IoT environment. Big data is a terminology which is referred to the vast amounts of data generated by connected technology. Big data is a tool that is used in modern competitive world by many business organizations to make their advertising and other marketing efforts more effective. Using the historic data for prediction and analysis of certain situation is not new, but what is new is the tremendous amount of data is available with us due to the Internet of Things (IoT). So the big data and IoT are really connected and must be used together while thinking about the security mechanisms. What is the impact of IoT on big data? The answer is IoT changing the way of using the big data by companies for analytics purposes.

The IoT and big data both are growing field, and are set to affect many areas of business and everyday life. But which particular sectors are likely to feel the IoT/big data disruption first? In its 2015 Internet of Things predictions, according to IDC, Presently over 50% of IoT activity is centered in manufacturing, transportation, smart city, and consumer applications, but within five years all industries will have rolled out IoT initiatives.

New generation of IoT and big data applications is required to address specific business solutions which requires needs such as predictive maintenance, loss prevention, asset utilization, inventory tracking, disaster planning and recovery, downtime minimization, energy usage optimization, device performance effectiveness, network performance management, capacity utilization, capacity planning, demand forecasting, pricing optimization, yield management, and load balancing optimization. In Figure1 shows the process of obtaining large data through various application interfaces available on internet. The big data then processed by using big data analytics which further can be utilized by enterprises for their strategically decisions and to increase their sales performance.

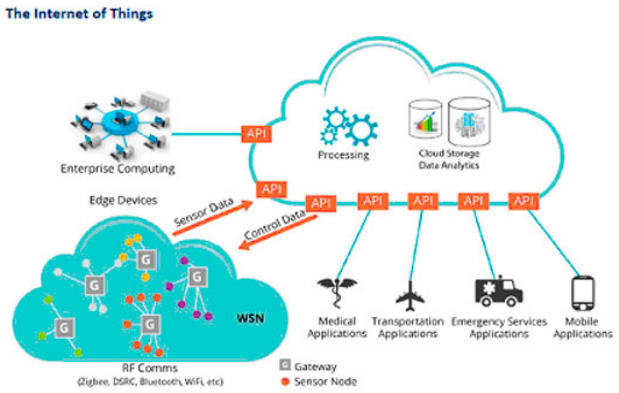

Figure 1. Internet of Things.

3. IoT and Big Data: A New Competitive Advantage

In modern business world it is very important for leading business organizations to use Big Data to compete in the market and to outperform. The well-known or brand value business organization using data-driven strategies to innovate, compete, and capture value. Business organizations are establishing a department which able to provide proper data analytics platform and infrastructure to analyze the big data on IoT environment. Big data analytics enables the organizations to make better decision and to compete better in the market.

In present era of business competition the use of business intelligence techniques is essential for any business organization. The BI techniques includes the Big data analytics which extracts the information which is untapped by classical approach of business data mining. So the data scientist, and analytical professionals came into existence and their work to do big data analysis can be achieved through software tools available for analysis of large amount of data. The recent techniques which are using for big data analysis such as data mining, predictive analysis and statistical analysis performing well for the business organizations. The amount of data is so vast that the data warehouses which are previously used for analytics purposes are not capable to handle the processing requirement of modern analytical tools. The latest technologies which are being used Big Data Analytics are Hadoop and related tools such as YARN, Map Reduce, Spark, Hive and S as well as NoSQL databases.

Big Data provides new growth opportunities and entirely new categories of business competitors, by analyzing and aggregating industry data. Many of these will be companies that stands in the middle of large information availability where data about products and services, buyers and suppliers, consumer preferences and intent can be captured by analytics tools and analyzed. The leaders have started aggressively cultivating the Big Data capabilities. An IoT device can generates continuous streams of data in a measurable way, and companies must handle the high volume of stream data and perform actions on that data to extract useful patterns. Business organizations must take actions after the big data analysis that can be event correlation, metric calculation, statistics preparation, and analytics. In a normal big data scenario, the data is not always stream data, and the actions are different.

4. Security Challenges within IoT and Big Data

The Internet of Things (IoT) has a data problem. Everyone is claiming to be the world's smartest thing. But that sprawl of devices, lacking context, with fragmented user groups, is a huge challenge for the rapid growing industry. This paper describes the security challenges when organizations start moving sensitive data to a Big Data repository.

The major security challenge in IoT is physical and virtual challenge. If we talk about physical challenge it will be more complex when the multilevel security provisions are used for the network devices. Since firewalls is kept behind the network devices and also data has to be flow across the business organizations, the things becomes complex. When the network devices accessed by business organization to gain the information from various sources the virtual challenge is also comes into the existence.

In IoT environment the main target of the security attacks is the whole communication process which is performed between IoT devices. The components involved in this communication process are the IoT device itself and the gateways. The gateways are the central point which controls the whole network and the related processes. If the gateways damaged the whole network is breakdown and the whole communication process affected. While communicating between IoT device one of the virtual threat i.e. interference can be occurred which has to be handled properly.

Interference caused in the situation when the data which is being communicated is distorted or totally destroyed due to occupancy of physical channel by another undesired information. In IoT environment sometimes permanent communication link has to be established which carries traffic flow continuously but due to interference denial of service occurs which makes the communication resources unavailable and it is really a devastating in IoT and big data environment. Interference problem can also be occurred due to jamming of physical communication channel between nodes.

While performing communication, it is completed in several steps and various devices involved viz. sensors, gateways, actuators throughout the communication process. At any step the attackers may be able to access the devices or signals being used in the communication process, the threat is signal interception. The signal inter-

ception attacks secretly relay and may alter or distort the information which is being communicated between the two parties. Signal interception mainly caused due to lack of protection in traffic flow, unauthenticated access and insecure network resources physical and virtual both.

One of the challenge at the physical level while communicating is intrusion. Intrusion is occurred due to insecure user interfaces, insecure software and firmware as well as unprotected network resources. The attacker takes the advantage of security loop holes and lack of authentication and authorization mechanism in devices and the IoT environment. An attacker may get succeed to authenticate himself for the system. By doing this attacker will be able to access data as well as all communication devices and functionality of them, and reads all the information. This situation may be referred as exploitation. So exploitation only occurred when an attacker may get access to the communication resources i.e. gateways and other devices as well as the data which is being transferred. One solution to this threat can be limiting the accessing rights to the data as well as physical resources by adopting access control mechanism. Therefore employing the accessing restriction on physical devices or gateways is an important part of security mechanism within IoT-environments for avoidance of the physical threats that can affect integrity, confidentiality of the communication process.

We have discussed virtual and physical threats while communication in IoT environment. In the communication process gateways plays a very important role since it connects many sensors and devices which are communication through it. If a gateway is hijacked the attacker can get the access to all the sensors and devices which are involved in communication process. Through hijacking of a gateway large amount of data can be distorted or the communication resources make not available which is a serious threat in IoT and big data environment.

It is very often and frequent action in IoT environment to install new devices, replace damaged devices and also to remove malfunctioned and unnecessary devices. These actions made the IoT as a dynamic environment. But it also increases the security threats since unknown or false devices and gateways can be deployed by the attackers. It must be ensured that any of these kinds of activities cannot get the authentication authorization for the running IoT environment. This must be achieved through end-to end encrypted communication. So no middle man can get access to any of the process in communication. In end-to-end communication even gateways would not able to access any of the text which is being communicated. But the disadvantage of this end-to-end encryption is that the endpoint nodes are responsible for managing the keys. And the terrorist can take advantage of this by hiding their communication and identity. The end nodes can also be hacked or data can be steal by hacking the cryptographic key generated by the end nodes. One solution for remedial of this threat is biometric information can be used to authenticate and authorize the communication.

5. Security Enhancing Techniques

We have discussed various security challenges in IoT and big data environment in the previous section. Security is the primary concern as well as challenging also due to involving billions of devices on the internet and different new technologies which claims to provide solutions to the security threats. The security mechanism ensures the correctness and integrity of the data which is being communicated through the communication devices and gateways. The security provision ensures to send correct data to its destination without any distortion and tempering throughout its journey from source to its destination. Security mechanism should build a trust that one is talking to the correct device and using the correct communication channel through which any confidential data can be sent.

To protect from threats an IoT environment should be having the process of strict identity checking when any of the things seeking the permission for accessing data or any resources involved in the communication process. Mutual identification and authentication is necessary while communicating. Two issues identification of each device and authentication of each identity are need to be resolved.

Identity checking of the components (sensor, device, gateway, or server) in communication process is important but it is difficult in IoT due to large number of devices involvement and restricted communication method. One of the barrier is that the lifetime of an IoT devices is too short so it is frequently changed. And also the same identity cannot be provided for a long time due to fear of hacking. When a thing is trying to authenticate itself a strong mechanism for authentication should be used viz. lightweight token and the private encryption key of the certificate. URL can also be associated with the device

IP which is a strong way for identification of any device or thing. Using secret software security tokens as well as hardware security tokens can be an option for identification and authorization. These methods produces one time passwords which has to be used within a stipulated time period.

While using encryption technique to protect data it is not sufficient to limit the access to cryptographic keys rather it is important to keep the secret keys completely confidential which can assures a high degree of authentication process. But the issue in adopting the cryptographic security is that the encryption keys or secret keys has to be stored somewhere in the IoT environment which is the part of communication process itself. To resolve this issue hardware intrinsic security can be adopted. This mechanism facilitates not to store any encryption key permanently but it can be generated while it is required for the authentication process. After completion the authentication process by using this secret key it must be deleted from all the storage devices i.e. registry and temporary storage device also. The encryption key generation algorithm should be designed in such a way that no key should be repeated and any step of the communication process cannot trace the key. The key should be linked with the device so it cannot be reproduced further.

The authentication of the things in the IoT environment can be done through biometric templates. The biometric templates are made of enrolled or registered users and then these templates can be used for matching with the templates provided by users at the time of authentication. The security of biometric templates of enrolled users is very important to protect the sensitive information which is contained in them. The protection of these biometric templates can be assured by using a combination of perceptual hashing techniques and Zero-Knowledge Proof of Knowledge (ZKPK) protocols.

To break the security mechanism a number of attacks can be possible on the network which is used for communication. These attacks may be denial of service attack, intrusion etc. Intrusion Detection Systems (IDS) are required to detect impostors and malicious activities in the network, and firewalls to block unauthorized access to networks. Updating of analytics algorithms that detect various security issues, predictively pre-empt attacks, and automatically alert, escalate, and log all priority issues should be provisioned continuously. There should be the provision of Escalating exceptional, unprecedented, and undiagnosed IoT issues to human security analysts for further investigation. To organize secure communication in IoT the provisions of assembling the compliance, legal, contractual, trust, reputation, governance, operational, and risk management frameworks to handle the interlocking responsibilities must be kept for ensuring end-to-end IoT security. Generally accepted IoT security practices should be done like Inspection, certify, vet, monitor, and audit the suppliers of IoT components and life-cycle services.

5.1 Combined Secure Storage and Communication for the Internet of Things

The future Internet of Things (IoT) may be based on the existing and established Internet Protocol (IP). Internet Protocol Security (IPsec) is a mechanism which ensures private and secure communication over IP networks. The protocol provides a number of functions and is quite flexible. It provides controlling the unauthorized access to the device, connectionless integrity, authentication of the data at the source, protection against various attacks and confidentiality by using encryption techniques. Access control can be achieved through cryptographic keys. For establishing secure IP connection many kinds of cryptographic methods are used. The cryptographic authentication process ensures the integrity and generates a hash key which is based on the IP packet and used for integrity checking. Hash keys used for integrity checking are produced by using hash functions. The secret key which is accessible to both the parties involved in communication can be used to compute the hash value for integrity checking by sender and receiver also.

Secure communication 4 in IoT-type systems currently requires many levels of configuration and/or application-level security mechanism, which discourages users from implementing protection and often encourages functionality to be prioritized over security. The lack of secured links encourages the hackers to do attacks on the network and theft of the data.

Generic Bootstrapping Architecture (GBA)[8] technology, based on the Authentication and Key Agreement (AKA) protocol which is used for device identification and authentication at the transport layer while communicating in IoT environment.

To secure data and IoT system from various threats information security techniques are to be adopted. These techniques identify the possible threats and by analyzing

the seriousness of these threats provides possible solutions for taking remedial actions. The main threats for an IoT environment which are virtual and physical must be handled by security techniques to ensure secure and smooth communication. Secure key storage and authentication methods should have used together which makes the means of communicating securely.

6. Conclusion

Big Data is the fastest growing technique that we perceive in the present world. The impact of big data and internet of things is manifold in our life. By 2020 we would be generating four times of the present data, and that is to be handled with security provisions. This data would be generating by various new gadgets, sensors that we are including daily in our life. The data which is generated day by day is have bring the tremendous changes in the business world also. The business world is utilizing this big data by analyzing it in targeting marketing in specific demographics. But at the same time while business world using big data analytics they should be concerned about the security mechanism of this data to protect it. Data is freely flows on the IoT environment, any malicious user can access it, can misuses it. Companies need to be aware of the security threats. IOT enabled devices would generate and transmit so much data that security issues as well as managing the life cycle of those data are other dimensions need attention. For ensuring secure communications through IoT new security techniques should be adapted rapidly and it should be a continuous process.

7. References

1. Okman L, Gal-Oz N, Gonen Y, Gudes E and Abramov J. Security Issues in NoSQL Databases. Proceedings of Trust Com IEEE Conference on International Conference on Trust, Security and Privacy in Computing and Communications. 2011, p. 541–7. Crossref
2. Top 10 Big Data Security and Privacy Challenges, Cloud Security Alliance. 2012 [Date Accessed: 5/12/2016]. Available from: Crossref
3. Jonker W and Petkovic M. Data Security challenges and research operations. Springer International Publishing. Switzerland; 2014. p. 9–13. LNCS 8425. Crossref
4. Feng J, Chen Y and Liu P. Bridging the Missing Link of Cloud Data Storage Security in AWS. Proceedings of 7th IEEE Consumer Communications and Networking Conference - Security for CE Communications (CCNC'10); Las Vegas, Nevada, USA. 2010 Jan. p. 9–12. Crossref
5. Sarkar D and Nath A. Big Data – A Pilot Study on Scope and Challenges. International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS). 2014 Dec 31. 2(12):9–19. ISSN: 2371-7782).
6. The ESG White Paper. The Big Data Security Analytics Era Is Here. 2013 Jan.
7. An Inside-Out Approach to Enterprise Security, Oracle/ CSO Custom Solutions Group white paper. 2013.
8. 3GPP. "3GPP Specification detail; 3GPP TS 33.220 – Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)," 2016. [Accessed February 2016]. Available from: Crossref
9. Ericsson White paper "Bootstrapping security" 284 23-3284 Uen. 2016 Feb.
10. Toshniwal R et al. Big Data Security Issues and Challenges. International Journal of Innovative Research in Advanced Engineering (IJIRAE). 2015 Feb; 2(2):15–20.