

BIG DATA ANALYTICS FOR DEVELOPING SECURE INTERNET OF EVERYTHING

Mr. K. Karthiban,

Assistant Professor, Technical Academy,
Karpagam College of Engineering,
Coimbatore, Tamil Nadu India.
Email: karthiban.gk@gmail.com

Dr. Jennifer S. Raj,

Department of Electronics & Communication Engineering,
Gnanamani College of Technology,
Namakkal, India.
Email: jennifer.raj@gmail.com

Abstract: Storage and processing of information is the major application of big data analytics. Internet of Everything (IoE) is the smart connection between people, data, things and processes. This paper studies the available frameworks used for developing secure Internet of Everything with big data analytics. Big data is a collection of data generated from the sensors embedded in the surrounding physical objects. This information can be used for analysis of the surroundings and development based on the inference. Internet of Everything uses this data for automation of the electronic equipment in the surrounding environment. However, with the increasing level of automation, the vulnerability to attack also increases. This paper presents a detailed analysis of big data analytics that is used for developing a secure internet of everything.

Keywords: Big data analytics, Internet of Everything, data security, Cloud Computing

1. INTRODUCTION

One of the prominent application of cloud computing includes big data storage and processing [1]. With the progress of paradigm like Internet of Everything, person to machine, machine to machine and person to person communications are established. However, it is essential to converge the IoE systems along with big data for software processing. In IoE, several sensors are used for accumulation of data. Big data analytics is used for gathering, combining and applying the data to improve the quality of living [2]. It is essential to ensure privacy and safety while doing this process.

Figure 1 represents Gartner's Hype Cycle of Emerging Technologies for the year 2014. IoT and Big Data technologies are in the peak of inflated expectations and are expected to sustain for the next 5-10 years. IoE generates huge volumes of diverse digital data. Big Data Analytics tools can assist in efficient storage,

management and analysis of this data. It is essential to combine big data analytics with IoE as IoE by itself cannot deal with the complete interaction between its subsystems and extract the meaning from the data. IoE platforms are scalable, easy to use, offer flexibility for deployment, clear system architecture and has user interface that are developer-friendly.

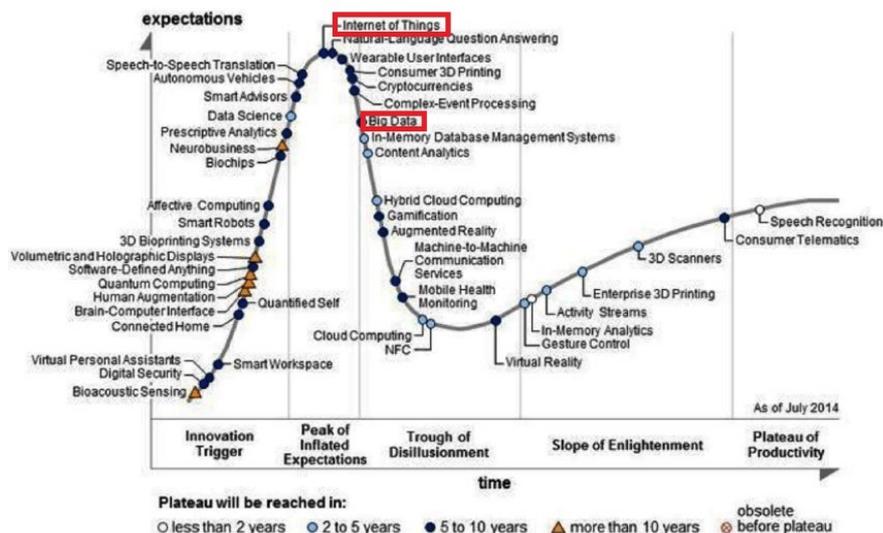


Figure 1. Gartner's 2014 Hype Cycle for Emerging Technologies.

(Source: <https://www.gartner.com/en/documents/2809728/hype-cycle-for-emerging-technologies-2014>)

2. BIG DATA ANALYTICS

The rapid advancement of digital data has led to the evolution of the term 'Big Data' [5]. The information is analysed and put to use in such a way that it improves decision making, productivity and facilitates innovation. Big data is defined by Gartner as "...high volume, velocity and variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making". Big data analytics offers multiple advantages like cost reduction, speed, better decision making, ability to develop new products and services.

Figure 2 represents the major features involved in Big Data Analytics. The voluminous data generated is vulnerable to security breaches. It is essential to secure this data. Data has to be secured at every level from source, transfer, storage to output. Alvaro et al. [17] discussed about the advances and challenges in big data analytics and applying the technology for security. Big data can be easily applied for fraud detection in case of credit card usage. Due to continuous increase in the size of data, data provenance issue occurs. Data mining

without notification or permission is a challenge to the safety of the data. The cluster-based property of the platform is another factor that makes big data vulnerable.



Figure 2. Big Data Analytics

In order to overcome these security issues, several technologies have been applied, tested and is being improvised. Some of the notable technologies for securing big data analytics include encryption, centralized key management, user access control, intrusion detection and prevention and physical security. Certain companies like Thales, IBM, Cloudwick, Logtrust and so on provide data security as an exclusive service. Big data is classified into three categories namely structured data, semi-structured data and unstructured data [18].

Analytic techniques used in big data includes HADOOP, MapReduce, HDFS, Hive, HCatalog, HBase, PIG, Mahout, Cassandra, In-Memory, NOSQL and so on. Big data architecture must satisfy certain high-level requirements such as sophisticated tools for analytics, query options, flexible storage and reliable data assimilation. Timeliness, accuracy, data organisation and relevance are the significant dimensions in machine learning. Privacy protection can be provided in big data using techniques like encryption, authentication, metadata, tagged data, unstructured distribution, anonymization, tracing and ensuring rules and legality.

3. INTERNET OF EVERYTHING

IoE depends on data, process, people and things connected together and to the internet [12]. It influences the lives of people, industrial processes and businesses. Real time information accumulated from various sensors are interlinked and applied to people-centred automated processes [14]. IoE assists in attainment of social and economic goals, environmental sustainability and public policy goals. It is also used in smart grid, traffic control

and planning, automation, e-learning, remote monitoring, fossil fuel mining and various other industries. Google reports over 346 hundred thousand entries for “IoE data sources” and 33.4 million entries for “IoT data sources” in August 2018. “The Global Information Technology Report 2014: Rewards and Risks of Big Data” reports generation of exabytes of data from IoE (People, Business, Government) every day.

An article on “Data Management in the Internet of Things (IoT) Era: Common Policy Principles and Data Handling Framework for Data Security and Privacy” [16] provides certain principles and points regarding security and privacy issue of IoT related data. “1) Consumers should own their own data, 2) Data can drive economic growth, and provide a multitude of societal and individual benefits, 3) Not all data is equally sensitive, 4) Consumers must have confidence in how their data is used, stored, and transported, 5) Technology is a significant part of the solution, and 6) A data-handling framework that categorizes different types of data and associated management strategies is required to unlock the potential of IoE” are the significant principles discussed.

Figure 3 represents the framework of Internet of Everything. It is a combination of people, things, data and processes. This results in generation of billions of billions of information every day. Traditional techniques can be used for management of data from IoE, but it may not prove to be efficient for data from all sources. Hence research is being conducted for securing the data created by IoE.

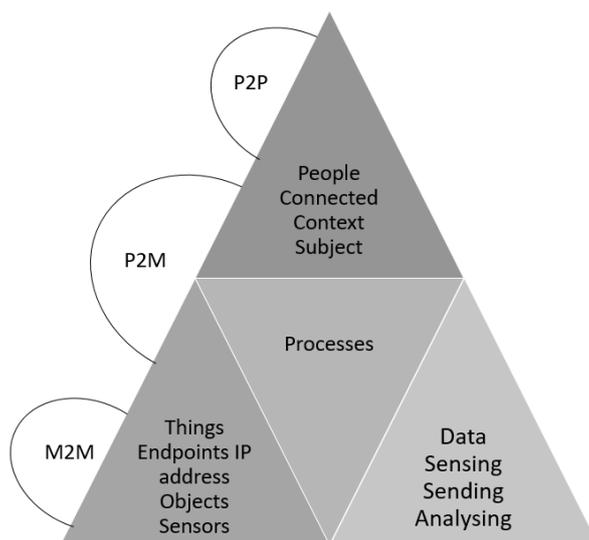


Figure 3. Internet of Everything (IoE)

General security measures in IoE can be taken by incorporating security at the design phase, avoiding hardcoded credentials, including public key infrastructure (PKI) and digital certificates, Application performance indicator (API) security, identity management, hardware security, strong encryption, network security, network access control, proper monitoring of network segments to detect anomalies, security gateways,

patch management and continuous software updates, integrating teams and providing proper consumer education.

4. SECURING IOE WITH BIG DATA ANALYICS

The Internet of Everything connected device count may reach a hundred billion by the year 2020. Voluminous data will be generated by IoE. Several issues and challenges may be associated with such data with respect to information and communication technology (ICT). Big data analytics is essential for processing this generated data and to put them to use [3]. Big Data is sometimes referred as facts that is collected regarding reality. The generation of these facts is done by sensors implanted in physical articles that surround us. Larger the information gathered, more it can be used for enhancing technology. Since monitoring and generating information is a continuous process, it is essential to keep these devices active and connected to the internet always to ensure uninterrupted updating of data to the server. This makes us vulnerable to attacks that can damage the safety and security of the information.

Laney et al. [15] related big data to three words namely Velocity, Volume and Variety (3 Vs). Variability, Veracity and Value of the data are also prominent properties of big data. It represents the rate of generation of data, amount of data generated and that data is available in different forms respectively. Most of this big data is stored on cloud platform. Even though this platform is supposed to be trustworthy and secure, several companies use this data to study the browsing and purchase habits of the user. This can be a major privacy concern for many users. The data is exposed to data leakage and security attack vulnerabilities. These data breaches affect the reputation of high profile companies if not addressed properly. The technologies used for Internet of Everything are not intended for communication security. This leaves the data as well as the network vulnerable. This issue is addressed by Big Data analytics in many cases.

IoE generates big data that is accurate. The cyber-criminal attackers may even alter data in the IoE environment leading to chaos and disorder. The increasing volume of huge amount of varied data represent the generation of big data by IoE [5]. Gunasekaran et al. [6] presents an architecture implementing IoT and big data for health care related applications with the help of Grouping and Choosing (GC) for security and Meta-Fog-Redirection (MF-R) architecture for data collection, transfer and storage. Tasweef et al. [7] proposes the combination of IoT, big data analytics and complex event processing techniques for solving the major issues in dealing with data in healthcare industry. They suggested a holistic healthcare system that can perform operations like drug detection, monitor patients from a remote environment, assist in health insurance settlement and progress the clinical results.

Tanzim et al. [8] presented a three layered approach by integrating IoT, Cloud Computing and Big data analytics. RandomForest classification algorithm is used which provides cyber-attack identification rate of up-to

93.9% in composite environment. Dr. Norbert et al. [10] performed an analysis on big data and internet of things and the growth of these technologies as a new software ecosystem. The paper reviews the platforms and concepts used in IoT solutions that are driven by voluminous data.

5. CONCLUSION

This paper performs a thorough analysis on developing a secure Internet of Everything framework based on big data analytics. It also gives an overview of the generation of big data from people, machines and sensors involved in IoE. The connected and smart community concept is introduced. The application of these technologies in smart cities, healthcare monitoring, industrial automation and several diverse fields and the research done is presented. Future extension can be made by segregating the roles of big data in different platforms like social media, business intelligence, data warehousing and so on. Data security during transfer from IoE to cloud or other storage is also a major factor to be considered.

References

- [1] Suciu, George, Victor Suciu, Alexandru Martian, Razvan Craciunescu, Alexandru Vulpe, Ioana Marcu, Simona Halunga, and Octavian Fratu. "Big data, internet of things and cloud convergence—an architecture for secure e-health applications." *Journal of medical systems* 39, no. 11 (2015): 141.
- [2] Sun, Yunchuan, Houbing Song, Antonio J. Jara, and Rongfang Bie. "Internet of things and big data analytics for smart and connected communities." *IEEE access* 4 (2016): 766-773.
- [3] Riggins, Frederick J., and Samuel Fosso Wamba. "Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics." In *2015 48th Hawaii International Conference on System Sciences*, pp. 1531-1540. IEEE, 2015.
- [4] Doku, Ronald, and Danda B. Rawat. "Big Data in Cybersecurity for Smart City Applications." In *Smart Cities Cybersecurity and Privacy*, pp. 103-112. Elsevier, 2019.
- [5] O'Leary, Daniel E. "BIG DATA', THE 'INTERNET OF THINGS' AND THE 'INTERNET OF SIGNS.'" *Intelligent Systems in Accounting, Finance and Management* 20, no. 1 (2013): 53-65.

[6] Manogaran, Gunasekaran, Ramachandran Varatharajan, Daphne Lopez, Priyan Malarvizhi Kumar, Revathi Sundarasekar, and Chandu Thota. "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system." *Future Generation Computer Systems* 82 (2018): 375-387.

[7] Naqishbandi, Tawseef, C. Imthyaz Sheriff, and S. Qazi. "Big data, CEP and IoT: redefining holistic healthcare information systems and analytics." *Int J Eng Res and Technol* 4, no. 1 (2015): 1-6.

[8] Khorshed, Md Tanzim, Neeraj Anand Sharma, Kunal Kumar, Mishal Prasad, ABM 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." In *2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)*, pp. 1-8. IEEE, 2015.

[9] Charmonman, Srisakdi, and Pornpisud Mongkhonvanit. "Special consideration for big data in IoE or Internet of everything." In *2015 13th International Conference on ICT and Knowledge Engineering (ICT & Knowledge Engineering 2015)*, pp. 147-150. IEEE, 2015.

[10] Jesse, Norbert. "Internet of things and big data—the disruption of the value chain and the rise of new software ecosystems." *IFAC-PapersOnLine* 49, no. 29 (2016): 275-282.

[11] Sahmim, Syrine, and Hamza Gharsellaoui. "Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review." *Procedia computer science* 112 (2017): 1516-1522.

[12] Shojafar, Mohammad, and Mehdi Sookhak. "Internet of everything, networks, applications, and computing systems (IoENACS)." (2019): 1-3.

[13] Fan, Xiayue, Xiaorui Liu, Wenbin Hu, Cheng Zhong, and Jun Lu. "Advances in the development of power supplies for the Internet of Everything." *InfoMat* (2019).

[14] Bradley, Joseph, Christopher Reberger, Amitabh Dixit, Vishal Gupta, and James Macaulay. "Internet of Everything (IoE): Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector." *Economic Analysis* (2013).

[15] Laney, Doug. "3D data management: Controlling data volume, velocity and variety." *META group research note* 6, no. 70 (2001): 1.

- [16] Media.corporate-ir.net. "Data Management in the Internet of Things (IoT) Era: Common Policy Principles and Data-Handling Framework for Data Security and Privacy". http://media.corporateir.net/media_files/IROLII/9/1_972_11/ARM%20and%20AMD%20Data%20Management%20in%20the%20Internet%20of%20Things.pdf
- [17] Cárdenas, Alvaro A., Pratyusa K. Manadhata, and Sreeranga P. Rajan. "Big data analytics for security." *IEEE Security & Privacy* 11, no. 6 (2013): 74-76.
- [18] Gahi, Youssef, Mouhcine Guennoun, and Hussein T. Mouftah. "Big data analytics: Security and privacy challenges." In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 952-957. IEEE, 2016.
- [19] Garzia, Fabio, and Luigivalerio Sant'Andrea. "The Internet of Everything based integrated security system of the World War One Commemorative Museum of Fogliano Redipuglia in Italy." In *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 1-8. IEEE, 2016.
- [20] Manogaran, Gunasekaran, Chandu Thota, and M. Vijay Kumar. "MetaCloudDataStorage architecture for big data security in cloud computing." *Procedia Computer Science* 87 (2016): 128-133.
- [21] Majeed, Asim, Rehan Bhana, A. Haq, I. Kyaruzi, and M. Williams. "Devising a Secure Architecture of Internet of Everything (IoE) to Avoid the Data Exploitation in Cross Culture Communications." *International Journal of Advanced Computer Science and Applications (IJACSA)* 7, no. 4 (2016).
- [22] Manogaran, Gunasekaran, Chandu Thota, and Daphne Lopez. "Human-computer interaction with big data analytics." In *HCI challenges and privacy preservation in big data security*, pp. 1-22. IGI Global, 2018.
- [23] Yang, Wen-Hau, Shao-Wei Chiu, Chun-Chieh Kuo, Yen-Ting Lin, Yan-Jiun Lai, Hung-Wei Chen, Yu-Sheng Ma et al. "A True Random Number Based Pseudo Hysteresis Controller for Buck DC-DC Converter in High-Security Internet-of-Everything Devices." *IEEE Transactions on Power Electronics* (2019).