Security Challenges and Opportunities related to Big Data in IoT

Prasad Suman Sourav[1]*, Mohanty Anita[2], Mishra Sambit Kumar[3]

[1]Department of MCA, Ajay Binay Institute of Technology, Cuttack
E_mail: prasadsuman800@rediffmail.com
[2]Department of MCA, Ajay Binay Institute of Technology, Cuttack
E_mail: anitamohanty56@gmail.com
[3]Gandhi Institute for Education and Technology, Baniatangi
E_mail: sambitmishra@gietbbsr.com
*Corresponding Author (prasadsuman800@rediffmail.com)

Abstract

The Internet of Things (IoT) is intended for global connectivity among different entities or "things". Its purpose is to provide effective and efficient solutions. Sometimes the security of the devices as well as network is a challenging issue. It is growing at a fast pace with new devices getting connected all the time. The wireless sensor networks are usually good way to integrate the wearable devices in the IoT concept and bring new experiences to the daily life activities. It is also experiencing exponential growth in research and industry, but it still suffers from privacy and security vulnerabilities. Conventional security and privacy approaches tend to be inapplicable for IoT, mainly due to its decentralized topology and the resource-constraints of the majority of its devices. Over the last few years, it has been observed a plethora of Internet of Things (IoT) solutions, products and services, making their way into the industry's market-place. All such solution may definitely capture a large amount of data pertaining to the environment, as well as their users. The objective of the IoT is to learn more and to serve better the system users. Some of these solutions may store the data locally on the devices ('things'), and others may store in the Cloud. The real value of collecting data comes through data processing and aggregation in large-scale where new knowledge can be extracted. However, such procedures can also lead to user privacy issues. This article discusses some of the main challenges of privacy in IoT, and opportunities for research and innovation along with the efforts that address IoT privacy issues.

Keywords: IoT, wireless sensor network, cloud, data aggregation, privacy in IoT.

1. Introduction

The Internet is a powerful global communication medium that provides instantaneous information across geographical, cultural, language, and time spheres. Internet is a network of networks that consists of millions of private, public, academic, research, business, and government networks, of local to global scope linked by a broad array of electronic, wireless and wired networking technologies. The internet brought marvellous changes into our daily life without leaving any field like day to day personal work, health, education, research, humanity, manufacturing, tourism, business, service, government sectors and so on. Thing can be defined as an entity, an idea, a quality perceived, or thought to have its own existence in the world. Things are also often interchanged with the word "Objects". When we are talking about things, they could be both Living Things and Non-Living Things. Things, in this context, can be people, animals, plants, birds, servers, applications, shampoo bottles, cars, steering wheels, coffee machines, electronic devices, park benches or just about any other random item that comes to our mind, even which could be vicinity dust also. Everyday objects include not only electronic devices we encounter but also use daily, and technologically advanced products such as equipment and electronic gadgets, but "things" that we do not do normally think of as electronic at all - such as food, clothing, and furniture, materials, parts, merchandise and specialized items, landmarks, monuments and works of art and all the miscellany of commerce, culture and sophistication . Internet of Things is defined as

ISSN: 2321-8363
Impact Factor: 5.515

"An open and comprehensive network of intelligent objects that have the capacity to auto–organize, share information, data and resources, reacting and acting in face situations and changes in the environment". Internet of Things is one of the last advances in Information and Communication Technologies, providing global connectivity and management of sensors, devices, users and information. Traditionally, the majority of sensor based systems have been closed systems. For example, cars, airplanes and ships have had networked sensor systems that operate largely within that vehicle. However, these systems' capabilities are expanding rapidly. Cars are automatically transmitting maintenance information and airplanes are sending real-time jet engine information to manufacturers. There is or will be even greater cooperation and 2-way control on a wide scale: cars (and aircraft) talking to each other and controlling each other to avoid collisions, humans exchanging data automatically when they meet and this possibly affecting their next actions, and physiological data uploaded to doctors in real-time with real-time feedback from the doctor. These systems require openness to achieve these benefits. However, supporting openness creates many new research problems. All of our current composition techniques, analysis techniques and tools need to be re-thought and developed to account for this openness. New unified communications interfaces will be required to enable efficient information exchange across diverse systems. Of course, openness also causes difficulty with security and privacy, the topics for the next two subsections. Consequently, openness must provide a correct balance between access to functionality and security and privacy. A fundamental problem that is pervasive in the Internet today that must be solved is dealing with security attacks. 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.

Structure of IOT System

The IoT heterogeneous essence, dynamics, intelligence, mobility and undefined perimeters makes it a high-demand technology domain but also makes the IoT vulnerable and risky under security terms. The different platforms where the IoT is available makes it even more difficult for security researchers to find comprehensive solutions to the current security challenges. Therefore, the importance of understanding the foundation and the components of the IoT becomes paramount.
The foundation for global computing, whose goal is to connect everyday life objects to the network using technological platforms, is made up of three components.
(a) Hardware
(b) Middleware
(c) Presentation
Also, the same pattern can be observed when determining the paradigms of the IoT, three factors can be attributed to the IoT environment.
(a) Internet-oriented
(b) Things-oriented
(c) Semantic-oriented
Therefore, the same concept can be applied to the IoT structure.
The IoT architecture is composed of three layers:
(a) The perception layer
(b) The network layer
(c) The application layer
The perception layer gathers environmental data, the network layer, which is composed of wired and wireless systems.

As trillions of things (objects) are connected to the Internet it is necessary to have an adequate architecture that permits easy connectivity, control, communications, and useful applications. How will these objects interact in and across applications? Many times, things or sets of things must be disjoint and protected from other devices. At other times it makes sense to share devices and information. One possible architectural approach for IoT is to borrow from the smartphone world. Smartphones employ an approach where applications are implemented and made available from an app store. This has many advantages including an unbounded development of novel applications that can execute on the smartphones. Various standards and automatic checks are made to ensure that an app can execute on a given platform. For example, the correct version of the underlying OS and the required sensors and actuators can be checked when the app is installed. A similar architectural approach for IoT would also have similar advantages. However, the underlying platform for IoT is much more complicated than for smartphones. Nevertheless, if IoT is based on an underlying sensor and actuator network that acts as a utility similar to electricity and water, then, different IoT applications can be installed on this utility. While each application must solve its own problems, the sharing of a sensing and actuation utility across multiple simultaneously running applications can result in many systems-of-systems interference problems, especially with the actuators. Interferences arise from many issues, but primarily when the cyber depends on assumptions about the environment, the hardware platform, requirements, naming, control and various device semantics. In general relatively simple dependencies have been considered related to numbers and types of parameters, versions of underlying operating systems, and availability of correct underlying hardware. Research is needed to develop a comprehensive approach to specifying, detecting, and resolving dependencies across applications.

2. Review of Literature

N.Hong et al.[1] in their work have focused on security framework. This is provided for IOT by SM2 encryption algorithm and resolving security problems between client and receptor in the information transmission process. It is carried out by using a wide range of IOT based on elliptically graph of ECC and an innovative way to research on the security of IOT.

S. Babar et al.[2] in their work have suggested for safe embedded security framework in IOT. This security framework is divided in to hardware, software and with highly light weight protocols in MAC layer and physical layer.

SB. Vinayaga et al.[3] in their work have focused on hash encryption which is presented with the aim of increasing security that was focusing on a smart home. In fact the main purpose was security in IOT devices that can send messages with more security.

X. Yi Chen et al.[4] in their work have aimed at key technologies associated with IOT such as radio frequency identification (RFID) technology (RFID), electronic technology code identification and Zigbee technologies. In this regard key technologies framework and their usage in digital agriculture have been analyzed.
A.F.Skarmeta et al.[5] in their work have proposed a method to resolve security challenges in IOT. In this method, first of all, the owner exports token related issues to access to the devices and connects to the token with oval ECDSA elliptically algorithm in order to prevent of exporter's security flaws.

L.yuan Zeng et al.[6] in their work have discussed a security framework is presented based on 4G connection. This framework enhances the communication speed of IOT. Through this method 4G client can access to wireless network resources.

P.Xu et al.[7] in their work have focused on system for IOT as well as security risks reduction in useful applications to equip management system and introduced a hybrid encryption algorithm based on DES and DSA encryption algorithms.

According to the NIST definition et al.[8] , new generation of services, based on the concept of the ‘cloud computing’, usually have made their appearance in the last few years with the purpose of providing access to the information and the data from any place at any time, thus restricting or eliminating the need for hardware equipment. The term ‘cloud computation’ is defined as the use of computing logistical resources, as well as the software level, through the use of services transported over the Internet. Nowadays, cloud computing services comprise one of the world’s largest areas of competition between giant companies in the IT sector and software.

Christos Stergiou et al.[9] in their work have defined the mobile Cloud Computing as an integration of cloud computing technology with mobile devices so as to make the mobile devices resourceful in terms of computational power, memory, storage, energy, and context awareness. Mobile Cloud Computing is the outcome of interdisciplinary approaches, combining mobile computing and cloud computing.

D. Huang et al.[10] in their work have discussed in their work about provision of cloud computing storage, services, and applications over the Internet. The technology of Mobile Cloud Computing is the outcome of interdisciplinary approaches, combining mobile computing with cloud computing. Thus, this transdisciplinary domain is also referred as Mobile Cloud Computing .

T. Bhattasali et al.[11] in their work have focused on integration of IoT and Cloud Computing. It has been observed that Cloud Computing may fill some gaps of IoT such the limited storage and applications over internet. Also, IoT can fill some gaps of Cloud Computing such the main issue of limited scope. Based in motivations such those referred previously and the important issue of security in both technologies we can consider some drivers for the integration. The security issue of this integration has a serious problem. When critical IoT applications move towards the Cloud Computing technology, concerns arise due to the lack of trust in the service provider or the knowledge about service level agreements (SLAs) and knowledge about the physical location of data. Consequently, new challenges require specific attention as mentioned in surveys.

Alessio Botta et al.[12] in their work have focused on security related issues lead to sensitive information leakage. Moreover, public key cryptography cannot be applied at all layers due to the computing power constraints imposed by the things. These are examples of topics that are currently under investigation in order to tackle the big challenge of security and privacy in Cloud Computing and IoT integration.
K. Jeffery et al.[13] in their work have discussed the performance and QoS requirements at various levels (i.e. for communication, computation, and storage aspects) related to Cloud Computing and IoT integration’s applications and observed that in some particular scenarios meeting requirements may not be easily achievable.

N. Grozev et al.[14] A big challenge in Cloud Computing and IoT integration is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications.

W. He et al.[15] in their work have discussed that when Cloud Computing and IoT integration are adopted for mission-critical applications, reliability concerns typically arise e.g., in the context of smart mobility, vehicles are often on the move and the vehicular networking and communication is often intermittent or unreliable. When applications are deployed in resource constrained environments a number of challenges related to device failure or not always reachable devices may exist.

Randeep Kaur et al.[16] in their work have focused on secure communication over the network, encryption algorithm. It is a valuable and fundamental tool for the protection of the data. Encryption algorithm converts the data into scrambled form by using ‘‘a key’’ and only the user have the key to decrypt the data. Regarding the researches that have been made, an important encryption technique is the Symmetric key Encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt the data.

3. Features associated with Cloud Computing

Cloud Computing technology has some features which determine its function. These features are analyzed and outlined subsequently. Storage over Internet Storage over Internet can be defined as a technology framework that uses Transmission Control Protocol/Internet Protocol (TCP/IP) networks to link servers and storage devices, and to facilitate storage solution deployment. The Storage over Internet technology is also known as Storage over Internet Protocol (SoIP) technology. With the combination of the best storage and networking industry approaches, SoIP provides high-performance and scalable IP storage solutions.

In enterprise IoT, a single point of entry is feasible. The devices are in contained and trusted environments. Industrial IoT, however, may prove a challenge. IoT devices can potentially disrupt operations based on invalid readings, such as an incorrect temperature. Plus, the sheer volume of wearable data makes industrial and corporate IT systems inefficient. Data analysis is a larger-scale challenge, too. For example, the goal of a wearable device could be to alert medical staff to anomalies in vital signs. In that case, waiting for a centralized batch process to run across a large data center to find irregularities is extremely inefficient. An alternative design is to place anomaly detection closer to the network's edge. Security will be a factor, too, though the extent of that concern will vary. In use cases where IoT devices hold personally identifiable information or that produce video content, device security will be a priority. Security is another advantage to this distributed data-collection-and-analysis because edge data collection devices act as security endpoints. The endpoints can detect security events and kick off a workflow for either isolating wearables or taking corrective action, such as flashing the device's firmware. The edge nodes allow scaling device configuration validation.

3.1. Creating a key

Usually, key production process is used to create a key. First of all, two matrices are used to produce key for encryption. After that the key matrix may be chosen randomly We can choose a place from the state matrix and a key from and produce public key of H by sender in XOR operation. This step of HAN algorithm has been drawn from AEC algorithm. It should be noted that produced key of h is on the basis of hexadecimal. Then public key h is produced. The aim is sending a hidden message from sender to receiver in which private key is just recognized by the receiver and public key by both sender and receiver. So encryption process must have a tight security. It means that the encrypted message by the sender will be sent to the receiver in secret and safety. Therefore NTRU asymmetric encryption is used to enhance the security. When the sent message by the sender is encrypted, it should not be identifiable by any person other than intended recipient.

3.2. Encryption

Assume that a message is sent from the sender to the receiver. This message is in a multinomial called message.

After making a multinomial message, the sender randomly choose a multi nominal like r from the collection like Lr. It should be noted that we can have a message by multi nominal r. So it should not be revealed by the sender.

Encryption = pr * h + message (1)

This message will be transmitted to the receiver as an encryption message with security capability.

3.3. Decryption

When the message is encrypted, in other way receiver tries to open the message by its private key or encrypt the message. For message decryption in HAN algorithm, NTRU algorithm will be used partially. The receiver has both private keys: f and fp. In fact fp is conversed with multinomial of f ,so it can be concluded that it will be $f * fp = 1$ message receiver multiplies a message on the part of private key that is displayed below with the parameter a:

a = f * encryption (2)

a = f * (pr *h + message) (3)

a = f * Pr * h + f * message (4)
To choose a correct parameter, coefficients of the polynominal formula between −q/2 and p/2 are selected.

3.4. Algorithm-1

```
Cipher(long int  input[ ][ ], long int output[ ][ ])
{

long int state[4] [4] ;

copy input into state[ ][ ] AddRoundKey
for (round = 1; round<Nr-1; ++round)
{
SubBytes ShiftRows MixColumns AddRoundKey
}
SubBytes ShiftRows AddRoundKey
copy State[ ][ ] to output[ ][ ]
}
```

Additionally, there is an important encryption technique from the Asymmetric key Encryption. In Asymmetric key encryption, two keys, private and public keys, are used. Public key is used for encryption and private key is used for decryption. This algorithm is the most commonly used encryption and used for private and public key generation and encryption. As compared to other algorithm, it also uses a key generator that provides two large primes to proceed to the encryption mode. Generally two types of keys for decryption and encryption are used i.e. the public key and the secret key.

3.5. Algorithm -2

```
Key Generation: KeyGen(p, q)
Input: Two large primes — p, q
Compute n = p . q
 ϕ(n) = (p − 1)(q − 1)
Choose e such that gcd(e, ϕ(n)) = 1
Determine d such that e . d ≡ 1 mod ϕ(n)
Key: public key = (e, n) secret key = (d, n)
 Encryption: c = me mod n
```

where c is the cipher text and m is the plain text. The algorithm has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts.

4. Experimental Analysis

Considering the benefits of the security models and algorithms of Internet of Things and Cloud Computing technologies we can observe that we can have a beneficial use of integration those two technologies. Instead of the wide use of IoT we can take advantage that Cloud Computing security through the AES algorithm performs consistently well in both hardware and software platforms under a wide range of environments. This use could be possible for all type of platforms and DSPs. Furthermore, the new integrated technology could has good potential for benefiting from instruction-level parallelism and will support any type of block sizes and key sizes that are multiples of 32 and used both of IoT and Cloud Computing.

5. Discussion and Future Direction

Considering the rich blend of various technologies involved in IoT, there is a need of lot of research required to stream line the efficient and optimized working of IoT based application. We have tried to enlist some open challenges based on elements of IoT. These challenges include privacy, standardization, data integrity, QoS support, and data analytics. For IoT to be accepted as an efficient technology for various applications efforts are required to be streamlined in development of scalable and suitable service delivery platforms that permits multiple services to coexist.

6. Conclusion

Accumulating data through IoT solutions and analyse them in large-scale will have a significant value to offer for both individual users and businesses. Further, it can also make significant impact towards society in general through increase productivity and reducing wastage. However, existing technologies and regulations are not sufficient to support privacy guaranteed data management life cycle. The Cloud Computing technology offers many possibilities, but also places several limitations as well. Cloud Computing refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. In this paper, we present a survey of Internet of Things Technology, with an explanation of its operation and use. Cloud Computing refers to an infrastructure where both data storage and data processing happen outside of the mobile device. Also, the Internet of Things is a new technology which is growing rapidly in the field of telecommunications, and especially in the modern field of wireless telecommunications. The main goal of the interaction and cooperation between things and objects sent through the wireless networks is to fulfil the objective set to them as a combined entity. In addition, based on the technology of wireless networks, both the technologies of Cloud Computing and Internet of Things develop rapidly. In this paper, it is primarily focused on the security issues of both technologies. Specifically, the two aforementioned technologies (i.e. Cloud Computing and IoT) may be combined order to examine the common features, and in order to discover the benefits of their integration.

References

[1] N.Hong, Z.Xuefeng, "A Security Framework for internet of thingsbased on SM2 cipher algorithm", Fifth International Conference on Computer Science and Network Technology, Shiyang, Hubia, China, IEEE, p.p13-16, 2013.

[2] S. Babar, A.Stango, N.Prasad, J.Sen, R.Prasad, "Proposed embedded seurity framework for internet of things", 2nd International Conference on Information Theory and Aerospace & Elentronic Systems Technology, Chennai, IEEE, p.p.1-5, 2011.

[3] SB. Vinayaga, M. Ramnath, M. Prasanth, and V. Sundaram. "Encryption and hash based security in Internet of Things." In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference, Chennai, p.p. 1-6. IEEE, 2015.

[4] X. Yi Chen, Zh.Gang Jin , "Research on Key Technology and Applications for Internet of Things", Physics Procedia, vol33, Science Direct, p.p 561-566, 2012.

[5] A.F.Skarmeta, J.L. Hernandez, M.V. Moreno" A decentralized approach for Security and Privacy challenges in the Internet of Things", IEEE Word Forum on Internet of Things (WF-IOT), Seoul, IEEE, p.p.67-72, 2014.

[6] L.yuan Zeng, "A Security Framework for Internet of Things Based on 4G communication,-2nd International Conference On computer Science And Network Technology, Chanchun, China, IEEE, p.p1715-1718, 2012.

[7] P.Xu, Li .Min, and He. Yu-Jie. "A hybrid encryption algorithm in the application of equipment information management based on Internet of things." In 3rd International Conference on Multimedia Technology (ICMT-13). Atlantis Press, 2013.

[8] The NIST definition of cloud computing, National Institute of Standards and Technology (Accessed 24 July 2015).

[9] Christos Stergiou, Kostas E. Psannis, Recent advances delivered by mobile cloud computing and Internet of things for big data applications: a survey, Int. J. Netw. Manag. (2016) 1–12. 11/03/.

[10] D. Huang, Mobile cloud computing, IEEE COMSOC Multimedia Commun. Tech. Comm. (MMTC) E-Lett. 6 (10) (2011) 27–31.

[11] T. Bhattasali, R. Chaki, N. Chaki, Secure and trusted cloud of things, in: India Conference (INDICON), 2013 Annual IEEE, IEEE, 2013, pp. 1–6.

[12] Alessio Botta, et al., Integration of cloud computing and Internet of things: a survey, J. Future Gener. Comput. Syst. (2015) 1–54. 14/09/

[13] K. Jeffery, Keynote: CLOUDs: A large virtualisation of small things, in: The 2nd International Conference on Future Internet of Things and Cloud, FiCloud2014, 2014.

[14] N. Grozev, R. Buyya, Inter-cloud architectures and application brokering: taxonomy and survey, Softw. - Pract. Exp. 44 (3) (2014) 369–390.

[15] W. He, G. Yan, L.D. Xu, Developing vehicular data cloud services in the iot environment, IEEE Trans. Ind. Inf. 10 (2) (2014) 1587–1595.

[16] Randeep Kaur, Supiya Kinger, Analysis of security algorithms in cloud computing, Int. J. Appl. Innov. Eng. Manag. (IJAIEM) 3 (3) (2014) 171–176. 1 3.

A Brief Author Biography

Prof. Suman Sourav Prasad – Prof. Suman Sourav Prasad is presently associated with the Department of MCA, Ajay Binay Institute of Technology, Cuttack and having more than 9 Years of teaching experience.
Prof. Anita Mohanty - Prof. Anita Mohanty is presently associated with the Department of MCA, Ajay Binay Institute of Technology, Cuttack and having more than 9 Years of teaching experience.
Dr. Sambit Kumar Mishra – Dr. Sambit Kumar Mishra is having 20 Years of experience in teaching in different Engineering Institutions in India. He is member of different professional bodies, i.e. ISTE, IAE, CSTA, IACSIT. He is also member of editorial board of some peer reviewed and indexed Journals.