International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

July-2018 Volume 5, Issue-4

Email: editor@ijermt.org www.ijermt.org

DATA SECURITY ASPECTS OF CLOUD COMPUTING USING INTERNET OF THINGS

Venkatesh H
Assistant Professor
Department of MCA
Acharya Institute of Technology
Bangalore

Dr.G.N.K.Suresh Babu
Professor
Department of MCA
Acharya Institute of Technology
Bangalore

ABSTRACT

Now a day's every where you can hear the terminology IoT. Since IoT is used in every place, the author proposes the data security concepts used in IoT and Cloud Computing. For the past one decade everybody is using cloud computing techniques to preserve the data. But the users are very much worried about the security related issues. Cloud computing and Internet of Things, two different technologies, are both already part of our life. Their massive adoption and use is expected to increase further, making them important components of the Future Internet. A novel paradigm where Cloud and IoT are merged together is foreseen as disruptive and an enabler of a large number of application scenarios. In this paper we focus our attention on the integration of Cloud and IoT, security challenges, encryption algorithms used in security concerns.

KEYWORDS: Cloud Computing, IoT, Security, Encryption, Decryption

INTRODUCTION

The Internet of Things (IoT) is a network of networks, in which, typically, a massive number of objects/things/sensors/devices are connected through the information and communications infrastructure to provide value-added services. The IoT allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using Any path/network and Any service. It is predicted that, by 2020, there will be 50 to 100 billion devices connected to the cloud. These devices will generate Big Data that needs to be analyses for knowledge extraction. The collection and analysis of data in the IoT applications has many objectives. For example in case of customer sentiment analysis, such data can be used for improving personalized recommendations hence leading to better customer experiences. On other hand in case of smart cities, governments and city councils can use the knowledge extracted to make strategic decisions and future city plans. However, the data collected by smart IoT devices may contain very sensitive personal data based on type of application and data sources. Therefore, such data must be managed carefully to avoid any user privacy violations. Consequently, in the subsequent text, we briefly discuss the importance on addressing IoT privacy challenges. Users are the people or the consumers who are using the product or the service. As IoT and Cloud becomes more integrated into our daily lives, the concerns surrounding its security aspects are growing at an alarming rate. The research community has already identified a number of security challenges in many areas of IoT. In terms of security, a prominent concern is Denial of Service (DoS) attacks in embedded devices, since such devices lack the resources to withstand repeated requests from malicious attackers. Man-In-The-Middle attacks are another acknowledged issue that takes advantage of either weak encryption algorithms of embedded devices or weak authentication mechanisms among the systems. Security researchers have found common vulnerabilities in many IoT devices that could have been prevented if simple security measures were taken into consideration during the development cycle. The practice of implementing security analysis during development ensures that the final product will meet specific security standards. The security standards, in turn, will ensure its robustness when the product is actively deployed in real life scenarios. The method of including secure practices early in the development cycle is advocated by the field of requirements engineering. Requirements engineering analysis is applied by identifying the stakeholders' requirements in the development cycle to produce security requirements. IoT systems allow the network integration of a variety of different devices. Devices such as personal computers, mobile phones, and printers can be considered traditional devices since they have been used in networking scenarios in the past. Traditional devices are used to access the Web, share files or host websites. Devices such as light bulbs, cars or heart monitors are only now gaining networking capabilities and as a result they have significant security flaws. IoT is unique in the sense that it brings together old and robust technology with new and untested technology. The pairing of mature technology with immature technology naturally results in security issues. Given the unique challenges faced by IoT systems, our main question in this paper is how do we provide security requirements in IoT systems? We are trying to give some optimized solution to provide more security to data available in Cloud database.

INTEGRATION OF IOT AND CLOUD COMPUTING

The two worlds of Cloud and IoT have seen an independent evolution. However, plenty of common advantage is the result of their integration have been identified in literature, predict the future. On the one hand, the Internet of things can benefit from cloud almost unlimited capacity and resources to make up for the technical constraints. Specifically, cloud computing can provide an effective solution to realize management of Internet services and composition and use of things or data applications. Cloud computing can benefit from the Internet of things, on the other hand, by extending its scope to deal with things in the real world more distributed and dynamic way, and to provide new services on a large number of real life scenarios. Essentially, the Cloud acts as intermediate layer between the things and the applications, where it hides all the complexity and the functionalities necessary to implement the latter. We summarize the problem and gain the advantage when using Cloud-IoT paradigm. IoT involves by definition a large amount of information sources. It produces a large amount of unstructured or semi-structured data of the three major characteristics of the data: volume, velocity and variety. Hence this means that the collection, acquisition, processing and visualization, archive, share, search large amounts of data. Provide almost unlimited and on-demand storage capacity, low cost, cloud is the most convenient and cost effective solutions to deal with the data generated by the Internet of things. This integration realizes a new convergence scenario, where new opportunities arise for data aggregation, integration, and sharing with third parties. Once to the cloud, data can be in a uniform way through a standard API, can use the top security protection, direct access from anywhere, and visualization. IoT equipment processing resources are not allowed to field data processing. Collected data are usually aggregated and transmitted to a more powerful node processing is feasible, but not an appropriate scalability challenges to achieve infrastructure. Cloud and its on-demand model of infinite capacity allows appropriate content, make the Internet of things to deal with unprecedented demand complex analysis. Data-driven decision making and prediction algorithms would be possible at low cost and would provide increasing revenues and reduced risks. One of the requirements of the Internet of things is to make the IP access devices communicate through dedicated hardware, and support the communication can be very expensive. The integration with the Cloud solves most of these problems also providing additional features such as ease-of-access, ease-of-use, and reduced deployment costs. Using Cloud-IoT paradigm to make intelligent services and applications of new scene based on the expansion of the cloud by things: (1) Sensing as a Service, (2) Sensing and Actuation as a Service, (3) Sensor Event as a Service, (4) Database as a Service, (5) Ethernet as a Service, (6) Identity and Policy Management as a Service, (7) Video Surveillance.

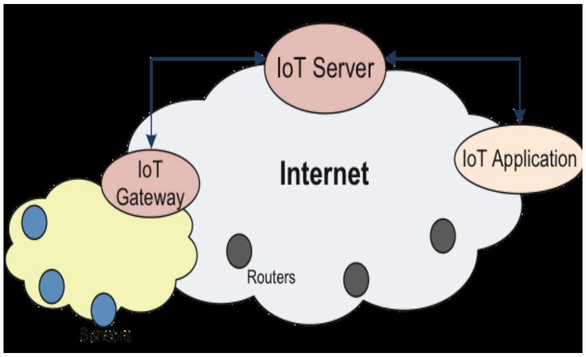


Fig.1 Represents the Integration of Cloud and IoT

SECURITY CHALLENGES

IoT is closely related to communication and information technology, it is justified to consider security and privacy challenges already known in information security and examine how these concerns are transferred to the current and future state of the IoT. At the first glance, the similarities seem so many and the differences so subtle that one may be deceived that security and privacy concerns in the IoT are the same challenges as those known in the information security and the same measures are sufficient to face these challenges. However, some characteristics make the security and privacy challenges in the IoT so distinct that a more careful investigation of the subject is required. The number of connected devices to the Internet has already surpassed the number of humans on the planet. This number continues to increase dramatically and is predicted to be between 26 billion and 50 billion by 2020. Several factors facilitate this development, among others the introduction of Internet Protocol version 6, which allows that every device has a unique IP-address, leading to much easier communication between devices. However, the security and privacy issue for the IoT does not increase linearly with the number of Internet-connected devices, but grows in a much faster rate. This is due to the fact that, even assuming everything is the same, the number of communication channels in a network increases faster than the number of nodes. Computer networks are often heterogeneous in nature, which can induce security challenges. The IoT is expected to be far more heterogeneous than current computer networks, integrating a multitude of various devices from different manufacturers, software platforms and communication protocols. While servers and workstations are protected in server rooms and offices, and personal computers, notebooks and handheld devices are protected by the owner’s presence, in an IoT setting, sensors and other devices are located everywhere, and exposed to theft, malicious damage and intrusion. Vicious attackers can use the increased physical accessibility of devices to find more vulnerability in IoT systems. IoT devices are usually battery-driven, fault-prone systems and generally have lower processing power and memory and used to not fulfill the requirements for implementing appropriate security and anonymization services, which require sufficient amount of processing and memory resources. Although in recent years, this has been less of an issue, many constructions still have a lack of security functions built in. The IoT is expected to be ubiquitous and pervasive. Connected devices are worn, carried or seamlessly embedded in the world around us. They may collect data, communicate and interact with other devices, without our permission or even our knowledge, simply because we do not own them (e.g. video surveillance cameras in a shopping mall, or connected vehicles that we travel in as a passenger). As the number of connected things increases, the amount of gathered and accumulated information about us in different databases increases continuously. Although sensitive data might be removed or protected by anonymization when the data is disseminated, an unpredictable combination of seemingly non-sensitive data from different sources can create a unique identifier resulting in privacy breaches. While until recent years, cyber-attacks have mainly threatened information systems, computer networks, and personal computers, the IoT will escalate security risks to a different level. In the IoT era, as actuators and control systems will be interconnected with other systems, attackers may be able to directly target connected devices and achieve physical destruction of the equipment and infrastructures, such as self-driving cars, smart houses, electric grids, oilfields, transportation systems, and nuclear plants. Stuxnet was the first malicious code that attacked the control system of a nuclear facility; however, with the explosion of the IoT, it will not be the last one that leaves the cyber realm to cause physical destruction. The IoT inherently has a dynamic characteristic. Pervasive devices such as wearable’s can join and leave the IoT network (e.g. smart homes) anytime. This, in combination with multiprotocol communication characteristics, makes the traditional information security measures insufficient for the IoT.

TYPES OF ATTACKS

The IoT is facing various types of attacks including active attacks and passive attacks that may easily disturb the functionality and abolish the benefits of its services. In a passive attack, an intruder just senses the node or may steal the information but it never attacks physically. However, the active attacks disturb the performance physically. These active attacks are classified into two further categories that are internal attacks and external attacks. Such vulnerable attacks can prevent the devices to communicate smartly. Hence the security constraints must be applied to prevent devices from malicious attacks. Different types of attack, nature/behavior of attack and threat level of attacks are discussed in this section. Different levels of attacks are categorized into four types according to their behavior and propose possible solutions to threats/attacks.

1) Low-level attack: If an attacker tries to attack a network and his attack is not successful.

2) Medium-level attack: If an attacker/intruder or an eavesdropper is just listening to the medium but don't alter the integrity of data.

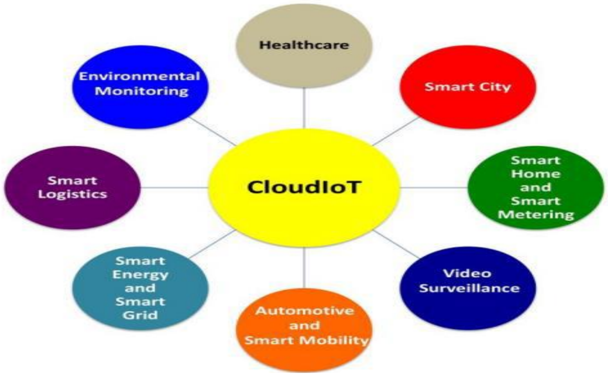
3) High-level attack: If an attack is carried on a network and it alters the integrity of data or modifies the data.

4) Extremely High-level attack: If an intruder/attacker attacks on a network by gaining unauthorized access and performing an illegal operation, making the network unavailable, sending bulk messages, or jamming network.

APPLICATIONS OF CLOUD AND IOT INTEGRATION

The two worlds of Cloud and IoT have seen an independent evolution. However, plenty of common advantage is the result of their integration have been identified in literature, predict the future. On the one hand, the Internet of things can benefit from cloud almost unlimited capacity and resources to make up for the technical constraints. Specifically, cloud computing can provide an effective solution to realize management of Internet services and composition and use of things or data applications. Cloud computing can benefit from the Internet of things, on the other hand, by extending its scope to deal with things in the real world more distributed and dynamic way, and to provide new services on a large number of real life scenarios.

Fig.2 represents the Applications of Cloud and IoT.

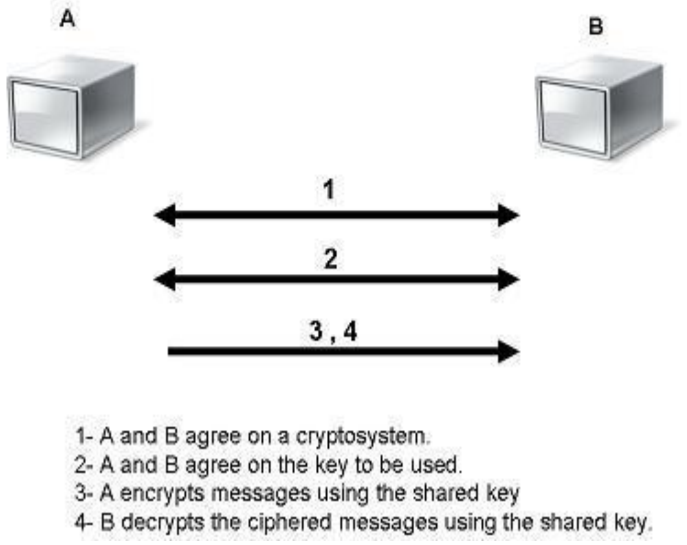

Healthcare
Environmental Monitoring
Smart City
Smart Logistics
CloudIoT
Smart Home and Smart Metering
Smart Energy and Smart Grid
Video Surveillance
Automotive and Smart Mobility

SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data. These two categories are: Symmetric and Asymmetric encryption techniques

SYMMETRIC ENCRYPTION

In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. Fig. 3 shows the process of symmetric cryptography. Node A and B first agree on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node a starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.



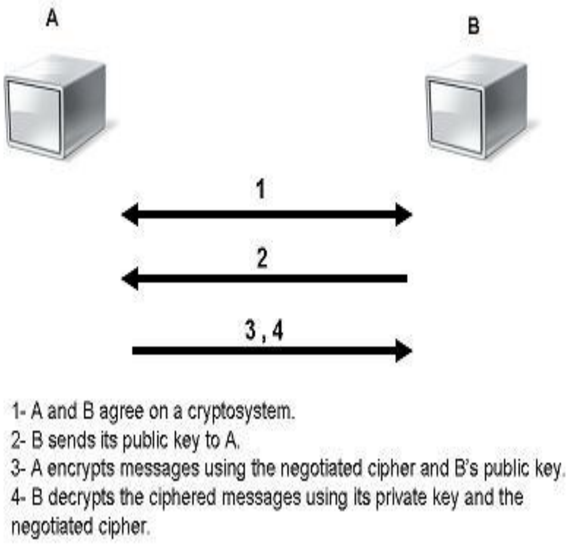
1- A and B agree on a cryptosystem.
2- A and B agree on the key to be used.
3- A encrypts messages using the shared key
4- B decrypts the ciphered messages using the shared key.

Fig.3 Symmetric Encryption

The main concern behind symmetric encryption is how to share the secret key securely between the two peers. If the key gets known for any reason, the whole system collapses. The key management for this type of encryption is troublesome, especially if a unique secret key is used for each peer-to-peer connection, then the total number of secret keys to be saved and managed for n-nodes will be n(n-1)/2.

ASYMMETRIC ENCRYPTION

Asymmetric encryption is the other type of encryption where two keys are used. To explain more, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is known to the public, and private key which is known only to the user. Figure 4 below illustrates the use of the two keys between node A and node B. After agreeing on the type of encryption to be used in the connection, node B sends its public key to node A. Node A uses the received public key to encrypt its messages. Then when the encrypted messages arrive, node B uses its private key to decrypt them.



1- A and B agree on a cryptosystem.
2- B sends its public key to A.
3- A encrypts messages using the negotiated cipher and B's public key.
4- B decrypts the ciphered messages using its private key and the negotiated cipher.

Fig.4 Asymmetric Encryption

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key, symmetric encryption is then used to transfer data between sender and receiver.

DIFFERENT TYPES OF ENCRYPTION ALGORITHMS

This section intends to give the readers the necessary background to understand the key differences between the compared algorithms.

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974 . Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cipher.

3DES: As an enhancement of DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Rijndael (pronounced Rain Doll) algorithm was selected in 1997 after a competition to select the best encryption standard. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers.

Blowfish: It is one of the most common public domain encryption algorithms provided by Bruce Schneier - one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. Blowfish is a variable length key, 64-bit block cipher. The Blowfish algorithm was first introduced in 1993.This algorithm can be optimized in hardware applications though it's mostly used in software applications. Though it suffers from weak keys problem, no attack is known to be successful against.

ADVANTAGES OF DATA ENCRYPTION

- Encryption Provides Security for Data at All Times
  Generally, data is most vulnerable when it is being moved from one location to another. Encryption works during data transport or at rest, making it an ideal solution no matter where data is stored or how it is used. Encryption should be standard for all data stored at all times, regardless of whether or not it is deemed “important”.
- Encrypted Data Maintains Integrity
  Hackers don’t just steal information, they also can benefit from altering data to commit fraud. While it is possible for skilled individuals to alter encrypted data, recipients of the data will be able to detect the corruption, which allows for a quick response to the cyber-attack.
- Encryption Protects Privacy
  Encryption is used to protect sensitive data, including personal information for individuals. This helps to ensure anonymity and privacy, reducing opportunities for surveillance by both criminals and government agencies. Encryption technology is so powerful that some governments are attempting to put limits on the effectiveness of encryption—which does not ensure privacy for companies or individuals.
- Encryption is Part of Compliance

Many industries have strict compliance requirements to help protect those whose personal information is stored by organizations. HIPAA, FIPS, and other regulations rely on security methods such as encryption to protect data, and businesses can use encryption to achieve comprehensive security.

- Encryption Protects Data across Devices
  Multiple (and mobile) devices are a big part of our lives, and transferring data from device to device is a risky proposition. Encryption technology can help protect store data across all devices, even during transfer. Additional security measures like advanced authentication help deter unauthorized users.

THE FUTURE OF ENCRYPTION

As hackers continue to become more savvy and sophisticated, encryption technology must evolve as well. Security professionals are working on a few different exciting technological advances in the encryption field, including Elliptic Curve Cryptography (ECC), homomorphic encryption, and quantum computation. ECC is a method of cryptography that isn’t so much an improvement of the encryption method itself, but a method that allows encryption and decryption to take place much faster, without any loss of data security. Homomorphic encryption would be a system allowing calculations on encrypted data without decrypting it. This method would allow encryption across cloud systems, and ensure greater privacy for users. As an example, a financial institution could make assessments for individuals without revealing personal information. Quantum computation and key distribution generate random sequences that result in codes that are virtually unbreakable. Attempted interceptions of the data would be detectable by both the sender and recipient, allowing for a quick response to any hacking attempts. Quantum computation can store data in multiple states, allowing for incredibly fast calculations.

CONCLUSION

The main focus of this paper is security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim’s knowledge of being infected. Considering the importance of security in IoT applications, it is really important to install security mechanism in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networks. Security is the most challenging issue in cloud and IoT technology. In this paper we have discussed various encryption algorithms to overcome this security issue, deals with advantages and disadvantages of these algorithms. Here we conclude that homomorphism algorithm is the most suitable algorithm in cloud computing environment to secure their valuable data in an open network. The ability of homomorphic algorithm to perform operations on encrypted data enables high security than other algorithms such as RSA, DES, and AES. Future work is to implement hardware or software technique with homomorphic algorithm to provide protection on cloud from any type of security attack. Considering all the above encryption algorithms, we are proposing to implement the Blowfish algorithm to maintain secured data in cloud computing.

REFERENCES

1. S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed security model and threat taxonomy for the internet of things (iot),” in International Conference on Network Security and Applications. Springer, 2010, pp. 420–429.
2. Y. H. Hwang, “Iot security & privacy: threats and challenges,” in Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM, 2015, pp. 1–1.
3. M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the internet of things,” in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.
4. L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
5. [TropSoft] "DES Overview", [Explains how DES works in details, features and weaknesses]
6. [Bruce1996] BRUCE SCHNEIER, "Applied Cryptography" , John Wiley & Sons, Inc 1996
7. J. Daemen, and V. Rijmen, \Rijndael: The advanced encryption standard," *Dr. Dobb's Journal*, pp. 137-139, Mar. 2001.

8. P. Ding, \Central manager: A solution to avoid de-nial of service attacks for wreless LANs," *International Journal of Network Security*, vol. 4, no. 1, pp. 35-44, 2007.
9. DiaasalamaAbdElminaam, Hatem Mohamad Abdual Kader, Mohly Mohamed Hadhoud, ―Evalution the Performance of Symmetric Encryption Algorithms‖ , international journal of network security vol.10,No.3,pp,216-222,May 2010.
10. N.K. Pareek., Vinod Patida., K.K. Sud.: Image encryption using chaotic logistic map. Image and Vision Computing 24, PP. 926–934 (2006).
11. Tiwaria S.P., Bansal K.K (2018), “Nature inspired algorithms on Industrial applications: A survey ” International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 pp. 4282-4290
12. Goodwin, J., Wilson, P. R., ―Advanced Encryption Standard (AES) Implementation with Increased DPA Resistance & low overhead‖ , IEEE International Symposium on Circuits and Systems, 2008. ISCAS 2008.
13. Li, H., Li., J., ―A New Compact Dual Core Architecture for AES Encryption & Decryption‖ , Canadian Journal of Electrical and Computer Engineering, 2008.
14. Ashton, K. That ‘Internet of Things’ Thing. RFID J. 2009, 22, 97–114.
15. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A Survey. Comput. Netw. 2010, 54, 2787–2805.
16. Named Data Networking. Available online: http://named-data.net/ (accessed on 19 June 2017).
17. Nebula Future Internet Architecture Project. Available online: http://nebula-fia.org (accessed on 19 June 2017).
18. J. Infanta and M. Hemalatha, “Enhancing Building Security with RFID and ZigBee,” Vol. 5, No. 1, pp. 265–272, 2013.
19. H. Yelin, X. Guo, and J. Zhu, “Research on RFIDbased Monitoring Platform for Wireless Sensor Networks,” vol. 1, no. 8051, pp. 1909–1912, 2011.
20. K. Ahmed and M. Gregory, “Integrating Wireless Sensor Networks with Cloud Computing,” 2011 Seventh Int. Conf. Mob. Ad-hoc Sens. Networks, pp. 364–366, Dec. 2011.
21. Hashizume K., Rosado D. G., Fernandez- Medina E. and Fernandez E. B.“An analysis of security issues for cloud computing”. Journal of Internet Services and Applications, 2013, 4(1), pp.1-13.