IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 28-32

A Novel Approach of Security Concern of IoT with Cloud Based Services

Prakash Kumar Patra[1], Tarun Kumar Behera[2]
[1](Electrical Engineering, GIET Bhubaneswar, India)
[2](Computer Science and Engineering, GIET Bhubaneswar, India)

Abstract: *Internet of Things use of standard Internet protocols for the human-to-thing or thing-to-thing communication in embedded networks. Cloud based services are high demand technology which makes an infrastructure where both data storage and data processing operate outside of the device i.e. irrespective of devices like smart phone, gadgets and traditional computer . Current market based situation Internet of Things. Internet of Things is growing rapidly in the field of telecommunications and wireless communications. So cooperation between wireless network like wifi, traditional network and different object need attention of security issue. The Internet of Things (IoT) is ''the network of physical existed objects, mobile devices, desktops ,vehicles and other items which are deals with either software, sensors with network connectivity, permitting these objects to gathering and interchange data make crucial in operation point of view.*
We provides an overview of the situation in IoT with a special emphasis on regulatory challenges that will emerge in the upcoming years in this area.An approaches of AES key which helps to resolve security issues in IoT and Cloud computing integration

I. Introduction

The Internet of Things (hereinafter: IoT) is a concept allowing for the networking of different things and objects from everyday life and their everyday communication over the Internet, without human interaction, with a view to improving the conditions and way of life. The term Internet of Things was employed for the first time by Kevin Ashton, the director of MIT's Auto-ID centre, in 1999 in his presentation for Procter & Gamble, but it took a few years for the term to enter into more frequent use. IoT was formally introduced as a term in 2006 by the International Telecommunication Union (ITU) in its Internet report . IoT is the revolution of the future as per current trends. According to Cisco Systems by 2020, the Internet consist of over 100 billion connected things including mobile gadgets, sensors, actuators, GPS devices, wifi devices, and all smart things that participate with combination. IoT have an impact on several aspects of the everyday-life as well as behavior of users. Internet of Things, as a private user could exist, would be visible in both domestic and working fields. Similarly business consequences like transports, intelligent logistics goods, automation and industrial manufacturing, and business/process management. With the development of IoT technology, every device in our surroundings will be able to communicate with another device and send information to that device or control it, depending on the collected information.

The potential for economic scenario and application of IoT was on reviewing Economist magazine as a result of a survey conducted in June 2013 when opinions of 789 business experts were collected to define the business class index of IoT. Results have shown that three quarters of companies have been actively researching or using IoT, and 96% stated that they would start using IoT in similar form or another form in the following 3 years. According to assessment of potential growth of the IoT in market next few years varies depending on number of devices used with their relative connectivity and on the growth of the market. Therefore, for example, Gartner estimated that 30 billion devices will be connected to the Internet in 2020 with a single IP address which would bring additional USD 1.9 billion (1012) for the world economy [1]. At the same time, Cisco and Ericsson forecast that this number would increase to 50 billion [2] [3] objects connected to the Internet, which will result in earnings for the world economy amounting to USD 14 billion. For comparison scinario, this amount exceeds total GDP of 17 EU Member States in 2011 [4]. IDC also envisaged in October 2013 that there will be a total of 212 billion "objects" by 2020, which would equal to EUR 8.9 billion per year with the annual growth rate of 7.9% [5]. Another aspect Internet of Things (IoT) is a widely used expression, as a fuzzy one, mostly due to the large amount of concepts it encompasses. The relatedness of IoT include concepts such as Wireless Sensor Networks, Machine-to-Machine communications and Low power Wireless Personal Area Networks (LoWPAN),or technologies such as Radio-Frequency Identification (RFID).In above mention materializes a vision of a future Internet where any object possessing computing and sensorial capabilities is able to communicate with other devices using Internet communication protocols, in the context of sensing applications. Which expected to employ a large amount of sensing and actuating devices, and in consequence its cost will be an important factor. On the other hand, cost restrictions with constraints in terms of the resources available in

sensing platforms, such as memory and computational power, and unattended employment of many devices will also require both batteries for energy storage. Overall, such factors motivate the design and adoption of communications and security mechanisms optimized for constrained sensing platforms, capable of providing its functionalities efficiently and reliably.

Throughout above survey basic focus on security for communications on the IoT, analyzing both the solutions available in the context of the various IoT communication technologies, as well as those proposed in the literature. We also identify and discuss the open challenges and possible strategies for future research work in the area. As our focus is on standardized communication protocols for the IoT, our discussion is guided by the protocol stack enabled by the various IoT communication protocols available or currently being designed, and we also discuss cross-layer mechanisms and approaches whenever applicable. This paper provides an overview of the situation in IoT with a special emphasis on regulatory challenges that will emerge in the upcoming years in this area.

II. Relation in Research Review with Literature

This Basic review of previous literature which has been forecast in the field of mobile computing, cloud computing and Internet of Things, with their combine effort on technology. The Internet of Things is a type of network of some physical objects or things which, embedded with software, electronics, sensors and connectivity that enables them, achieves greater value and service by exchanging data with manufacturers, operators and some other connected devices [5].So, the intensive computations and the mass storage, which are supported by clouds with respect to mobile communication, are often inefficient. Now Mobile Cloud Computing integrates multiple technologies for maximizing capacity and performance of the existing infrastructure [7].

Different security risks that pose a threat to the cloud is mentioned was given a survey more specific to the different security issues relate to service delivery models of a cloud computing system. So a solution to trustworthy cloud computing environment is important because momentum of evolving paradigm is very high. It is also important cloud computing capacities for provision and support of ubiquitous connectivity and real-time applications and services. Another aspect presentation of a framework for data procured from highly distributed, heterogeneous, decentralized, real and virtual devices (both sensors, actuators, smart devices) that need to be automatically managed, analyzed and controlled by distributed cloud-based services. Researchers realize that the full sharing, free circulation, on-demand use, and optimal allocation of various manufacturing resources and capabilities, the applications of the technologies of IoT and Cloud Computing in manufacturing are investigated[8]. Moreover, data generated needs to be managed according to its requirements, in order to create more valuable services. For the previous purpose, integration of IoTs with cloud computing is becoming very important. This new paradigm is termed as Cloud of Things (CoTs) and it is presented in [9]. So integration components: Cloud platforms, Cloud infrastructures, mobile computing and IoT Middleware proposals and data analytics techniques are surveyed as well as different challenges and open research issues are marked out.

III. Internet of Things and Security

Internet of Things is a network of devices that transmit, share, and use data from the physical environment to provide services to individuals, corporations, and society. They function either individually or in connection with other but have unique IDs (identifiers). The applications in health, transport, environment, energy or types of devices are important. So in Business scenario opportunities applicable in streaming data with need enhance existing services. These are listed below.

(a) Smart solution in the bucket of transport
(b) Smart power grids incorporating more renewable.
(c) Remote monitoring of patients.
(d) Sensors in homes and airports.
(e) Engine monitoring sensors that detect & predict maintenance issues.

IoT security[15] is the area of prime concerned with safeguarding connected devices and networks in the Internet of things. There are increasing prevalence of objects and entities that are known, as context of things need provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids home and building automation, vehicle to vehicle communication. So networking appliances and other objects is relatively new, security has not always been considered in product design. Buyers often fail to change the default passwords on smart devices—or if they do change them, fail to select sufficiently strong passwords. To improve security, an IoT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should then be monitored to identify potential anomalous traffic, and action should be taken if there is a problem [10, 11].

IV. Security Spec

Encryption algorithm always plays an important role in secure communication over the network. Encryption algorithm converts the data into arbitrary form by using ‘‘a key’’ and only the user have the key to decrypt the data. So, an important encryption technique is the Symmetric key Encryption which use only one key is used to encrypt and decrypt the data. The AES algorithm block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

AES algorithm used in this work as original key consists of the number of bytes in any case, which are represented as a 8×8 matrix.

```
Cipher(byte[] input, byte[] output)
{
byte[8,8] State;
copy input[ ] into State[ ] AddRoundKey
for (round = 1; round <Nr-1; ++round)
{
SubBytes ShiftRows MixColumns AddRoundKey
}
SubBytes ShiftRows AddRoundKey
copy State[] to output[]
}
```

These following points makes us promptly select AES mechanism.

• AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP’s.
• Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
• This algorithm has slightly slow key setup time but good key agility.
• It requires less memory for implementation, making it suitable for restricted-space environments.
• The structure has fair potential for benefiting from instruction level parallelism.
• There are no serious weak keys in AES.
• It supports any block sizes and key sizes that are multiples of 64 (greater than 256-bits).
• No differential and linear cryptanalysis attacks have been yet proved on AES.

V. Security Issues in IoT and Cloud Computing Integration

Processing, storage and communication could be a benefit for the Internet of Things technology. But virtually unlimited capabilities and resources of Cloud Computing and technological constrains related to processing, storage and communication to real world. Distributed in dynamic manner with delivering new services is vital in Cloud. Through the integration of IoT and Cloud Computing could be observed that Cloud Computing can fill some gaps of IoT such the limited storage and applications over internet. Also, IoT can fill some gaps of Cloud Computing. Multi-tenancy could also compromise security and 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 [12–14].

Proposed Security Model Algorithm

AES algorithm provides better secure in Cloud Computing, mobile computing and give benefits in security issues in IoT .we propose a new method that uses those benefits in order to improve the security and privacy issues in the integration of technologies.

Key Generation: KeyGen(p, q)
Input: Two large primes - p, q
Compute n = p . q
buffer(n) = (p □ 1)(q □ 1)
Choose e such that gcd(e, buffer(n)) = 1
Now buffer[x] = 0xff is combined. With the use of this new type of RSA algorithm in the encryption process,

Now 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.

Also, as a proposal of this work could be the following part of algorithm which uses the original key consists of 256 bits/64 bytes which are represented as a 8×8 matrix. With the use of this part of AES algorithm we can draw that data which encrypted with 256 bit (or 32 bytes) can be have better encrypted as an 8 × 8 matrix in order of providing a better use of communication privacy but slight slower.

```
Cipher(byte[] input, byte[] output)
{
byte[8,8] State;
copy input[] into State[] AddRoundKey
for (i = 4; i < 44; i++){
for (i = 4; i < 44; i++)
{
T = W[i − 1];
if (i mod 4==0)
T = Substitute (Rotate (T )) XOR RConstant [i/4];
W[i] = W[i − 4] XOR T ;
SubBytes ShiftRows MixColumns AddRoundKey
}}
SubBytes ShiftRows AddRoundKey
copy State[ ] to output[ ]
}
```

Table 1 lists the key characteristics of the two encryption algorithms which have been studied and used in order to use them for the experimental proposal. The key characteristic which is more important is their Speed in which both algorithms are very fast. The key characteristic in which there is a relative difference is the Rounds, where AES needs 10, 12 or 14 rounds instead of the RSA that needs only 1.But here we take AES additional round of 16.

Table 1: Comparison of AES and RSA algorithms.

Characteristics	**Developed**	**Key length**	**Rounds**	Rounds	**Certifications**	**Speed**
AES	1998	128, 192 or 256 bits	10, 12 or 14		AES winner, CRYPTREC, NESSIE, NSA	Very fast
RSA	1977	1024–4096 bits	1	x	PKCS#1, ANSI X9.31, IEEE 1363	Very fast

VI. Experimental Results

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. Also, each transmitted signal through the new technology can transmitted as a relay and trusted signal with a weighted version of the re-encoded symbol. By the use of RSA algorithm we can take advantage the two keys encryption in order to provide better secure in the use of the new model.However, many other challenges and other benefits remains to be addressed through the integration of Internet of Things and Cloud Computing regarding the security issues, but also regarding the hole use of both technologies together[16].

Table 2: AES contribution in IoT and Cloud Computing and mobile computing.

AES characteristics	Key length	Rounds	Certifications	Speed
Internet of Things	x		x	x
Cloud Computing	x	x	x	less
IoT & CC integration	x	x	x	x
IoT & MC integration	x	x	x	more

The Tables 2 suggested the key characteristic of the encryption algorithms that used in order to achieve integration of the technologies of IoT and Cloud Computing ,mobile computing concerning the security issue. Table 2 presents which of the key characteristics of AES encryption algorithm contributes both IoT and Cloud Computing , mobile computing technologies, and at the end how completely contributes the integration model of IoT and Cloud Computing.

Through this integration we can achieve some useful functions, i.e. we can use the Cloud-based IoT service in order to connect sensors as well as mobile computing and also made them capable to share the sensor readings with others, reducing the security issues.

VII. Conclusion

The Cloud computing & mobile 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. Moreover, we present the main features of the Cloud Computing, mobile computing and its trade offs. 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.

Our next goal of the interaction and cooperation between things and objects sent through the wireless networks is to fulfill the objective set to them as a combined entity. In addition, based on the technology of wireless networks, both the technologies of Cloud Computing ,mobile computing and Internet of Things develop rapidly. In this paper, we present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. Regarding the rapid development of both technologies the security issue must be solved or reduced to a minimum in order to have a better integration model. These security challenges that surveyed in this paper could be the sector for further research as a case study, with the goal of minimizing them.

References

[1]. "Forecast: The Internet of Things, Worldwide, 2013. ", Gartner, 2013.
[2]. D.Evans, " The Internet of Things How the Next Evolution of the Internet Is Changing Everything", White Paper, Cisco, April 2011.
[3]. Miguel Blockstrand, Tomas Holm, Lars-Örjan Kling, Robert Skog and Berndt Wallin, „Operator opportunities in the internet of things", Ericsson review, 2011
[4]. Rooney, B. "Internet of Things Poses Big Questions." Wall Street Journal Online, July 3, 2013.
[5]. International Data Corporation (IDC) Press Release. "The Internet of Things Is Poised to Change Everything, Says IDC." October, 2013.
[6]. J. Mongay Batalla, P. Krawiec, Conception of ID layer performance at the network level for Internet of things, Springer J. Pers. Ubiquitous Comput. 18 (2) (2014) 465–480.
[7]. Y. Kryftis, G. Mastorakis, C. Mavromoustakis, J. Mongay Batalla, E. Pallis, G. Kormentzas, Efficient entertainment services provision over a novel network architecture, IEEE Wireless Commun. Mag. 23 (1) (2016).
[8]. Fei Tao, et al., CCIoT-CMfg: Cloud computing and Internet of things-based cloud manufacturing service system, IEEE Trans. Ind. Inform. 2 (10) (2014) 1435–1442. 02/05/.
[9]. Mohammad Aazam, et al., Cloud of Things: Integration of IoT with Cloud Computing, Springer International Publishing, 2016, pp. 77–94. 01/01/.
[10]. M. Rouse, IoT security (Internet of Things security), IoT Agenda, 01/11/2015. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/ IoT-security-Internet-of-Things-security (Accessed 27 July 2016).
[11]. N. Park, N. Kang, Mutual authentication scheme in secure Internet of things technology for comfortable lifestyle, Sensors 1 (16) (2016) 1–20. 24 12 2015.
[12]. T. Bhattasali, R. Chaki, N. Chaki, Secure and trusted cloud of things, in: India Conference (INDICON), 2013 Annual IEEE, IEEE, 2013, pp. 1–6.
[13]. Y. Simmhan, A.G. Kumbhare, B. Cao, V. Prasanna, An analysis of security and privacy issues in smart grid software architectures on clouds, in: 2011 IEEE International Conference on Cloud Computing, (CLOUD), IEEE, 2011, pp. 582–589.
[14]. Synapse Internet of Things Cloud, 2014. https://www.synapsewireless.com/snap-components/iot.
[15]. Mario Weber, Marija Boban, Security challenges of the Internet of Things, MIPRO 2016, , Opatija, Croatia.pp.20-25.
[16]. Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 3, THIRD QUARTER 2015.pp1294-1312.