International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, (2020), pp. 308 – 316

Model Simulation of Secure Cloud Computation in Iot Environment

Akanksha Gupta[1], Priyank Nahar[2]
[1]*Shri Venkateshwara University, Gajraula, Uttar Pradesh*
[2]*Shri Venkateshwara University, Gajraula, Uttar Pradesh*

Abstract

Agriculture is the one of the most important things for survival of humans in this world and all things of this world can be connected together to exchange information with the help of IoT. In this paper we connect these two, that is, we are going to combine agriculture and IoT. In agricultural sector, a large amount of data needs to be stored and retrieved securely but the IOT devices we use have a low amount of memory space. Hence, we need a storage area that has a large amount of secured storage space and so we implement a cloud storage system for our purpose. In this paper, we propose a secure data sharing system for IOT devices in which they are connected to the edge of the cloud and the data we receive from the IOT devices is encrypted and stored on the cloud. Only the corresponding receiver knows the exact key to decrypt the cipher text so the data is stored and retrieved securely. In this system we have used advanced wheat stone algorithm to encrypt the data from the IOT devices. The algorithm helps us to avoid Botnet attack and various other types of attacks on the data. We have used Omnet++ to simulate our entire scenario and collected the results. We show the verification process of the shared data as well as data retrieval after searching and thereafter analyze the performance of our proposed algorithm and prove that our algorithm is efficient to be used in many IoT applications.
Keywords: *IOT, Security, Cloud, Omnet++.*

I. Introduction

IOT is the emerging technology that connects various devices internally from watches to car, all of which are connected with the help of Internet using sensors. The sensors in these devices sense the environment around them and share the information with other devices with the help of Internet. One of the major drawbacks in these sensors is memory storage problem, that is, the device has a low memory area but it needs to store a large amount of data from the sensors.

Extreme changes in climate and changes in the weather conditions pose a big challenge in the agriculture field. So IOT may play a major role to predict the abrupt weather and help the farmers to product crops on the land properly and efficiently. Smart farming is the emerging technology which helps the farmers to reduce the waste and increase their productivity. The IOT based farming also helps them to grow the plants and herbs in a hygienic way.

IOT devices play a vital role in both industrial and commercial purpose. IOT devices can be classified into:

- home automations devices
- Industrial application devices
- domestic application devices

These devices are mainly used in humidity sensing, network switches, temperature sensing, movement checking etc. Typical domestic application devices are CCTV cameras (surveillance camera), smart TVs and cars. In home automation, the IOT devices are used in smart home management, light control system, monitoring moisture around home and various other applications.

When we look at the industrial use of IOT, IOT devices can cover many automation systems. Any industry that uses the IOT devices for the automation system is called a ‘smart factory’. The machines in this factory make use of the IOT sensors and communicate with each other without human interference. Since the involvement of human activity decreases, the productivity of the system gets

ISSN: 2233-7857 IJFGCN

increased.
Many organizations use the benefits of IOT but in turn also expose some security attacks on the devices. So it is essential to create a secure environment in the communication between the IOT devices.

When we talk about security, we need to concentrate more on cyber security, that is, we need to secure our data to be transferred online. So we have to consider about the various possible attacks on the Internet. For this purpose, the security analyzer needs to follow the following steps:

- Analyze the environment
- Test the IOT environment
- Report about the possible attacks
- Design the system

The security analyzer needs to know about the weakness and the strength of the system so that one can design a high quality and highly secured IOT system. Once after designing the attacking vectors the designer needs to know about the data flow of the IOT devices and if there exist any physical immunity, then there are many possible ways for the attackers to attack the system and as the worst case, there can exist the possibilities for botnet attacks.
In this paper, we are going to use IOT in agricultural sector and for the storage of data, we use the cloud storage system, for the security of which we implement the Wheatstone algorithm. In this way, the data sensed from the IOT device is encrypted and stored on the cloud storage and the required receiver has the key to decrypt this data. In this way, the attackers cannot read or intercept the data in an unauthorized manner. Hence the security of the system is maintained from outsider attacks. The IOT devices include smart devices like watches, mobile phones etc. The data path and the network play a vital role in such an IOT oriented system.
The IoT device architecture is as shown in the figure below:

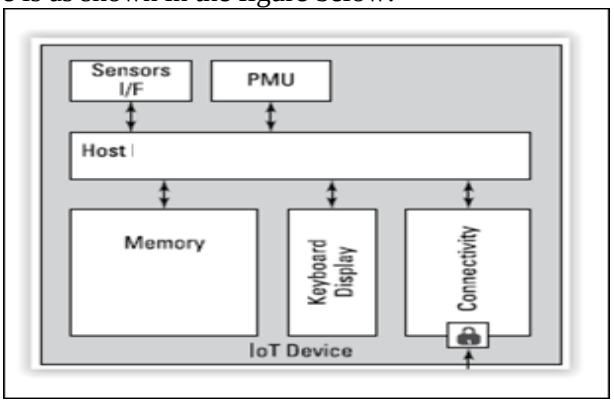

Fig 1. Architecture of IOT

II. Literature review

Wang et.al. “Research on Security Management for Internet of Things” [3] in their paper discussed the communication between machines by static or dynamic means. A machine is attached with the IOT device and in turn with the internet. This paper mainly concentrates on machine to machine communication, sensors and security. Raja et.al. in “An internet of things (IoT) based security alert system using raspberry pi”[5] proposed new methods which are introduced in the market for a security system. It follows sensor touch reorganization and wireless sensor security as the key roles of this system. The methods will be used in different applications with feasible costing and it will be easy to replace the faults but with the exception of disseminating in home applications. In this paper, the authors also discussed about Python scripting, which is used in raspberry PI and Raspbion OS coding. The python scripts will capture the motion and send email and SMS to the assigned system regarding the sensed data. Alam et.al. in “Interoperability of Security-Enabled Internet of Things”[6] proposed an IoT layered architecture and its

ISSN: 2233-7857 IJFGCN

frameworks. The system focuses on security reasons and their challenges. In the current scenario, different types of applications have been structured with IoT. The IoT network has been designed with a multi layer concept which will help the network work in a secure way. Suo et.al. in "Security in the Internet of Things: A Review" [8] have discussed about sequence of applications and their associations with each other. The proposed concept will be network secure through encryption and decryption and the proposed system also works on scheduling sensor networking. Chen in "An ibe-based security scheme on Internet of things"[9] proposed a system to mainly concentrate on Identity based encryption and its layers. It uses three layered architecture and finally concludes with an elliptic curve cryptosystem and identifies public key based encryption methodology and both of them are hence used for public key cryptography. Poslad et.al. in "International Workshop on Adaptive Security and Privacy management for the Internet of Things" have proposed different IoT applications with various security concerns. Also the author has discussed about different low powered and low security applications and user managed security threats in this paper. Razzaq et.al. in "Security Issues in the Internet of Things (IoT): A Comprehensive Study"[11] have discussed about the number of people connected through the Internet and the people who are connected on the network using the IoT applications on a daily basis and utilize the benefits. Most of the IoT devices are affected by attackers and security issues will be present on this entire network. The network system will be under secure roof and security system will protect the network by allowing only authorized people to access the network. Tahir et.al. in their paper "Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation"[13] have discussed about mobiles, tablets, computers and Internet connections. These are the devices that will access Internet connections through Wifi, Bluetooth and many other methods. In this paper, they have discussed about the various possibilities of the connections and communication ways. Suchitra and Vandana in their paper "Internet of Things and Security Issues"[15] discussed about the various IoT devices and the security challenges in different applications defining the integration of devices and communications. The system has talked about Denial of service and their corresponding attacks. Kai et.al. in their paper "Security and privacy mechanism for health internet of things"[16] have discussed about IoT in WBAN networks and its integration with smart homes and smart hospitals. The smart hospital applications work upon integrating the system with the patient's body and tracking his conditions stage by stage to easily identify the patient's wellness.

III. System model

The IOT devices in our proposed model use the cloud storage system. The data sensed from the IOT devices are encrypted with the help of wheat stone algorithm and at the receiver side, the data is decrypted using the same algorithm. We use the IOT devices in the agricultural field in such a way that the data forwarded through the IOT device will be secure.

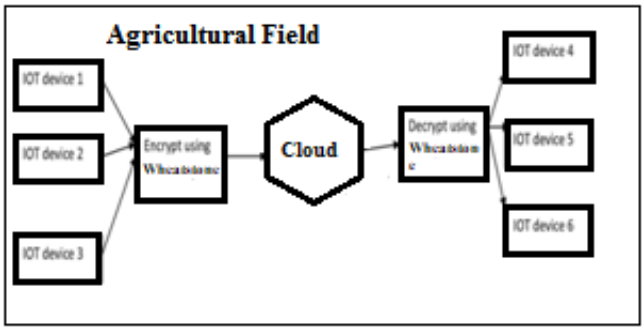

Fig 2. Proposed System Model

IV. Proposed System

ISSN: 2233-7857 IJFGCN

Smart Agriculture is a developing sector where the IOT devices are used to communicate with the farmers once after the climatic conditions of the farming land is sensed to increase yield. The current trends and the concept of internet of things (IoT), which has been deployed in many areas, can be extensively used in our system. The problem os security is an important drawback in IoT[21]. When the data is sent from an IoT device to another, the message can be intercepted which is a major security concern. To counter this, our research shall handle the question about how data can be sent securely through an IoT device using the advanced Wheat stone cipher encryption algorithm, which we describe in the following section.

Encryption:

To encrypt a message, divide the letters into several set of letters. We have to concentrate more on symbols, non-alphabet characters and spaces between words. Consider the following example; if one needs to encrypt the message – "Why don't you?", one should frame a lattice of 5X5[23] first, then fill the lattice with the message that needs to be encrypted and the remaining cells with the remaining alphabets. The alphabets I/J are placed on the same cell. In the example "why don't you?" the cell becomes:

W	H	Y	D	O
N	T	U	A	B
C	E	F	G	I/J
K	L	M	P	Q
R	S	V	X	Z

To encrypt the match WH is the pair at the two different corners of this square shape, specifically YI[10]. (In this we have picked YJ, for this situation.) The word is encrypted as:

YI EA ES VK EZ

Note that the letters in the word turned into second set of pairs, but it converted to a fourth pair. To create a cipher one has to insert punctuation, spacing and the message would be:

Yie ae, svkez.

At the receiver's end, the receiver of the message would know how the message is encrypted and the receiver ignores the unwanted characters like punctuations and spacing.

Encryption Algorithm
1. Begin
2. Generate Key
3. for (i = 0; i < 25; ++i)
   {
      Find all Occurance of key
         Remove All Duplicates of key

ISSN: 2233-7857 IJFGCN

```
  }
4. Remove non-alphabetic characters
5. If input length < 2
                Append the string
6. for (i=0;i< length; i++)
        {
                Get the position of the key
                Append the string
                 Create the Cipher
        }
7. End.
```

Decryption:
The same process is done from the last step to first step, ie in the reverse order. The receiver can decrypt the system with the key of the sender.

```
Decryption Algorithm
1. Begin
2. Get the Cipher text
3. Generate Key Square
4. Remove the Non Alphabeticc Characters
5. Find the length of the cipher text
6. for (i = 0; i < length; ++i)
   {
      Remove non-alphabetic characters
        If input length < 2
           Append the string
           Get the position of the key
           Append the string
           Create the decrypted Text
    }
         Get the position of the key
         Append the string
         Create the Cipher
  }
7. End
```

The proposed system uses the encryption and the decryption system[22] in the IOT devices so that the sensed data can be securely transferred through cloud.

V. Results and Discussion

We have used Omnet++ for our simulation. The data owners are the IOT devices which sense and then transmit the data once after it is encrypted by the wheat stone cipher [18]. The Access point, with the help of router sends the data to the cloud and in turn, the cloud stores this data. The corresponding data receiver receives the encrypted data from the nearby access point and decrypts the data with the help of the wheat stone decryption algorithm. The simulation and the corresponding results are as shown in the following figures:

ISSN: 2233-7857 IJFGCN

Fig 3. Simulation Scenario

Fig 4. Data transferred during simulation

Fig 5: Data is transferred in simulation

ISSN: 2233-7857 IJFGCN

Fig 6: Data is transferred in simulation

When compared to the other encryption algorithms, the wheat stone algorithm is more secure and the data is transferred in a controlled manner, as can be seen in the following graphs analysis:

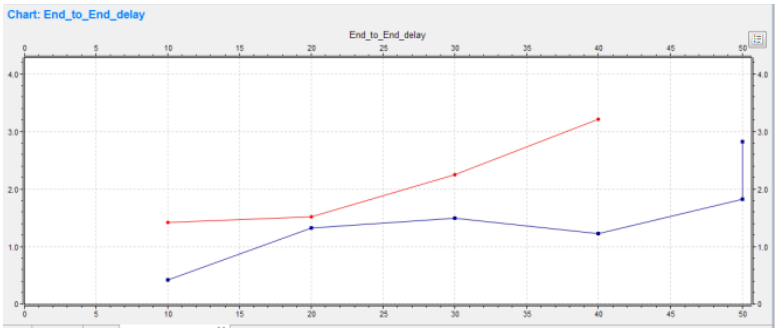

Fig 7: Result of End to end Delay

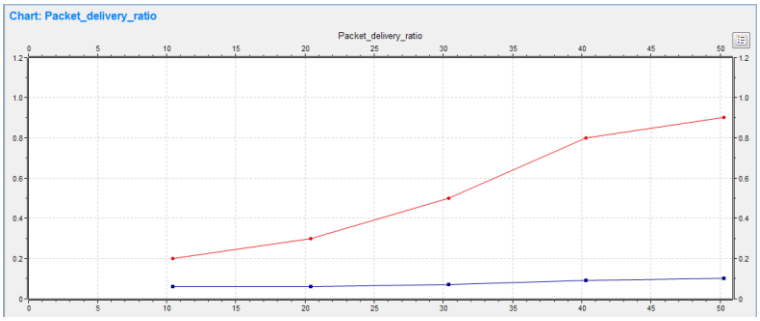

Fig 8: Result of Packet Delivery Ratio

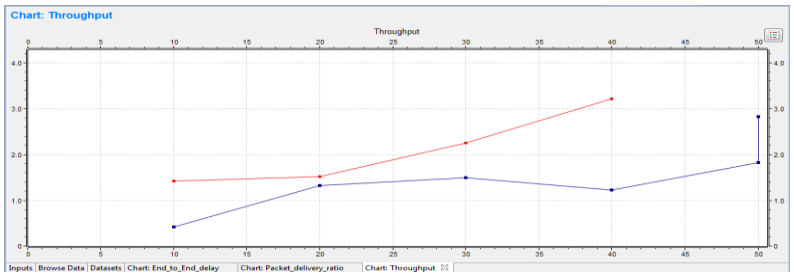

Fig 9: Result of Throughput

ISSN: 2233-7857 IJFGCN

The comparison table of various encryption algorithms and its efficiency is given below:

Table 1. Comparison Table of Efficiency

Algorithm	Efficiency
DES	30%
IDEA	60%
BLOWFISH	40%
RSA	65%
AWSA(proposed)	85%

The security of the IOT devices get increased since the data is encrypted and only can be decrypted by the respective receivers using a secure key.

VI. Conclusion

Agriculture is the basic necessity of human life. Day by day we need to increase the yield so that we can handle the ever increasing human demand. Here we propose a new method to use IOT devices in the agricultural sector. IOT is the emerging technology in the developing world but the security of the devices in use is the big question. In this paper we have proposed a new technology system that provides high security from any kind of malicious attack. We have proposed an advanced algorithm called the "advanced wheat stone" algorithm. The data sensed from the devices is encrypted and stored on the cloud system and the key is shared with the receiver so that the receiver can decrypt the sensed data from the cloud. In this manner, any third party can not read the data from the cloud. The proposed system is safer when compared to the existing systems as shown. We have used Omnet++ simulation tool to simulate the entire scenario. We have observed that the results thus obtained are much better comparatively to other algorithms in the market today.

VII. REFERENCES

[1] T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes", in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1844- 1852, Dec. 2017.

[2] I. Andrea, C. Chrysostom and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 180- 187.

[3] Wang, Kun & Bao, Jianming & Wu, Meng & Lu, Weifeng. (2010). Research on security management for Internet of Things. 15. 10.1109/ICCASM.2010.5622549.

[4] R. K. Kodali, V. Jain, S. Bose and L. Boppana, "IoT based smart security and home automation system" 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 1286-1289.

[5] A.Arun Rajaa, R.Naveedhab, G.Niranjanadevic and V.Roobinid, An internet of things (iot) based security alert system using raspberry pi, Asia pacific international journal of engineering science vol. 02 (01) (2016) 37–41.

[6] Alam, Sarfraz & Chowdhury, Mohammad & Noll, Josef. (2011). Interoperability of Security-Enabled Internet of Things. Wireless Personal Communications. 61. 10.1007/s11277-011-0384-6.

[7] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," in IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, Oct.-Dec. 1 2017.

[8] Suo, Hui & Wan, Jiafu & Zou, Caifeng & Liu, Jianqi. (2012). Security in the Internet of Things: A Review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. 3. 10.1109/ICCSEE.2012.373.

ISSN: 2233-7857 IJFGCN

[9] Chen, Wang. (2012). An IBE-based security scheme on Internet of Things. 1046-1049. 10.1109/CCIS.2012.6664541.
[10] Akinyele, J. A., Garman, C., Miers, I., Pagano, M. W., Rushanan, M., Green, M. & Rubin, A. D. (2013). Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2), 111–128.
[11] Security issues in the Internet of Things (IoT): A Comprehensive Study - Mirza Abdur Razzaq,Sajid Habib Gill,Muhammad Ali Qureshi,Saleem Ullah-International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.
[12] Almorsy, M., Grundy, J. & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
[13] Tahir, Hafsa et al. "Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation." (2016).
[14] Ambrosin, M., Conti, M. & Dargahi, T. (2015). On the feasibility of attribute-based encryption on smartphone devices. Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, pp. 49–54.
[15] Suchitra.C, Vandana C.P, Internet of Things and Security Issues, IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 – 139.
[16] Kang, Kai & PANG, Zhi-bo & Wang, Cong. (2013). Security and privacy mechanism for health internet of things. The Journal of China Universities of Posts and Telecommunications. 20. 64–68. 10.1016/S1005-8885(13)60219-8.
[17] Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M. & Liljeberg, P. (2016). On the feasibility of attribute-based encryption on internet of things devices. IEEE Micro, 36(6), 25–35.
[18] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[19] R. Want and S. Dustdar, "Activating the internet of things [guest editors' introduction]," Computer, vol. 48, no. 9, pp. 16–20, 2015.
[20] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, "Security in the industrial internet of things," 2016.
[21] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.
[22] Rabin, M.O.: Digitalized signatures and public-key functions as intractable as factorization. Tech. rep., Massachusetts Inst of Tech Cambridge Lab for Computer Science (1979).
[23] Kong, J. H., Ang, L.-M., & Seng, K. P. (2015). A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. Journal of Network and Computer Applications, 49, 15 – 50.

ISSN: 2233-7857 IJFGCN