INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Ensure the securities in IoT for smart home monitoring system

Kaviya S.
kaviyaoct20@gmail.com
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Divya Lakshmi R.
ldivya892@gmail.com
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Jenifa G.
gjenifa@gmail.com
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu

ABSTRACT

Smart building using IOT technique is used to maintain home automation in a smart way. In order to improve security in the home, the various sensor is used. In that PIR and MQ-6 sensors plays a major role. The data from various sensors are sent to the Arduino board and get stored in the cloud. In this paper home monitoring system with intrusion, detection technique is used. For data security, wireless sensor network (WSN) playa a major role. To facilitate data encryption, a method namely DES based on efficient key generation mechanism was proposed.

Keywords— *IoT technique, Intrusion detection, DES, RSA*

1. INTRODUCTION

The smart automation using IOT is a wireless home security project. In today's world security for home is essential. If any sensors found any intruders, then it will send an alert message and for faster data transmission the ESP8266 sensor plays a major role, which is used to control and monitor the system. To provide security for the transmitted data the Data Encryption Standard and RSA algorithms are used. In this proposed system the security algorithms used are highly reliable and it will consume very less time in comparison with the existing system. IoT involves extending internet connectivity in many devices such as desktops, laptops, smartphones and tablets.

In SHAS schema, connecting a TV to the Internet might be considered as a normal scenario, since it would make our life easier. However, the single fact of connecting such devices to the IoT world might generate a potential vulnerability since a hardening standard is still not in place to protect such devices. In addition, the risk arises as the SHAS is being used to handle physical security services, such as opening doors or preventing burglars from entering a place.

2. SECURITY APPROACHES

2.1 A monitoring system is built for the home automation system

In Shetel and Agarwal IOT paper (2016) explain internet connectivity for all kind of devices and physical objects in real time system. This paper used to provide security for the data.

In Lee(2017) explains in their paper the explains the physical objects in IOT which contains the embedded technology helping in developing machine to machine or man to machine communication. This paper gives data about the security provided for the stand-alone system.

In Chou (2017) describes in their paper a home automated system has a remote-controlled operation. This paper tells about the problem of providing security for the data. The Home Automation System requires heterogeneous, an eternal and distributive computing environment's careful study to develop the suitable HAS.

3. PROPOSED SYSTEM

In this paper, we are proposing a smart home automation system with some sensors. The Arduino is an important sensor and acts as a brain of the system and it will receive all the data sent by the sensors. The Arduino board is used to transfers the collected data to the cloud for storage. During data transmission, to prevent the data from intruders an algorithm named Data Encryption Standard and RSA is used. This algorithm provides confidentiality and security for the data by comparing their efficiency. So that the data can be prevented from the third party.

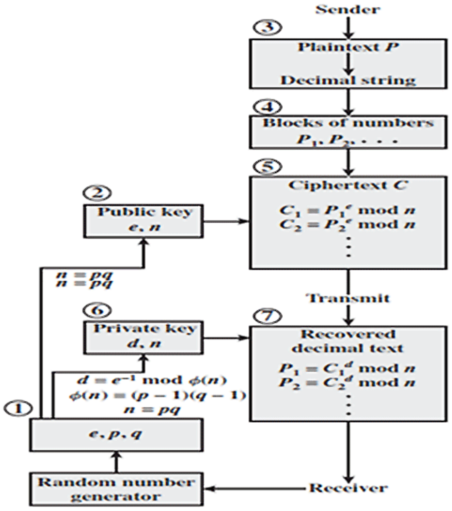


Fig. 1: Proposed system algorithm

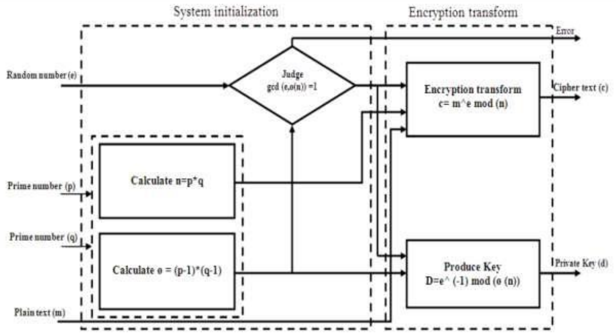


Fig. 2: Proposed system process

4. SYSTEM DESIGN

The **Data Encryption Standard (DES)** is a symmetric-key block cipher used to provide encryption for the data. DES is an implementation of a Feistel Cipher. It uses a 16 round Feistel structure. The block size is 64-bit. Though the key length is 64-bit, DES has an effective key length of 56 bits since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only)

RSA (Rivest–Shamir–Adleman) is the public-key encryption algorithm used to provide security for data. In such an algorithmic program the secret writing secret's public and it's totally different from the secret writing key that is unbroken secret (private). In RSA, this spatiality relies on the sensitive issue of the factoring of the merchandise of 2 giant prime numbers, the "factoring problem".RSA may be a comparatively slow algorithmic program, and sense of this,less unremarkablelyaccustomed directly inscribe user knowledge. More often, RSA passes encrypted shared keys for regular key cryptography that successively will perform bulk encryption-decryption operations at abundant higher speed. cryption operations at much higher speed.

5. HARDWARE REQUIREMENTS

Arduino acts as a brain of the system and processes the information from the **s**ensing element and facilitates the shift ON/OFF of the electrical appliances. Arduino is an associate ASCII text file physical science platform **s**upported easy-to-use hardware and code. Arduino boards are able to browse inputs - light-weight on a sensing element, a finger on a button, or a Twitter message- and switch it into associate output - activating a motor, turning on the associated diode, business one thing online.it consists of each a physical programmable printed circuit and a bit of code, or IDE (Integrated Development Environment) that runs on your pc, wont to write and transfer coding system to the physical board.

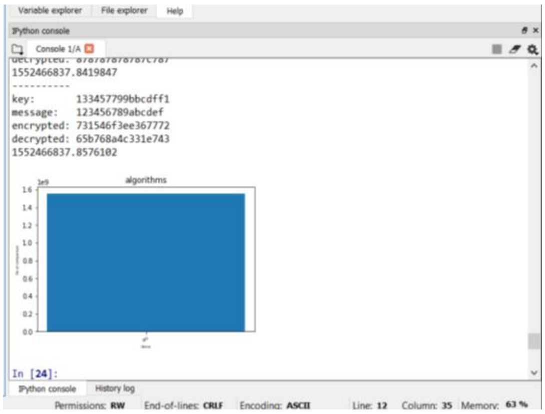
6. INTRUSION IN THE CLOUD

Many IoT systems use a cloud for data analysis, storage, and management. Because cloud providers are responsible for security.Cloud infrastructure working in Internet protocols, which may encourage potential attackers. While part of the responsibility lies with the cloud provider, device manufacturers are responsible for the end user.

7. IMPLEMENTATION AND RESULTS

From this implementation, the comparison graphs clearly show that the data encryption standard (des) security algorithm provides the best security than RSA algorithm for data in the Arduino board then the data are securely stored in the cloud.

7.1 DES algorithm



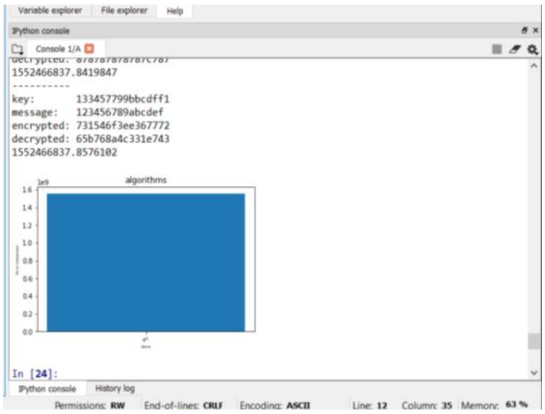
```
1552466837.8419847
----------
key:        133457799bbcdff1
message:    123456789abcdef
encrypted:  731546f3ee367772
decrypted:  65b768a4c331e743
1552466837.8576102
```

```
In [24]:
```

Permissions: RW   End-of-lines: CRLF   Encoding: ASCII   Line: 12   Column: 35   Memory: 63 %

Fig. 3: Efficiency of DES algorithm

7.2 RSA algorithm



```
1552466837.8419847
----------
key:        133457799bbcdff1
message:    123456789abcdef
encrypted:  731546f3ee367772
decrypted:  65b768a4c331e743
1552466837.8576102
```

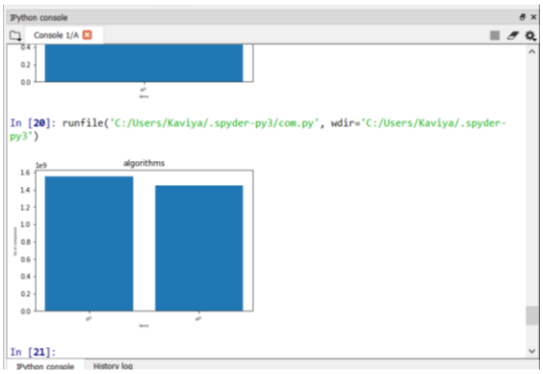
```
In [24]:
```

Permissions: RW   End-of-lines: CRLF   Encoding: ASCII   Line: 12   Column: 35   Memory: 63 %

Fig. 4: Efficiency of RSA algorithm

7.3 Efficiency graph

This graph will clearly prove the data encryption standard algorithm provides the best efficiency.



```
In [20]: runfile('C:/Users/Kaviya/.spyder-py3/com.py', wdir='C:/Users/Kaviya/.spyder-py3')
```

```
In [21]:
```

Fig. 5: Efficiency graph

8. CONCLUSION

The purposed system helps to provide a complete secured building by providing features such as intruder alert, automating electronic item usage. The sensors used here are of low cost. The sizes of the devices are also manageable which makes the purposed system cost-effective. Secured IoT-based home automation applications using WSNs. In WSNs, because of the limited power of sensor nodes, effective key generation mechanism which could accomplish all major data security requirements and consumes less processing time for data encryption is well needed. A security algorithm, namely DES is based on a simple and efficient key generation procedure. The proposed IoT integrates low power ESP 8266 and the proposed DES in WSNs with internet to provide additional benefits of increased coverage range and capability of supporting a large number of sensor nodes due to the usage of low power ESP 8266, it also consumes less processing time for data encryption because of the utilization of DES algorithm.

9. REFERENCES

[1] Rosslin John Robles and Tai-hoon Kim, “Review: ContextAware Tools for Smart Home Development”, International Journal ofSmart Home, Vol.4, No.1, January 2010

[2] HitendraRawat, Ashish Kushwah, Khyati Asthana, AkankshaShivhare, “LPG Gas Leakage Detection & Control System”, NationalConference on Synergetic Trends in engineering and Technology(STET-2014) International Journal of Engineering and technical research ISSN: 23210869, Special Issue

[3] Nicholas D., Darrell B., Somsak S., “Home Automation using cloud Network and Mobile Devices”, IEEE Southeastcon2012, Proceedings of IEEE. [14] Chan, M., Campo, E., Esteve, D., Fourniols, J.Y., “Smart homescurrentfeatures and future perspectives,” Maturitas, vol. 64, issue 2, pp.90-97, 2009

[4] Savitha, S., and S. Yamuna. "Implementation of AES algorithm to overt fake keys against counter attacks." In Computer Communication and Informatics (ICCCI), 2016 International Conference on, pp. 1-5. IEEE, 2016.Plagiarism Check Report.

[5] Alexandru-CorneliuOlteanu*, George-Daniel Oprina*, Nicolaeğăpuú* and Sven Zeisberg,” Enabling mobile devices for home automation using ZigBee”.2013 19th International Conference on Control Systems and Computer Science

[6] Luigi Coppolino, Valerio D’Alessandro, Salvatore D’Antonio, Leonid Lev † and Luigi Romano, “My Smart Home is Under Attack” 2015 IEEE 18th International Conference on Computational Science and Engineering.

[7] Makkad, Ritu Kaur, and Anil Kumar Sahu. "Novel design of fast and compact SHA-1 algorithm for security applications." In Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on, pp. 921-925. IEEE, 2016.

[8] Ratna, AnakAgungPutri, Prima DewiPurnamasari, Ahmad Shaugi, and Muhammad Salman. "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple- O authentication based security system." In QiR (Quality in Research), 2013 International Conference on, pp. 99-104. IEEE, 2013.

[9] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms. "International Journal of Security and Its Applications 9, no. 4,2015

[10] N.Singh, Shambhu Shankar Bharti, R. Singh, and Dushyant Kumar Singh. Remotely controlled home automation system. In2014 Inter-national Conference on Advances in Engineering Technology Research(ICAETR - 2014), pages 1–5, Aug 2014.

[11] R.Shete and S. Agrawal. Iot based urban climate monitoring using raspberry pi. In2016 International Conference on Communication and signal Processing (ICCSP), pages 2008–2012, April 2016.

[12] E.Ahmed, I.Yaqoob, A.Gani, M.Imran, and M. Guizani. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges.IEEE Wireless Communications, 23(5):10–16, October 2016.

[13] Y.Upadhyay, A.Borole, and D. Dileepan. MQTT based secured home automation system. In2016 Symposium on Colossal Data Analysis and networking (CDAN), pages 1–4, March 2016.

[14] S.Lee, N.Lee, J.Ahn, J.Kim, B.Moon, S. h. Jung, and D. Han.Construction of an indoor positioning system for home Iot applications.In2017 IEEE International Conference on Communications (ICC), pages 1–7, May 2017.

[15] M. S. Kamal, S. Parvin, K. Saleem, H. Al-Hamadi, and A. Gawanmeh.Efficient low-cost supervisory system for the internet of things enabled smart home. In2017 IEEE International Conference on CommunicationsWorkshops (ICC Workshops), pages 864–869, May 2017.

[16] A.Sahadevan, D.Mathew, J.Mookathana, and B. A. Jose. An offline-online strategy for iot using mqtt. In2017 IEEE 4th InternationalConference on Cyber Security and Cloud Computing (CSCloud), pages369–373, June 2017.

[17] R. K. Kodali and S. Soratkal. MQTT based home automation system usingesp8266. In2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), pages 1–5, Dec 2016.

[18] A.Sahadevan, D.Mathew, J.Mookathana, and B. A. Jose. An offlineonline strategy for iot using mqtt. In2017 IEEE 4th InternationalConference on Cyber Security and Cloud Computing (CSCloud), pages369–373, June 2017.

[19] I. Aydin and N. A. Othman. A new iot combined face detection of people by using computer vision for security application. In2017 InternationalArtificial Intelligence and Data Processing Symposium (IDAP), pages1–6, Sept 2017.

[20] D.Pavithra and R. Balakrishnan. Iot based monitoring and controlsystem for home automation. In2015 Global Conference on Communication Technologies (GCCT), pages 169–173, April 2015. [19] S. L. S. S. Harsha, S. C. Reddy, and S. P. Mary. Enhanced homeautomation system using internet of things.In2017 InternationalConference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pages 89–93, Feb 2017.

[21] K. Vijayakumar, N. Divya Sri, M. Vijayashree, “An Effective User Revocation and Anti Collusion System for Dynamic Groups in Cloud”, International Journal for Research in Applied Science & Engineering Technology, ISSN: 2321-9653, Volume 4 Issue V, May 2016