International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21767

Investigation the scope of security in IoT Considering RSA Algorithm

Kamal Arora[1], Deepinder Kaur[2]
[1]M.Tech. Scholar, Department of CSE, SUSCET Tangori Mohali, Punjab, India
[2]Assistant Professor, Department of CSE, SUSCET Tangori, Mohali, Punjab, India

Article Info
Volume 7, Issue 6
Page Number : 302-304

Publication Issue :
November-December-2021

Article History
Accepted : 05 Dec 2021
Published : 18 Dec 2021

ABSTRACT

The Internet of Things (IoT) has emerged as an area of incredible impact, with the arrival of savvy homes, savvy cities, and savvy everything. For current and future research areas it is one of the hot topics involved by both industry sector and academia. The Internet of Things (IoT) also known as a web of everything or the economic Internet is a new technology paradigm imagine as a worldwide network and devices competent to interacting with each other. Privacy and security are the major challenges in the Internet of Things (IoT) security due to the distributed nature of IoT networks [1]. Internet of things (IoT) is an upheaval of the internet. IoT are often said the expansion of internet services. It provides a platform for communication between gadgets where gadgets can manage and organize themselves. The IoT allows everyone to be connected anytime and anywhere.

Keywords : Internet of Things, RSA algorithm

I. INTRODUCTION

Internet of things (IoT) is an upheaval of the internet. IoT are often said the expansion of internet services. It provides a platform for communication between gadgets where gadgets can manage and organize themselves. The IoT allows everyone to be connected anytime and anywhere. The Internet of Things (IoT) has emerged as an area of incredible impact, with the arrival of savvy homes, savvy cities, and savvy everything. For current and future research areas it is one of the hot topics involved by both industry sector and academia. The Internet of Things (IoT) also known as a web of everything or the economic Internet is a new technology paradigm imagine as a worldwide network and devices competent to interacting with each other. No doubt, it can be said that AI and IoT based devices are responsibly making our life better and upgrading our life standard. It is easy for these devices to enhance the comfort, convenience and better management. It is obvious that if our devices work automatically and take decision according to situation, our life will be easy and comfortable.

Privacy and security are the major challenges in the Internet of Things (IoT) security due to the distributed nature of IoT networks [1]. To tackle with these problems we use the concept of cryptography with RSA algorithm.

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

II. Literature Review

Mahalakshmi et.al (2019) proposed the approach of combined two existing encryption algorithms and implemented their model in simulation tool named Matlab. It is very difficult to provide security to IoT devices using traditional encryption technique. They explained that a hacker can know the cipher key. [6].
Ge Wu and Willy (2019) discussed the need of tight security and key generations in public-key cryptography. First of all, the researcher of this work generalized key generation algorithms related to traditional schemes. [7].

Marek and Ogiela (2019) proposed the new security solutions based on cognitive approaches. In this paper they considered innovative computing paradigm which is also known as cognitive cryptography. These modules have been formulated in order to semantic evaluate the encrypted data. [8].

Xiangyu Chang et.al (2019) examined that optical scanning cryptography (OSC) is one of most utilized optical encryption systems. OSC scheme is vulnerable to COA attacks. [9].

Irosh and Malka (2019) considered the remote monitoring of health should be made trustworthy by incorporating WBAN, IoT, and cloud computing. These are beneficial for intelligent healthcare setting. Cloud computing also provides real-time data storage and processing for IoT devices like WBAN devices. [10].

III.Research Methodology

The present dissertation is entitled as “A Two Tier Security model for IoT Based Devices”. The primary focus of this research is to ensure the security of IoT based devices using a combination of two encryption techniques that are Multiplicative Inverse and Advance Encryption Standard (AES). Many of IoT based security systems consumes a lot of time to process the data during transmission. When data is transferred over any network there is always threat from crypto analyst. In order to secure the data and to disable unauthentic user to access the data, there is need of more secure mechanism to maintain the efficiency and faster transmission.

IV.Objective of Research Work

In this proposed work following research objectives will be achieved:

To study the existing security mechanism and to find out their Loopholes.
To propose a multilayer security model using Multiplicative Inverse and AES to resolve the issues and threats related to security of IoT based devices.
To design a simulator for comparison of securing of IoT based devices of proposed and existing system in terms of packet size, error rate and time consumption.

Proposed Encryption Method

The proposed method uses an advanced encryption standards and multiplicative inverse algorithm for encryption. To implement IP filter-based security system in order to secure IoT based devices from different kind of attackers. To secure the data transmission over cloud, first of all size of packets is decreased using replacement policy.

In this work, IP filter is considered for the rejection of unauthenticated data transmission between servers to client. Port no is specified to enhance the security of data.
After that, the data is encrypted with the help of Multiplicative Inverse Cryptographic technique. In next step, the packet of data is encrypted applying AES technique.

In the proposed work, own socket server and client side data sender and receiver module is proposed which are coded in Net beans in order to enhance the security of data and avoid unauthentic access during data transmission. Therefore the proposed model is a multilayer security mechanism as the data is encrypted at two levels.

V. Conclusion

The Internet of Things is comprised of a widely diverse range of devices which are found in utilities, industrial and manufacturing systems. Although IoT explosion offers a wide range of opportunities for manufacturers and consumers, it also poses major risks in terms of security being a widespread network. A security mechanism is needed to protect the devices from cyber attacks. This can only be achieved by including security mechanism in the early stages of IoT design to observe privacy and safe transmission of data over network. Hackers can target the weak points and exploit the data of entire infrastructure if security concerns are not addressed at early stages in implementation of IoT. This necessitates the implementation of security mechanism of IoT based devices at early stage.

VI. REFERENCES

[1]. Vithya Vijaylakshmi, “Enhancing the security of IoT Data using Multilevel Encryption (2017)”

[2]. B.S Kumar and T.C.S.P Raju “Introduced the Intrusion Detection System- Their Types and Prevention (2013).

[3]. Trivedi,”Cryptographic Approach for Securing IoT Device” (2018)

[4]. Vinay Sagar and Kusuma S.M,”Home Automation using Internet of things” (2015)

[5]. Cryptography- Wikipedia, en.wikipdedia.org/wiki/cryptography.

[6]. Mahalakshmi et.al,"Image Encryption Method Using Differential Expansion Technique, AES and RSA Algorithm," (2019).

[7]. Ge Wu and Willy, “Generalized public-key cryptography with tight security” (2019) Y. Yusfrizal and F. Agustin, "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption," 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapet, Indonesia, 2018, pp. 1-6.

[8]. Marek R.Ogiela et al.”Cognitive solutions for security and cryptography” (2019)

[9]. Xiangyu Chang and Z.Zhang,” Cipher text-only attack on optical scanning cryptography” (2019)

[10]. IroshaJayatilleka and Malka N. Halgamuge “Internet of Things in healthcare: Smart devices, sensors, and system related to diseases and health conditions” (2019).

Cite this article as :

Kamal Arora, Deepinder Kaur, "Investigation the scope of security in IoT Considering RSA Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 302-304, November-December 2021. Journal URL : https://ijsrcseit.com/CSEIT217663