IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT

Impact Factor: 6.252

Volume 2, Issue 2, June 2022

# Study of Data Protection in IOT based Cyber Security Physical Systems

**Rohit Lathigra**

Student, Department of MCA

Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

**Abstract:** *In this paper it is discussed about how can one protect data by using techniques and algorithm. Cyber Security is to protect computers, servers, mobile/electronic devices from malicious attacks. It is mainly used to maintain the security of data from computers or servers so that data cannot be theft by others or any kind of disruption of the services. Cyber Security risk is traditionally focused on machine-based threat. As IOT contains large amount of data, to protect the confidential as well as sensitive information need to apply security mechanisms or protocols to protect such kind of data from cyber-attackers.*

**Keywords:** Data security, Data Protection, IOT, Encryption algorithms

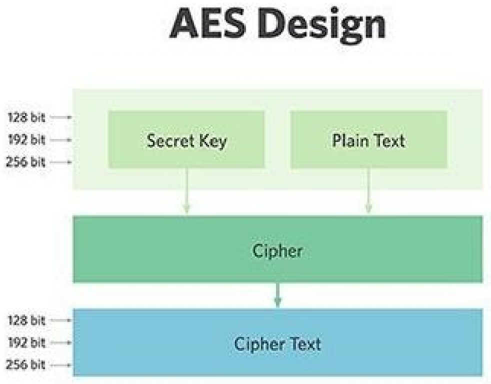
## I. INTRODUCTION

With the development and formation of digital society, the issue of ensuring data security is becoming more and more urgent. At present Internet of Things (IOT) connected devices is increasing more and more nowadays so one need to protect the data so that any kind of cyber-attacks do not steal the data. All modern organizations strive to increase the integration of information technologies in their areas of activity, because this allows you to move to a qualitatively new level of storage, processing and transmission of information. IOT is defined as the physical objects with sensors, software and technologies that connects to the internet and exchange data with other devices over the communication networks. IoT makes objects (things) and machines in our surrounding environment to connect, communicate, act and react with each other autonomously without human intervention.

## II. LITERATURE REVIEW

In the paper end to end encryption process is discussed wherein the transmission of data from the source point to the end point the security message is not affected. It should be implemented at transport layer or can be higher. The disadvantage of encrypting the data at transport layer is that it is transparent, means data can be stolen by hackers while transmission of data. Limitation of the article is that it is just discussed about the techniques used to protect data in IOT systems. Mostly Phishing attack is done to steal the confidential data which is stored in IOT based systems.

## III. IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

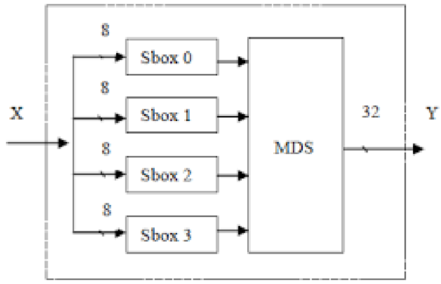


Advanced Encryption Standard Algorithm is the algorithm where the sensitive data can be protected by assigning a secret key to the data where its size can be of 128-256 bit of key. The flexibility of this algorithm is that up to the given range

DOI: 10.48175/IJARSCT-5457

of bit one can assign more number of bit as the data is more sensitive and confidential. The key is created in the arrangement as Mix Alphabets, Symbols and Numbers wherein the key cannot be decrypted easily by hackers. In AES each block consists of 16 byte (4 byte x 4 byte=128) grid. Till now this algorithm fails the hacker to decrypt the data.

## IV. IMPLEMENTATION OF TWO FISH ALGORITHM



Basically, Two Fish Algorithm is stronger algorithm to protect any kind of files and folders. It is optimized for 32-bit central processing units and it works in both hardware and software environments. To secure the data it creates of about 16 rounds wherein the actual data is not visible to others rather only the long bits of key will be seen.

## V. FUTURE OF DATA ENCRYPTION IN IOT

Nowadays, as the encryption algorithm is increasing more and more hackers are working on algorithms to crack it, one needs to encrypt its data by using multiple algorithms so that hackers cannot crack it very easily. Hence the data will be more secure in software as well as hardware environments.

## VI. CONCLUSION

As discussed in this paper one can keep its data protected by using algorithms and techniques and changing its encryption frequently so that the data will not be stolen from IOT Based systems which are nowadays been implemented in small scale. As the growth of storing the data is increasing and to keep data secure one needs to use techniques and algorithm to keep the sensitive and confidential data away from the hackers.

## REFERENCES

**[1].** A model of threats to the confidentiality of information processed in cyberspace based on the information flow model : Department of Complex information security of computer systems – Author: Egoshin N.S. Konev A.A and Shelopanov A.A

**[2].** Research on Data Confidentiality and Security of Computer Network Password : Journal of Physics – Author: Hanyu Liang

**[3].** https://www.simplilearn.com/data-encryption-methods-article

**[4].** https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future

**[5].** A Novel Security Systems for IOT Applications : 12th International Conference on Computing Communication and Network Technologies – Author : Ayesha Sameer Shaikh, Guntakala Likhita, Fouzul Atik

**[6].** https://ieeexplore.ieee.org/document/9579502

**[7].** Exploring Data Security and Privacy Issues in Internet of things based on five layer architecture : International Journal of Communication Networks and Information Security – Author : P.Ravikumar, Thein Wan and Wida Susanty Haji Suhaili

**[8].** https://www.researchgate.net/profile/Ravi-Kumar-22/publication/341201776_Exploring_Data_Security_and_Privacy_Issues_in_Internet_of_Things_Based_on_Five-Layer_Architecture/links/5eb37657299bf152d6a1c8fc/Exploring-Data-Security-and-Privacy-Issues-in-Internet-of-Things-Based-on-Five-Layer-Architecture.pdf

DOI: 10.48175/IJARSCT-5457