Securing the IOT network with use of enhanced blowfish algorithm

Saritha. K,

Assistant professor,

Computer Science & Engineering,
Navrachana University, Vadodara, Gujarat, Country
saru.rose123@gmail.com

***Abstract*— The paper explains about the use of internet of things in the all the different field of the engineering and also explains the use of securing the data in the internet of things network. The first problem was the generation of data from the IOT network from different application. The security of the data was not up to the mark. To enhance the security, we use blowfish algorithm. The blowfish algorithm proposed in the system is modified depending upon the rounds and the substitution boxes, which faster the process of encryption and decryption. The IOT can be combined with cloud computing. The data stored will be in the cloud in the IOT network.**

Index Terms— Blowfish algorithm, security, Internet of things

I. INTRODUCTION

Today world of science is evolving with new technologies. The word digitization pays a key role in the market. The computer science field has evolved too much that new technologies are coming to the eyes more frequently. The Internet of things and cloud computing has come to the action in the combined manner. The security seems to be a major concern for the market as all the services are using the Internet of things everywhere. The applications include marketing, health care, government, manufacturing, business and much more. 1.1 Internet of Things

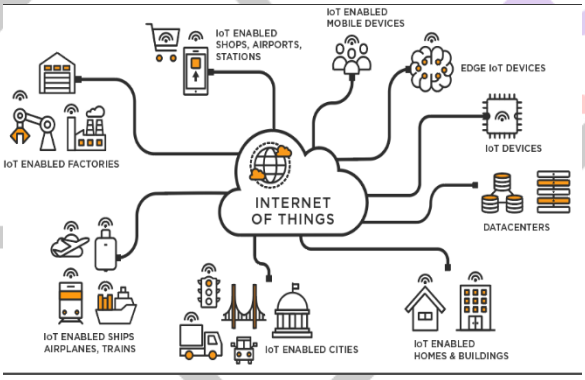

Fig 1.1 Architecure of IOT network[1]

The internet of things plays avery important role in day to day life ,starting from the houshlod system like the automation system till the health care system.The internet of things where the devices are connected in an environment and analysed with the help of sensores.There are various sensors inlcluding the aurdino board whhc will help for monitoring the data and storing thr data for future purpose in the cloud environment.

1.2 Cloud computing

Cloud computing as the word says everything is internet, we can access the data everywhere from different parts of the world thorough cloud. There are various companies which are offering their own cloud for customers to use their spaces. The different services offered by the cloud are the software as a service, Infrastructure as a service and much more.

Fig 1.2 Architecture of Cloud Computing [2]

II. LITERATURE REVIEW

2.1 Secure integration of IOT and cloud computing

The paper explains the use of how cloud computing will enhance the internet of things. It describes only the survey of different techniques used in cloud computing. The paper focus on the security aspect of the cloud computing and internet of things [3].

Fig.2.1.1 Integration of IOT and Cloud computing [3]

2.2 Scalable and secure Internet of things system using multifactor authentication and light weight cryptography

The paper describes about the use of hybrid cloud environment.The security of the data is enhanced by the use of multifactor authentication.The private cloud data is protected with the use of AES algorithm and the public cloud data is protected with the help of RC4 algorithm[4].

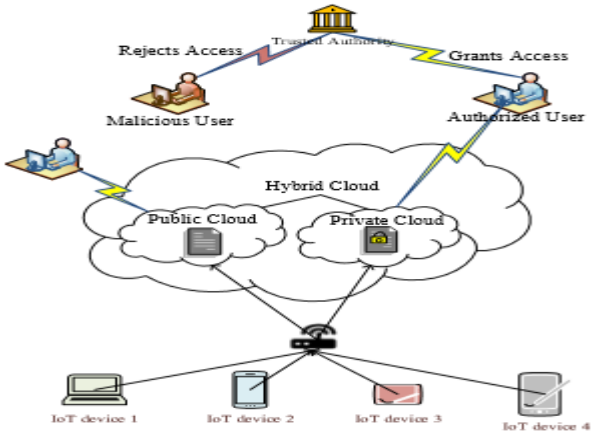

Fig 2.2.1 A hybrid cloud approach for protecting data in IOT network[4].

2.3 Hardware implementation of blowfish algorithm

The paper explains the implementation of blowfish algorithm with change in the f function. The technique seems effective in the case of protection of data but complexity is high. The time taken by the algorithm is high though the software implementation blowfish is not effective[5].

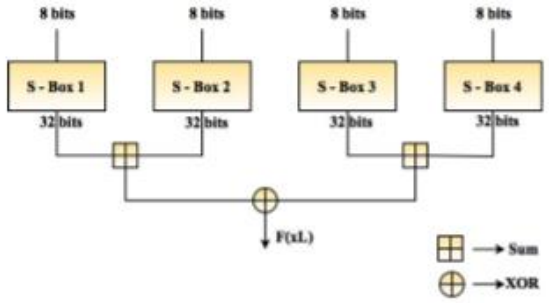

Fig 2.3.1 Blowfish algorithm structure

III.PROPOSED SYSTEM

3.Proposed System

Blowfish is an encryption technique designed by **Bruce Schneider** in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use.

1. **blockSize**: 64-bits
2. **keySize**: 32-bits to 448-bits variable size
3. **number of subkeys**: 18 [P-array]
4. **number of rounds**: 16
5. **number of substitution boxes**: 4 [each having 512 entries of 32-bits each]

The proposed algorithm uses P-array, that is number of sub keys as 15 and the rounds in the algorithm is being reduced to 12 so that the use of plaintext will be effective. The substitution boxes will be enhanced to 6 to perform the encryption and decryption in an effective manner. The proposed algorithm reduces the rounds and and makes the algorithm to work in a smarter way reducing the complexity. The enhanced blowfish algorithm is a symmetric key encryption algorithm. In the case of symmetric keys same key is used by the two parties the sender part and receiver party to encrypt and decrypt the data. The symmetric key algorithm is a block cipher where the individual plain text is considered as a block for encryption and decryption of data.

The symmetric key encryption algorithm also includes Advanced Encryption algorithm too.

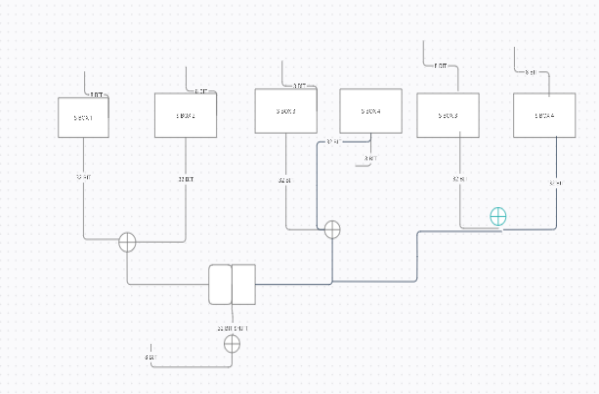

Fig 3.1 Modified blowfish algorithm

Modified algorithm

1. The plain text of the algorithm is 64 bit.
2. The plaintext is denoted by P.
3. The P is divided into 32 bit and 32 bit which is the subkeys
4. Key generation algorithm is used which gives 48 bit keys.
5. The F' Function is used for xoring the bits
6. The rounds denoting R will be for 12.
7. The substation boxes denoted by S' will be used is 6.
8. The generation of Cipher text of 64 bit.
9. Stop
10. Iterate back to step 2
11. Stop

The data is protected before it is uploaded in the cloud environment. The generated data from the IOT device is regularly taken and blowfish algorithm is used to protect, where it is protected from the intruder.

Case Study: Health care monitoring system

A device is attached to the body of the patient which include sensors detecting body temperature, Blood pressure where frequent data has to be uploaded in the cloud. For providing security to the data we use the blowfish algorithm with changes. The health monitoring system used Arduino board, temperature sensor, light sensor. These sensors will effectively measure the temperature and blood pressure of the patient in the hospitals or can be used in the home too.

S.No	Number of rounds	Blowfish Algorithm	Enhanced Blowfish algorithm
1	2	6.74	6.82
2	4	7.03	7.04
3	6	6.96	6.97
4	8	7.06	7.07
5	12	7.07	7.08

Table 1: Comparison of blowfish with enhanced blowfish

III. RESULT AND DISCUSSION

The graph explains how efficient the enhanced blowfish in terms of rounds and use sub arrays and the substitution boxes.

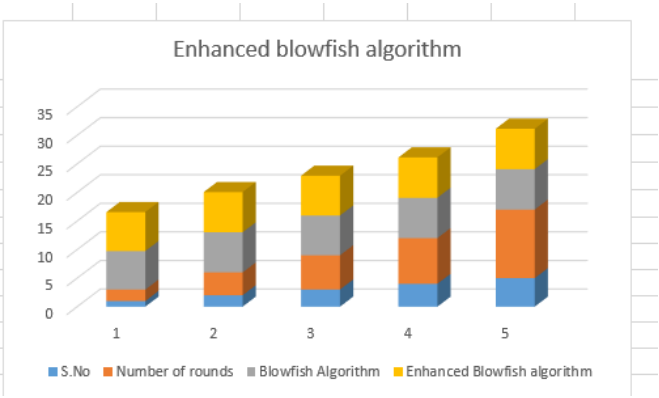

Fig 4.1 Chart for the enhanced blowfish algorithm

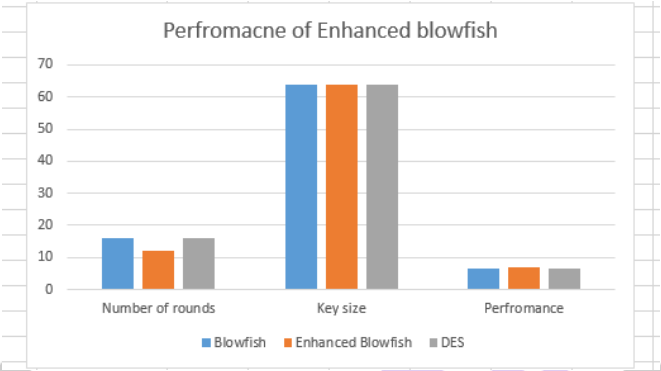

Fig 4.2 Performance of enhanced blowfish

IV. CONCLUSION

The blowfish algorithm used are not secure to protect the data in cloud in terms of performance. The enhanced blowfish algorithm used with give protection to the data stored in the cloud with effective time management and in terms of efficiency. The future of the work will be enhancing the key size and other parameter with respect to the blowfish algorithm.

VI. REFERENCES

1.https://www.tibco.com/reference-center/what-is-the-internet-of-things-iot

2.https://data-flair.training/blogs/features-of-cloud-computing/

3.C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and Cloud Computing, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.031

4. S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.

5.Manju Suresh, M. Neema, "Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things, Procedia Technology, Volume 25,2016,Pages 248-255, ISSN 2212-0173, https://doi.org/10.1016/j.protcy.2016.08.104.

6. S. Ramesh and M. Govindarasu, "An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data," in *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8700-8708, Sept. 2020, doi: 10.1109/JIOT.2020.2998109.

7. Han, Y. Liu, X. Sun and L. Song, "Enhancing data and privacy security in mobile cloud computing through quantum cryptography," *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2016, pp. 398-401, doi: 10.1109/ICSESS.2016.7883094.