ISSN 2581 – 3781

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2018;3(1):22-26

RESEARCH ARTICLE

Fog and Internet of Things Network Security through Blowfish Cipher

B. Usharani

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Guntur, Andhra Pradesh, India

Received: 02-12-2017; Revised: 25-12-2017; Accepted: 20-01-2018

ABSTRACT

The data are stored and accessed in a cloud from the remote server with the help of services provided by cloud service providers. Security is a major issue as the data are transmitted to the remote server through the internet. Encryption is a better solution to secure the information when storing data at remote servers. Fog computing is evolved to overcome the security issues in cloud. Still, there are some data security issues in fog computing. An encryption algorithm plays a key role in the cloud security. Network-based intrusion prevention system is used to detect threats in real time. To provide a secure data access in cloud, advanced encryption techniques can be used for storing and retrieving data from cloud. Furthermore, proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data. The Blowfish encryption can never be hacked. In this paper, Blowfish cipher technique is implemented for the security to fog of internet of things network.

Key words: Blowfish, cipher techniques, fog, internet of things, network security

INTRODUCTION

As the number of devices connected to internet increases, there would be definitely a problem in storage and information retrieval process. Fog computing has been introduced overcome the security issues in the cloud computing. Huge amount of data produced by internet of things (IoT) devices and storing data into cloud and retrieving is highly difficult. Hence, fog has been introduced. IoT had led evolution to the fog computing because of the increased number of devices producing massive amount of data. In cloud computing, there are many security issues as of man in the middle attack and even the encryption of data is not safe method for cloud. It does not identify the difference between user and attacker. It does not concentrate on the security of the data. Cloud provides various services for storing and accessing of the data in which the major problem is that failure to provide security for the data against attackers. It is not providing any level of assurance to the user about the security of the data. Hence, developing a more secure cloud is not enough because there would be continuous attacks happening on the cloud, and there are chances that the data would be leaked or it might be lost forever. Hence, fog computing came into existence which is considered to be the most secure form of data storage. Hence, in this, we are trying to achieve more security at the level of fog by introducing encryption to the data using the Blowfish encryption standard algorithm technique. The paper introduces Blowfish algorithm in the fog environment, so whenever user sends data to fog for storing in the cloud, the fog will encrypt the data and send it to the cloud. Moreover, whenever user requests for the data, the encrypted data travel from cloud to fog and fog to end user, and the data will be decrypted at end user.

FOG COMPUTING [FIGURE 1]

In cloud computing concept, all the data produced from the users will be directly stored into the cloud and then it is analyzed with massive warehouses with analytics going on it and then decisions are made to act on data, and eventually, notifications are pushed to act on those decisions. In fog computing, the users will be notified what are the actions that are needed to be taken on the data and then analytics are applied on the received data and

Address for correspondence:
B. Usharani,
E-mail: ushareddy.vja@gmail.com

stored it into the cloud. Fog computing is said to be an extension of the cloud but not a replacement of it. As the number of the devices connected to the internet has been increasing at rapid speed, and even advancement in the IoT has led this number to increase drastically [Figure 2].

IoT devices interact with fog nodes only when they need to offload a processing or storage request. Any other interactions would not be considered as part of the fog environment as such communications would happen as part of the network. These fog nodes interact with each other when they need to effectively manage network resources or to manage network itself. They may even operate in distributed manner to perform a specific task. To secure communications in a fog computing environment, the following communications between these devices are to be secured:

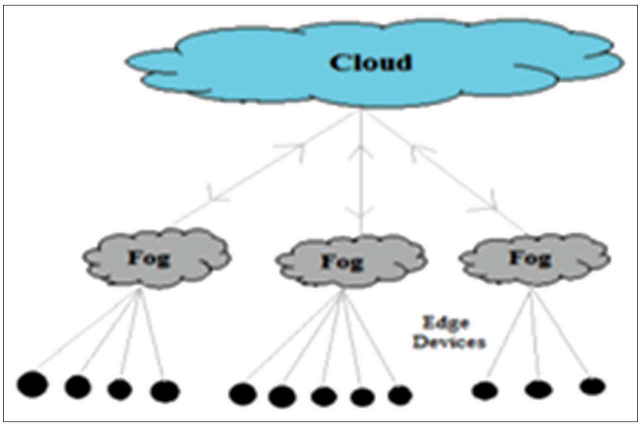

Figure 1: Fog computing architecture

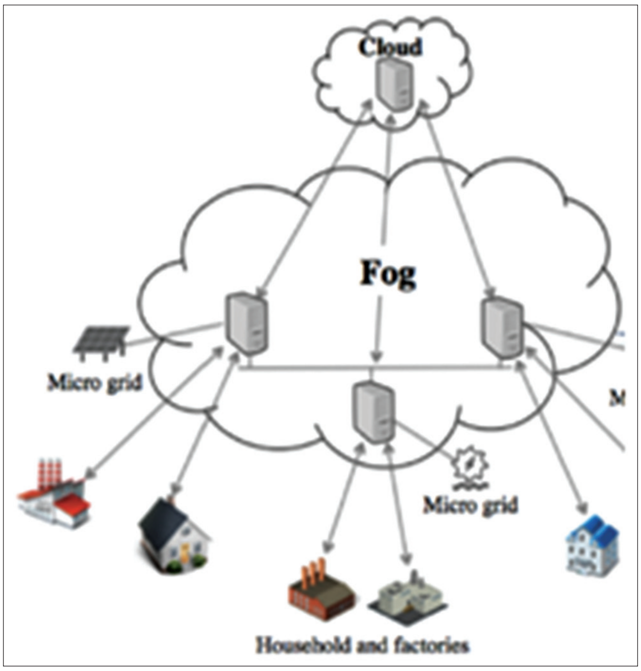

Figure 2: An example for IOT based on fog computing

1. Communications between constrained - IoT devices and fog nodes and
2. Communications between fog nodes.

Usually, an IoT device can initiate communication with any of the fog nodes in the fog network requesting for a processing or storage requirement.

RELATED WORK

Alrawais *et al.* discussed the security and privacy challenges of fog computing in IoT environments. They discussed how to use fog computing to improve the security and privacy issues in IoT environments. In addition, Hong *et al.* evaluated the programming model for large scale and latency sensitive IoT applications exploiting the fog computing platform. They studied the model with a camera network and connected vehicle applications and showed the efficient role of fog computing in IoT. Al Faruque and Vatanparvar proposed a software-defined network based on vehicle *ad hoc* networking supported by fog computing. The proposed architecture solves many issues in vehicle *ad hoc* networks by rising the connectivity between vehicles, vehicle-to-infrastructure, and vehicle to base station while integrating fog computing to decrease latency and provide resource utility. Koo and Hur proposed a deduplication scheme for encrypted data.

CIPHER TECHNIQUES

The original message is called as the plain text. The coded message is known as ciphertext. The process of converting plain text to ciphertext is known as encryption or enciphering.

Cryptographic algorithms and protocols are divided into four categories:

1. Symmetric encryption
2. Asymmetric encryption
3. Data integrity algorithms
4. Authentication protocols.

Network and Internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information. A logical information channel is established by defining the route through the internet from source to destination by the use of communication protocols such as transmission control protocol/internet protocol by the sender and receiver.

Encryption key is used in conjunction with the transformation to scramble the message before transmission and unscramble it on receiver side.

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. Symmetric encryption transforms plain text into ciphertext using a secret key and encryption algorithm.

$$E(K,X) \qquad (1)$$

Symmetric encryption of plain text X using secret key K.E. is the encryption algorithm applied on the plain text and key to transform to a ciphertext. The process of converting ciphertext to plain text is known as decryption or deciphering. In the symmetric encryption, using the same key that is used for encryption and a decryption algorithm, the plain text is recovered from the ciphertext.

$$D(K,Y) \qquad (2)$$

Symmetric encryption of ciphertext Y using secret key K.D. is the decryption algorithm applied on the ciphertext and key to recover original message. With the message X and the encryption key as input, the encryption algorithm forms the ciphertext $Y=(Y_1,Y_2,Y_3,\ldots\ldots Y_n)$.

$Y=E(K,X)$

With the cipher message Y and the decryption key as input, the decryption algorithm forms the plain text

$X=D(K,Y)$

Security of an encryption scheme depends on the length of the key.

BLOWFISH CIPHER TECHNIQUE

Blowfish is an encryption algorithm that can be used as a replacement for the data encryption standard (DES) or International Data Encryption Algorithm (IDEA) algorithms. It is a symmetric or conventional block cipher that uses a variable-length key, from 32 bits to 448 bits. Blowfish uses a 64-bit block size and a key length of any size from 32 bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It uses fixed S-boxes [Figure 3].

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern. The secret key is then XORed with the P-entries in order (cycling the key if necessary). A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P1 and P2. The ciphertext is then encrypted again with the new subkeys, and P3 and P4 are replaced by the new ciphertext. This continues replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4 KB of data is processed.

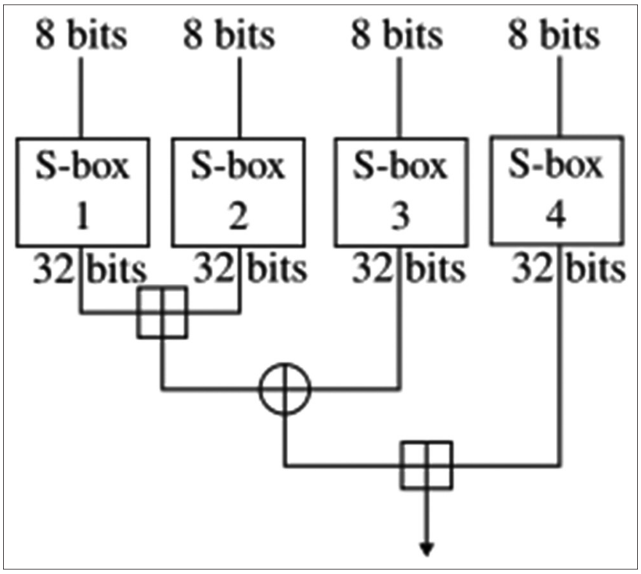

Figure 3: S-box structure

a. Blowfish flowchart
b. Blowfish data encryption technique [Figures 4 and 5].

Blowfish uses 16 rounds. Each round consists of key-dependent permutation and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

PROPOSED SYSTEM [FIGURE 6]

By selecting the cloud services, the users are able to store their local data in the remote data server. The data stored in remote data center can be accessed or managed through the cloud services provided by the cloud service providers. Hence, the data stored in a remote data center for data processing should be done with utmost care. To achieve more security at the level of fog, the proposed system introduces encryption to the data using the Blowfish encryption standard algorithm technique. The proposed system introduces Blowfish algorithm in the fog environment, so whenever user sends data to fog for storing data in the cloud, the fog will encrypt the data and send it to the cloud. When user requests data,

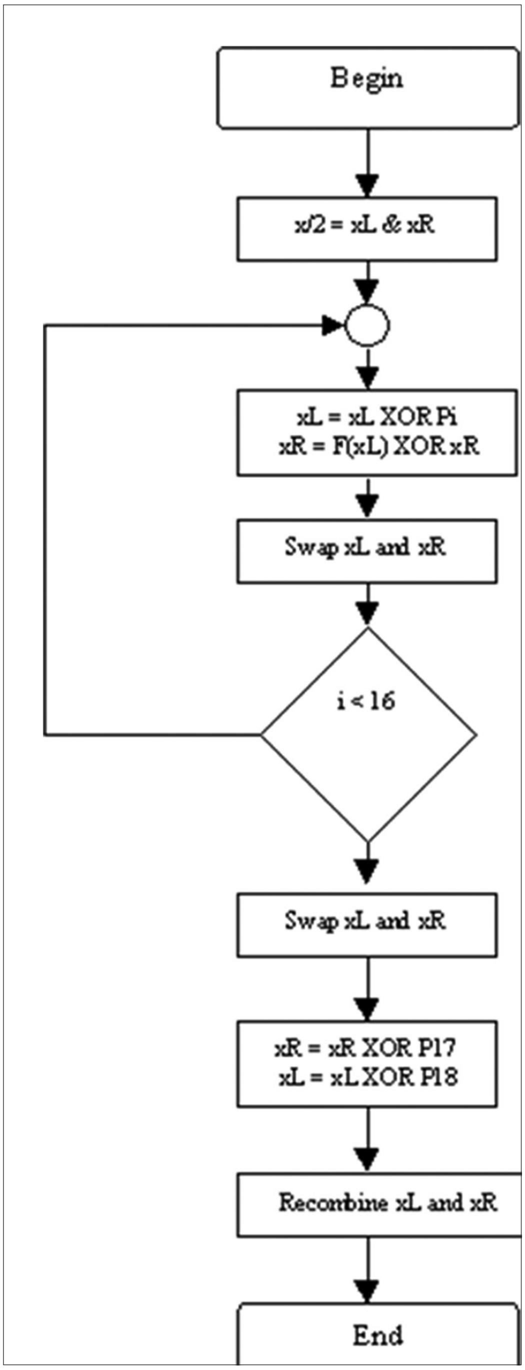

Figure 4: Flowchart for Blowfish algorithm

the encrypted data travel from cloud to fog and fog to end user, and the data will be decrypted at end user. It is very difficult to hack the Blowfish algorithm. The proposed system presents security to the network or transmission data by Blowfish algorithm in fog computing, which makes the data of the end user more secured while the data are traveling from cloud to fog or fog to cloud.

CONCLUSIONS

Conventional methods of encryption work on letters, so their usage has been declined for blocks. Blowfish algorithm is the replacement of DES and IDEA algorithms in the cipher techniques. The advantage of Blowfish is the variable length of the key size, i.e., from 32 to 448 bits. Blowfish is accepted as a strong encryption algorithm and fast cipher technique. The strength of the Blowfish is the generation of the subkeys, and it is very difficult to the attacker because it is very complex to identify a key, i.e., for each key generation, the encryption routine runs 522 times. In this paper, Blowfish is implemented in fog network for IoT devices. An additional layer of security is added for data retrieval; this makes the intruder very difficult to hack the data.

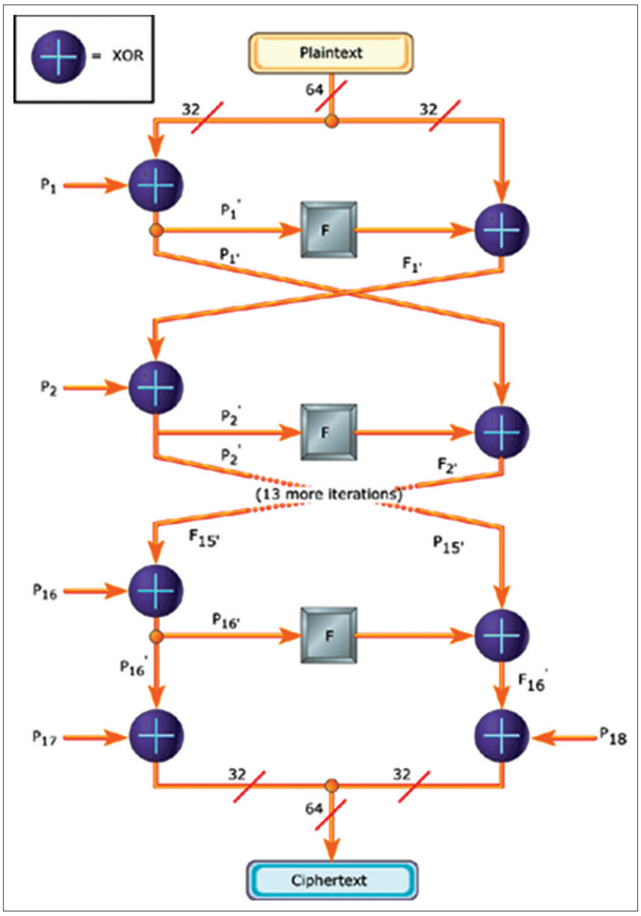

Figure 5: Encryption procedure in Blowfish cipher algorithm

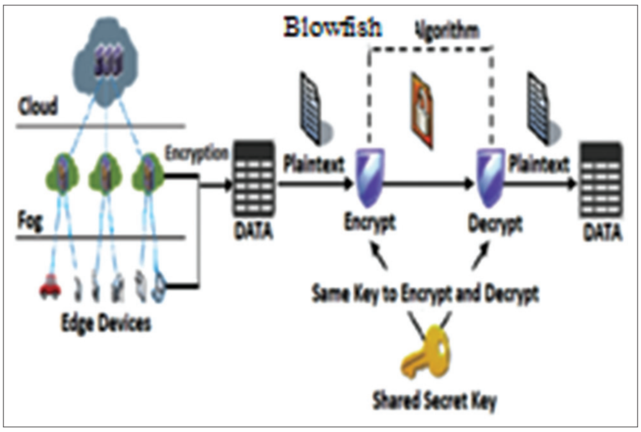

Figure 6: System architecture

AQ4

REFERENCES

1. Shen Z, Li L, Yan F, Wu X. Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation. Vol. 1; 2010. p. 942-5.
2. Pearson S, Benameur A. Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference; 2010. p. 693-702.
3. Bhadauria R, Sanyal S. A survey on security issues in cloud computing and associated mitigation techniques. Int J Comput Appl 2012;47:47-66.
4. Mohammed EM, Ambelkadar HS. Enhanced Data Security Model on Cloud Computing, 8th International Conference on IEEE publication; 2012. p. 12-7.
5. Wang L, von Laszewski G, Kunze M, Tao J, Fu C, He X, *et al*. Cloud computing: A perspective study, new generation computing. Adv Distribut Inf Processing 2010;28:137-46.
6. Khairnar S, Borkar D. Fog computing: A new concept to minimize the attacks and to provide security in cloud computing environment. Int J Res Eng Technol 2014;3:124-7.
7. Stojmenovic SIT, Wen S. The Fog Computing Paradigm: Scenarios and Security Issues. Vol. 02. Federated Conference on Computer Science and Information Systems, ACSIS; 2014.
8. Dhande NS. Fog computing: Review of privacy and security issues. Int J Eng Res General Sci 2015;3:864-8.
9. Stolfo SJ, Salem MB, Keromytis AD. Fog computing: Mitigating insider data theft attacks in the cloud" IEEE; 2014.
10. Nag KS, Bhuvaneswari HB, Nuthan AC. Implementation of Advanced Encryption Standard-192 Bit Using Multiple Keys. Vol. 1, 7. Research and Technology in the Coming Decades (CRT 2013), National Conference on Challenges; 2013. p. 27-8.
11. Sumitra G. Comparative analysis of AES and DES security algorithms. Int J Sci Res Publ 2013;3:1-5.
12. Singh S, Maakar SK, Kumar S. Enhancing the security of DES algorithm using transposition cryptography techniques. Int J Adv Res Comput Sci Soft Eng 2013;3:464-71.
13. Kruti RS, Gambhava B. New approach of data encryption standard algorithm. Int J Soft Comput Eng 2012;2:322.
14. Karthik S, Muruganandam A. Data encryption and decryption by using triple DES and performance analysis of crypto system. Int J Sci Eng Res 2014;2:24-31.
15. Sachin M, Kumar D. Implementation and analysis of AES, DES and triple DES on GSM Copyright. Int J Comput Sci Netw Security 2010;10:298-303.
16. Singh G, Supriya. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. Int J Comput Appl 2013;67:33-8.
17. Jain R, Jejurkar R, Chopade S, Vaidya S, Sanap M. AESalgorithm using 512 bit key implementation for secure communication. Res J Appl Sci Eng Technol 2014;8:2116-20.
18. Saraf KR, Jagtap VP, Mishra AK. Text and image encryption decryption using advanced encryption standard. Int J Emerg Trends Technol Comput Sci 2014;3: 118-26.
19. Advanced Encryption Algorithm and its Implementation. Available from: https://www.en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Last accessed on 2015 Jul 07].

Author Queries???
AQ4: Kindly cite references 1-19 in the text part