International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 860-862 www.ijaem.net ISSN: 2395-5252

On Sharing Secrets: A Multi-Layer Approach To Reduce Cyber-Security Risks Using Fog Computing

Tejas Wadekar, Tejal Patil, Devyani Desai, Prof.K.S.Munde

Tejal Patil, Computer Department, PVPIT Bavdhan, Pune.
Tejas Wadekar, Computer Department, PVPIT Bavdhan, Pune.
Devyani Desai, Computer Department, PVPIT Bavdhan, Pune.
Prof.K.S.Munde, Computer Department, PVPIT Bavdhan, Pune.

Submitted: 05-04-2022 Revised: 16-04-2022 Accepted: 19-04-2022

ABSTRACT - In order to reduce the burden of maintaining big data, more and more enterprises and organizations have chosen to outsource data storage to cloud storage providers. This makes data management a critical challenge for the cloud storage providers. Cloud computing is the long dreamed vision of computing as a utility. Besides all the benefits of the cloud computing security of the stored data need to be considered while storing sensitive data on cloud. Cloud users cannot rely only on cloud service provider for security of their sensitive data stored on cloud.

Key Words: Security, Fog-Computing, AES Algorithm, Encryption

I. INTRODUCTION

In order to reduce the burden of maintaining big data, more and more enterprises and organizations have chosen to outsource data storage to cloud storage providers.This makes data management a critical challenge for the cloud storage providers.Cloud computing is the long dreamed vision of computing as a utility.Besides all the benefits of the cloud computing security of the stored data need to be considered while storing sensitive data on cloud.Cloud users cannot rely only on cloud service provider for security of their sensitive data stored on the cloud.

II. ALGORITHAMS

1. AES Algorithm

a. Encryption

You take the following AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state array.

These steps involve four types of operations called:

1. Sub-Bytes
2. Shift-Rows
3. Mix-Columns
4. Xor-Round Key

b. Decryption

As you might expect, decryption involves reversing all the steps taken in encryption using inverse functions:

1. InvSub-Bytes
2. InvShift-Rows
3. InvMix-Columns

Operation in decryption is:

1. Perform initial decryption round:

• Xor-Round Key
• InvShift-Rows
• InvSub-Bytes

2. Perform nine full decryption rounds:

Xor-Round Key
InvMix-Columns
InvShift-Rows
InvSub-Bytes

3. Perform final Xor-Round Key

2. SHA 512 Algorithm

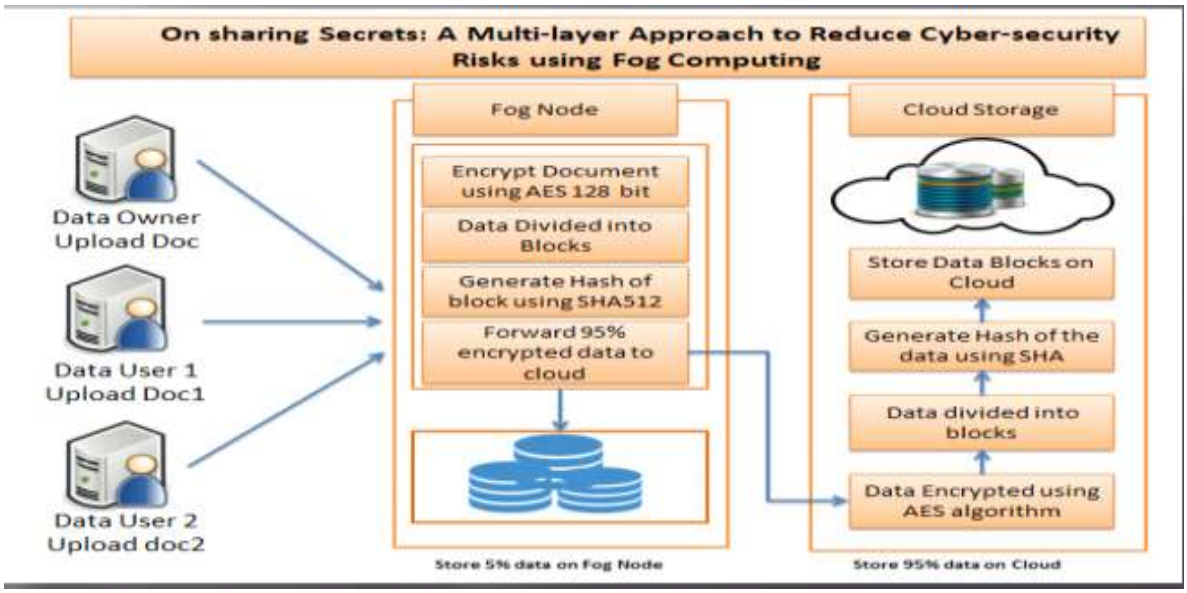
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 860-862 www.ijaem.net ISSN: 2395-5252

a. Append Padding Bits and Length Value: This step makes the input message an exact multiple of 1024 bits:
b. Initialize Hash Buffer with Initialization Vector: Before we can process the first messageblock, we need to initialize the hash buffer with IV, the Initialization Vector
c. Process Each 1024-bit (128 words) Message Block Mi: Each message block is taken through 80 rounds of processing.
d. Finally: After all the N message blocks have been processed, the content of the hash buffer is the message digest.

3. SYSTEM DESIGN

In proposed system we are making use of fog computing to overcome the problem with the semi trusted cloud service provider, while user will upload the file and file will be uploaded on the fog node, here the fog node performs the encryption of the uploaded file and then divide the file into blocks and hash of the data will be computed. And only the 5% of data will be stores on the fog device then the remaining 95% data will be forwarded to the cloud on the cloud we again going to perform encryption of the data to make it more secure and the data will be divided into the blocks and stored on the cloud with the computing the hash of the data. It maintains the privacy of the stores data due to double encryption of the data and also the file is stored on two different locations so if csp tries to access the filethen he cannot get whole data.

- Proof of Ownership Data Owner uploads document, the document will be uploaded on the fog node.
- Data Encryption model Uploaded file then encrypted using the 16 byte AES key which is entered by the user at the time of Registration.
- Data block Generation The encrypted file now divided into the blocks. The blocks are of the same size.
- Data Block Hash Generation The Hash will be computed of the each block. We Maintains the Hash of file data and block of file data as reference and used at the time of downloading. Both the fog and the clouds will follow this step for storing of data.



III. CONCLUSIONS

We propose system that provides double security i.e. by using double encryption than existing system. By analysing the security we can substantiate that our planned proposal are provably protected by encrytpting the file twice i.e. one at the time when data owner uploaded the file to the fog node the fog node performs the encryption of the uploaded file and when we forward the data to the cloud on the cloud we again going to perform encryption of the data to make it more secure. Here we used an AES 128 bit for the encryption og the file.

IV. ACKNOWLEDGEMENT

I have great pleasure in presenting report on **On sharing Secrets: A Multi-layer Approach to Reduce Cyber-security Risks using Fog Computing.** Completing a task is never a one-man effort. It is often a result of invaluable contribution of a number of individuals in direct or indirect manner. I would like to express deepest

appreciation towards **Prof.Dr.C.M.Sedani**, Principal Padmabhooshan Vasantdada Patil Institute of Technology,Bavdhan Pune – 21 and **Prof.S.V.Bodke**, HOD Computer Department, whose invaluable guidance supported me in completing this report.

I am profoundly grateful to **Prof.K.S.Munde** for his expert guidance and continuous encouragement throughout to see that this project report rights its target since its commencement to its completion.

At last I want to express my sincere heartfelt gratitude to all the staff members of Computer Engineering Department who helped me directly or indirectly during this course of work.

REFERENCES

[1]. Kavyashree M B1, Shoba M2, Nagashree C3, Nischitha D Raj4, "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing", International Research Journal of Engineering and Technology(IRJET), 2020.

[2]. Rose K Johney; Elizabeth Shelry; K R Remesh Babu, "Enhanced Security through Cloud-Fog Integration", International Conference on Communication and Electronics Systems (ICCES), 2019.Gyusoo Kim and Seulgi Lee, "2014 Payment Research", Bank of Korea, Vol. 2015, No. 1, Jan. 2015.

[3]. Yang Li; Tian Wang; Guojun Wang; Junbin Liang; Hongyu Chen, "Efficient Data Collection in Sensor-Cloud System with Multiple Mobile Sinks", Asia-Pacific Services Computing Conference, 2016.

[4]. Jonathan Chase ; Rakpong Kaewpuang ; Wen Yonggang ; Dusit Niyato ,"Joint virtual machine and bandwidth allocation in software defined network (SDN) and cloud computing environments",IEEE, 2014.