Securing Cloud Data Using ABE Under Key Exposure For Outsourced Decryption

[1]Pratiksha Mirgude, [2]Aarti Zagade, [3]Priti Chavan, [4]Harshada Gaikwad, [5]Prof.Mangal Kotkar,
[1,2,3,4]U.G.Students , [5]Assistant Professor
[1]Department of Computer Engineering,
[1]Dhole Patil College of Engineering , Kharadi , Pune, India

Abstract : The intruders acquire the keys through backdoor, bribe, or coercion. Once the key is exposed, the only way to protect the data is by limiting access to the cipher text. The most common and strongest algorithms are already defined, the security lies into keys. Although the key is exposed we can still secure our data by dividing and distributing the cipher blocks on the multiple administrative domains so that it becomes very difficult for the intruder to gain access, assuming that intruder cannot compromise all the cipher blocks stored on the server. In the existing scheme, the data is stored on a single server so the attacker can easily get access to the user's confidential data by acquiring a key. In this paper, we propose a method i.e. dubbed Fortress method initially known as Bastion method which guarantees data security even if the key is Exposed, unless and until the attacker gets access to all the cipher blocks. Fortress method gives less than 5% overhead compared to existing secure encryption methods. We are additionally using the reverse circle cipher algorithm and ABE(attribute-based encryption) with outsourced decryption to increase efficiency and reduce decryption cost increased by ABE.

***IndexTerms* - Key Exposure, ABE, Outsourced Decryption.**

I. Introduction

Over the last few years, it has been observed that there is a massive increase in hacking[14] and other malicious activities. So it's our prime duty to secure our digital data as the data is a precious asset[14] whether it is financial information and payment details, contact information, private pictures or any other sensitive data. The World has witnessed too many attacks by the attackers[8][9] who steal victims confidential data. Sony pictures hack and i-cloud leak are some of the examples in which personal information about employees and their families, e-mails between employees, copies of unreleased Sony films and other sensitive data[8] was hacked by the hacker in sony pictures whereas in i-cloud attack, many private photos of celebrity almost 500 especially of women were posted on social media[9] such attacks causes really bad impact on victim as well as on society. If proper measures are not used, the attacker can read obstruct or steal personal information. the intrusion can range from mild to severe attacks on data depending on the intention of the intruder. He can circulate or resell the data using for unlawful purposes also.it can cause a devastating impact on an individual who is affected.so we suggest that CSP should encrypt their digital assets as encryption is needed to protect the data confidentiality as it is stored on the internet during transmission. for encryption, the key and algorithm are required. The most common and strongest algorithm is already defined, so the security lies between the key used. The encryption key is sent or exchanged secretly over the network. The attacker tries to acquire the key through backdoor or coercion. Once the key is exposed, the only way to protect the data is by limiting access to the cipher blocks.

In the existing cryptographic security algorithm, the major drawbacks of DES, AES, and Rijndael[11] are fixed Key size which is 56 bit, 128 bit, 192 bit and 256-bit keys. But still we can increase the strength by using an algorithm[2] in which keys size is the size of plaintext or the key size vary according to the text size.

In this paper, we provide data security even if the key is exposed and the attacker has access to the major portion of data but not the whole data. Hackers can acquire keys from many different sources mentioned in[7]. Here we are additionally using ABE to increased efficiency and outsourced decryption to reduce users device load.

To counter such attacks, we proposed a method called as dubbed fortress initially known as bastion method[1] which fortifies the data and ensures that data cannot be recovered as long as the attacker cannot gain access to at most all but two ciphertext blocks even if the key is exposed. The fortress method works by combining any encryption method with a linear transform. Fortress is similar to AONT[1] but it is more efficient as than AONT.

II. Related Work

AES and DES are the symmetric encryption algorithm that runs many passes[11] the same plaintext like DES runs 16 round passes and AES runs 10,12,14 round for processing 128, 192, 256-bit keys. whereas the RSA and EL Gamel are asymmetric encryption algorithm which is more suitable for mobile system and are more secure[12]. RSA is the most popular asymmetric encryption technique which decrypt the data by using only one block which uses the method cipher-block-chaining mode(CBC)[13]. The increased in the decryption cost with the increased in the file size was the major drawback of ABE[3] so we recommended to used an outsourced server for the decryption process to reduce the users overhead.

A similar method to the fortress is AONT where AONT is preprocessing step means it is the process before data encryption. It was used to reduce key-search attacks to decrypt the original message. AONT requires all the blocks without all the blocks you cannot get the original message[4]. AONT rounds are sequential, AONT requires two rounds of block cipher encryption: one for preprocessing the data and another for actual encryption of data.

III. Our Contribution and Motivation

We propose a very efficient method, known as the dubbed fortress method. In this method, the user's data remains still secure even if the key is exposed by the intruder and has access to the majority portion of the data. The fortress method is similar to AONT but it is more efficient than AONT and can combine with any other encryption techniques. The fortress method improves 50% more performance than the current secure key exposure technique.

The fortress method is a postprocessing method i.e. this method is applied after the data encryption. Fortress method consist of a square matrix such that all the diagonal elements are set to 0 and the remaining are set to 1.block cipher techniques like AES & DES can be vulnerable to attacks[2] since they have fixed key size and relatively small key size, to increase key size or use of longer key in AES will increase the computational cost. we suggest a reverse circle cipher method as it is efficient and requires less time as well as memory. Reverse circle cipher[2] uses variable key length and it can be as long as the plaintext size. Along with the Reverse cipher circle, we also suggest ABE scheme to increase more security. Due to CBC (Cipher-Block-Chaining) and method we propose, the encrypted message after applying the fortress method is divided into blocks and distributed on the multiple administrative domains. To reduce the load of decryption and to decrease the users overhead created by ABE we recommend an Outsourced server. Here even if the key is exposed the attacker cannot compromise every server to get all the data as it is a very difficult task.

IV. Proposed Methodology

In this section, we proposed our methodology dubbed fortress method which ensures data security even if the key is exposed. The working of our method is as follows in the fig given below. The ABE method is applied on the user's metadata i.e. on the user's file content and the key is generated using a unique key generation module. The key generated is as long as the plaintext size of users data. And along with the key generation the reverse circle cipher is applied on it. By using ABE the data gets encrypted. After the encryption, the data is sent forward to the fortress method for processing the data as the fortress is a postprocessing method. The Fortress method consist of an n×n matrix where ai,j = 0 if i = j and ai,j = 1 if i ≠ j. This n×n matrix is linearly transformed with ciphertext as shown in figure 2. This processed data is then divided into smaller files and these files are distributed across multiple administrative domains. The files on the different servers are useless until and unless all of them are re-combined and the inverse of Fortress is applied.

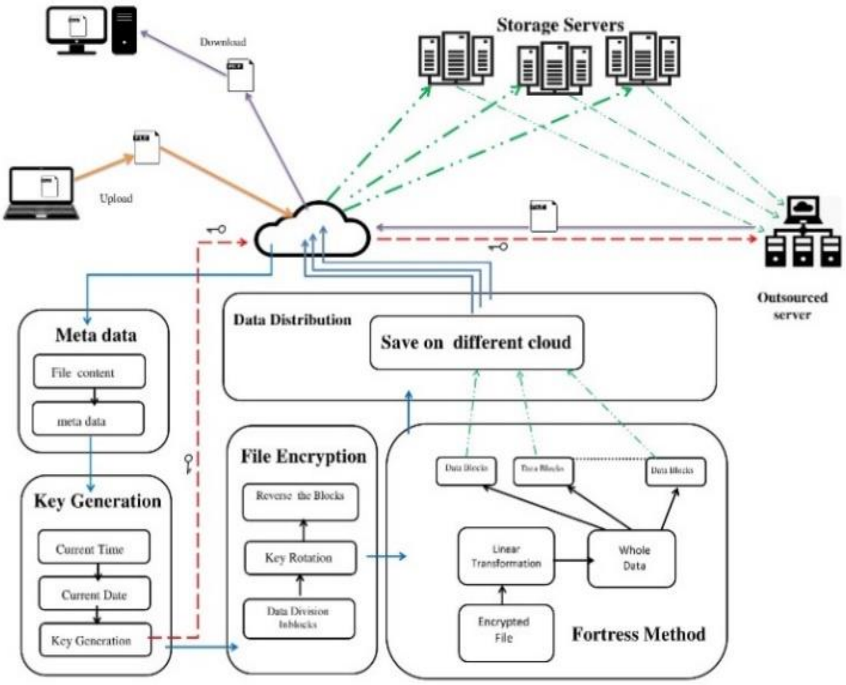

Figure 1 System Architecture

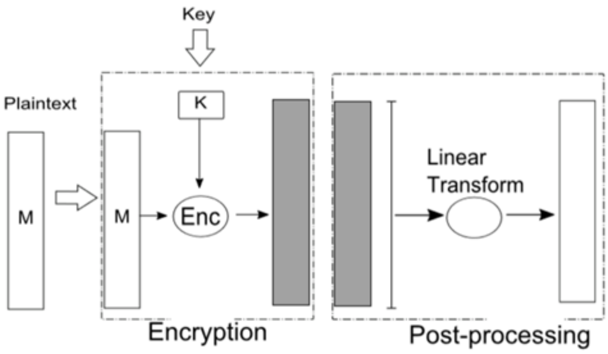

Figure 2 Fortress Method

During the file sharing, the main original file is requested from an outsourced server, the outsourced server recollects all the distributed files from multiple administrative domains and recombines them. after recombining the files the inverse of the fortress is applied and by using the unique key the data is decrypted. And then it is sent to an authorized party in original plaintext. To increase the performance and to reduce the ABE drawback we have used an outsourced server.

V. Proposed Methodology Result and Discussions

The Fortress method is compared with the existing AONT method[1] which shows that it has improved performance by 50% more. [1] Evaluated with respect to different block sizes and found that there was negligible performance decrease. By using the Reverse Circle cipher algorithm[2] and ABE we are able to increase more efficiency and data security. To overcome the ABE overhead problem we have introduced an outsourced server for data decryption.

VI. Conclusion

Hence, We are able to increase efficiency and data security by combining the above-discussed methods. Data confidentiality is maintained even if the key is exposed and as long as the attacker has access to all but two cipher blocks. We can increase more security by re-encrypting and re-applying the fortress method and distributing them again on different servers, assuming that attackers cannot hack all the servers and get access to all the data, recombine them, apply the inverse of fortress method, and an algorithm applied for encryption and decryption.

References

[1] G. O. Karame, C. Soriente, K. Lichota and S. Capkun, "Securing Cloud Data under Key Exposure," in IEEE Transactions on Cloud Computing. doi: 10.1109/TCC.2017.2670559.

[2] Isaac, Ebenezer & Isaac, Joseph & Visumathi, J. (2013). Reverse Circle Cipher for personal and network security. 346-351. 10.1109/ICICES.2013.6508354.

[3] J. Li, Y. Wang, Y. Zhang and J. Han, "Full Verifiability for Outsourced Decryption in Attribute Based Encryption," in IEEE Transactions on Services Computing. doi: 10.1109/TSC.2017.2710190.

[4] Desai A. (2000) The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search. In: Bellare M. (eds) Advances in Cryptology — CRYPTO 2000. CRYPTO 2000. Lecture Notes in Computer Science, vol 1880. Springer, Berlin, Heidelberg.

[5] National Bureau of Standards, NBS FIPS PUB 81, "DES modes of operation," U.S Department of Commerce, 1980.

[6] Rivest R.L. (1997) All-or-nothing encryption and the package transform. In: Biham E. (eds) Fast Software Encryption. FSE 1997. Lecture Notes in Computer Science, vol 1267. Springer, Berlin, Heidelberg.

[7] Wikipedia, "Edward Snowden," http://en.wikipedia.org/ wiki/Edward_Snowden#Disclosure.

[8] Wikipedia, "Sony_Pictures_hack," https://en.wikipedia.org/wiki/Sony_Pictures_hack.

[9] Wikipedia, "ICloud_leaks_of_celebrity_photos," https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos

[10] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Public Key Cryptography (PKC '11), pp. 53-70, 2011.

[11] Matt Bishop, "Computer Security: Art and Science", Pearson Education, pp. 270-300, 2005.

[12] Vigila, S and Muneeswaran, K. Implementation of text based cryptosystem using Elliptic Curve Cryptography. First International Conference on Advanced Computing. ICAC 2009. December 2009.

[13] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[14] Star certification official curriculum, "star cyber secure user", 2018.