IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Novel Approach for Achieving Cloud Data Confidentiality Under Key Exposure

G. Sravani[1*], G.V. Padma Raju[2]

[1] Department of Computer science and Engineering SRKR Engineering College, Bhimavaram, India
[2] Department of Computer science and Engineering SRKR Engineering College, Bhimavaram, India

Available online at: www.ijcseonline.org

Accepted: 22/Jun/2018, Published: 30/Jun/2018

Abstract - An attacker will break cloud data confidentiality by abusing cryptographic keys utilizing secondary passages in cryptographic code. The main plausible measure is restricting assaulter from getting to the cipher text, when cryptography mystery key is uncovered. Existing cryptography plans can't protect cloud information classification underneath key presentation as despite everything they bargain at one figure square. Bastion, a proficient system is suggested that jam cloud data confidentiality against an assaulter who knows about the cryptography key and approaches the encoded information. We have a tendency to dissect Bastion's security and we survey its execution with existing plans in parts of security, stockpiling and calculation.

Keywords - assaulter, key exposure, confidentiality

I. Introduction

These days, distributed storage has turned out to be one of the chief choices for people and undertakings to store their enormous size of data. It will abstain from conferring enormous capital of clients for getting and overseeing equipment and programming [13]. Despite the fact that the benefits of distributed storage are enormous, security contemplations wind up essential difficulties for distributed storage. One noteworthy worry on distributed storage security is about the uprightness of the cloud information. Since customers may lose their cloud information control and information misfortune may occur in distributed storage, it is normal for customers to question whether their information is accurately put away in cloud or not.

The principal issues in cloud data security incorporate data protection, data assurance, data accessibility, data area, and secure transmission. Dangers, data misfortune, benefit interference, outside malignant assaults and multi residency issues are the security challenges incorporated into the cloud. [4] Cloud information security is a standout amongst the most hindrances to its appropriation and it is trailed by issues including consistence, protection, trust, and legitimate issues. Consequently, one of the vital objectives is to keep up security and trustworthiness of information put away in the cloud on account of the basic idea of Cloud processing and enormous measures of complex information it conveys. The clients worry for security ought to be corrected first to make cloud condition dependable, with the goal that it helps the clients and undertaking to embrace it on enormous scale [1]. Information secrecy is likewise an essential angle from client's perspective as they store their private or secret information in the cloud. Confirmation and access control systems guarantee information privacy. The information privacy could be tended to by expanding the cloud unwavering quality and reliability in Cloud processing. In this way security, uprightness, protection and privacy of the put away information on the cloud ought to be viewed as and are imperative necessities from client's perspective.

In this paper, information classification against a foe which knows the encryption key and which approaches ciphertext squares was considered. The foe can secure the encryption key either by utilizing indirect accesses in the key-age programming or by trading off the gadgets which stores the keys (e.g., at the client side or in the cloud). Bastion accomplishes information privacy by joining the utilization of standard encryption capacities took after by a productive straight change. Bastion convention imparts similitudes to the approach of win or bust change. AONT isn't an encryption mode yet it is utilized as preprocessing advance to encryption. AONT is for the most part utilized against savage power assaults. [5] AONT accomplishes information privacy under key introduction until and except if the enemy can't access no less than one figure content square. Be that as it may, it requires two rounds of encryption which increments extensive overhead and calculation time.

Above all else, applying the typical determination of key denial under key introduction isn't sensible. This can be because of, at whatever point the customer's mystery key is uncovered, the shopper needs to fabricate a substitution attempt of open key and mystery key and recover the authenticators for the customer's data aforesaid kept in cloud [6]. The strategy includes the downloading of entire data from the cloud, producing new authenticators, and re-transferring everything back to the cloud, which might all be repetitive and unwieldy.

Additionally, it can't consistently ensure that the cloud gives genuine data once the customer recovers new authenticators. Furthermore, straightforwardly receiving typical key-advancing system is also not fitting for the new drawback setting. It will bring about recovering the greater part of the specific records squares once the confirmation is gone before. This can bring about a method inconsistent with square less confirmation [7]. The following authenticators can't be aggregative, bringing about deplorably high calculation and correspondence esteem for the capacity evaluating.

II Preliminaries

A) Encryption modes

An encryption mode based on a block cipher F/F^{-1} is given by a triplet of algorithms

∏= (K, E, D) Where,

K The key calculation is a probabilistic calculation which takes as information a security parameter k and yields a key a∈ $\{0,1\}^k$ that indicates F_a and F_a^{-1}.

E The encryption calculation is a probabilistic calculation which takes as information a message x∈ $\{0,1\}^*$, and utilizes F_a and F_a^{-1} as prophets to yield figure content y.

D The decoding calculation is a deterministic calculation which takes as info a figure content y, and utilizations F_a and F_a^{-1} as prophets to yield plaintext x ∈$\{0 , 1\}^*$ if y is substantial or ⊥ if y is invalid.

B) All or Nothing Transformations

An All or Nothing Transformation (AONT) is a productively processable change which maps groupings of information squares to successions of yield hinders with the accompanying properties:

1. Given all the yield obstructs, the change can be proficiently transformed (i.e., the first information can be processed), and

2. Given everything except one of the yield squares, it is infeasible to figure any of the first info squares. The formal linguistic structure of an AONT is given by a couple of polynomial-time calculations

∏= (E, D)

Where, E The encoding calculation is a probabilistic calculation which takes as info a message x∈ $\{0,1\}^*$, and yields a pseudo cipher text y.

D The disentangling calculation is a deterministic calculation which takes as information a pseudo cipher text y, and yields either a message x∈ $\{0,1\}^*$or ⊥ to show that the info pseudo-cipher text is invalid.

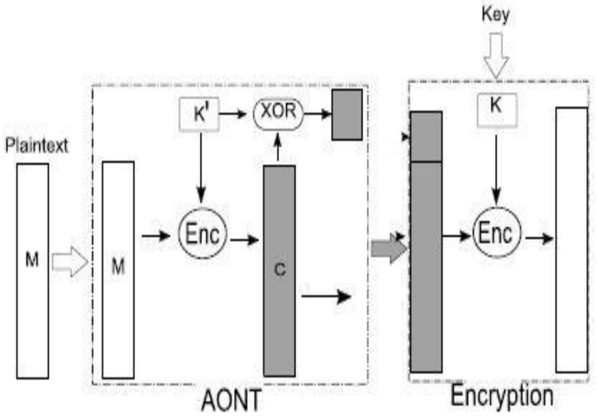


Fig: Current AON encryption schemes require a pre-processing round of block cipher encryption for the AONT, followed by another round of block cipher encryption.

C) Definition and Security Model:

Bastion accomplishes information privacy by consolidating the utilization of standard encryption capacities took after by a productive straight change. Bastion convention imparts similitudes to the approach of win or bust change. Our proposed framework, Bastion is an encryption plot with the accompanying properties. The security of our convention is characterized in two definitions:

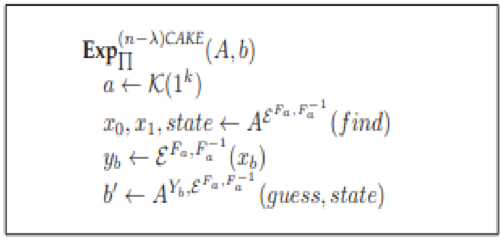
Definition1: Chosen plain text attack(CPA) secure

Adversary does not know the encryption key but has access to all ciphertext blocks by compromising all storage servers.

$$\begin{array}{l}
\mathbf{Exp}_{\prod}^{ind}(A,b) \\
\quad F \leftarrow BC(k,l) \\
\quad a \leftarrow \mathcal{K}(1^k) \\
\quad x_0, x_1, state \leftarrow A^{\mathcal{E}^{F_a, F_a^{-1}}}(find) \\
\quad y_b \leftarrow \mathcal{E}^{F_a, F_a^{-1}}(x_b) \\
\quad b' \leftarrow A(guess, y_b, state)
\end{array}$$

Here, we characterize security through the above definition. The foe approaches all figure content squares in the "discover" organize. Accept that A yields two messages x_0, x_1 and some other state data identified with the outcome. Toward the finish of discover organize, enemy secures the two messages alongside the state data. Amid "Figure" arrange, foe needs to figure which message was the really scrambled one out of the two gained.

Definition2:(n-λ) Cipher text Access under Key Exposure(CAKE) secure
Adversary knows the encryption key and has access to all cipher text blocks but not λ cipher text blocks since it cannot compromise all storage servers.



$$
\begin{aligned}
&\mathbf{Exp}_{\Pi}^{(n-\lambda)CAKE}(A,b)\\
&\quad a \leftarrow \mathcal{K}(1^k)\\
&\quad x_0, x_1, state \leftarrow A^{\mathcal{E}^{F_a,F_a^{-1}}}(find)\\
&\quad y_b \leftarrow \mathcal{E}^{F_a,F_a^{-1}}(x_b)\\
&\quad b' \leftarrow A^{Y_b,\mathcal{E}^{F_a,F_a^{-1}}}(guess, state)
\end{aligned}
$$

The enemy has unlimited access in both "find" and "figure" stages. As foe has unhindered access, it secures the mystery key for encryption amid the "discover" organize. Amid the "Figure" arrange, the enemy can question just (n-λ) inquiries as it can't get to λ figure content squares.

III Proposed Scheme: Bastion

Here we execute Bastion conspire which guarantees information secrecy against a foe that knows the encryption key and approaches the greater part of the ciphertext hinders aside from two.

Bastion accomplishes information privacy by joining the utilization of standard encryption capacities took after by an effective direct change.

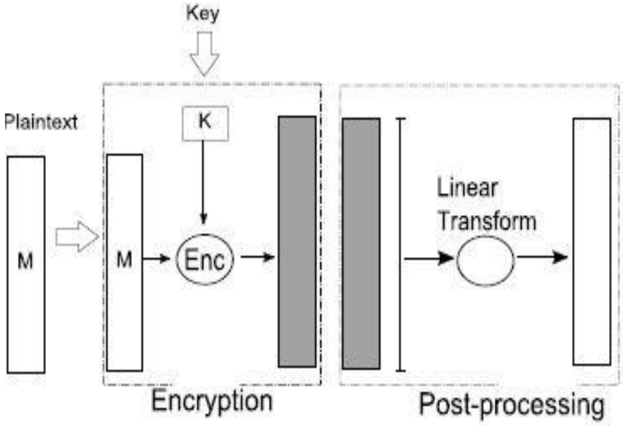
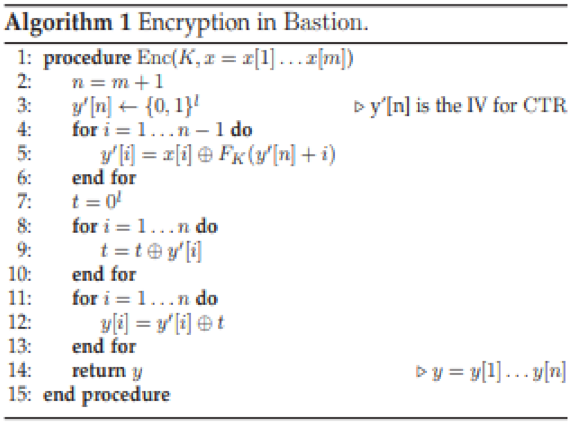


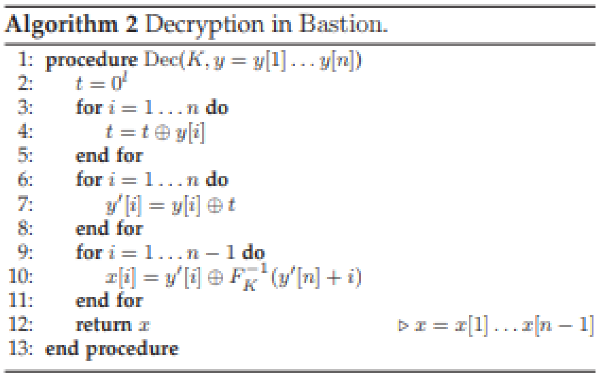
Fig: Bastion first encrypts the data with one round of block cipher encryption, and then applies an efficient linear post-processing to the ciphertext.

Bastion Protocol:
a) The key age calculation yields a key K ∈ {0, 1}^{k} for the basic square figure, on input security parameter k.
b) Bastion Encryption: On contribution of plain content x, Bastion utilizes CTR mode square figure encryption, partitions it into squares x[1], x[2],… x[m],m is odd^2 with the end goal that square size is l^3 .
Set of information squares are scrambled under key K coming about figure content of frame y ′ = y ′ [1],… ..y′ [m+ 1], where y′ [m+ 1] is looked over from {0,1}^{1} .
c)Applying straight change to y ′. Let n=m+1 and A be n-by-n grid with the end goal that a_{ij}=0^l if i=j, generally a_{ij}=1^l.
Figuring y= y ′. A where increases and duplications are AND, XOR activities separately.
d)Bastion Decryption: Bastion figures y ′= y. A^{-1} and decodes y ′ utilizing given key K. (Here A=A^{-1} and A is invertible). The pseudo code of Bastion encryption and decoding is as per the following



Algorithm 1 Encryption in Bastion.

```
procedure Enc($K, x = x[1]\dots x[m]$)
    $n = m + 1$
    $y'[n] \leftarrow \{0,1\}^l$                      ▷ y'[n] is the IV for CTR
    for $i = 1 \dots n - 1$ do
        $y'[i] = x[i] \oplus F_K(y'[n] + i)$
    end for
    $t = 0^l$
    for $i = 1 \dots n$ do
        $t = t \oplus y'[i]$
    end for
    for $i = 1 \dots n$ do
        $y[i] = y'[i] \oplus t$
    end for
    return $y$                                     ▷ $y = y[1] \dots y[n]$
end procedure
```



Algorithm 2 Decryption in Bastion.

```
procedure Dec($K, y = y[1]\dots y[n]$)
    $t = 0^l$
    for $i = 1 \dots n$ do
        $t = t \oplus y[i]$
    end for
    for $i = 1 \dots n$ do
        $y'[i] = y[i] \oplus t$
    end for
    for $i = 1 \dots n - 1$ do
        $x[i] = y'[i] \oplus F_K^{-1}(y'[n] + i)$
    end for
    return $x$                                     ▷ $x = x[1] \dots x[n-1]$
end procedure
```

IV Comparison of Bastion with Existing Encryption schemes

Assume plain text m is divided into n-1 blocks.

	Security	**Storage (blocks)**	**omputation overhead**
CTR encryption	CPA secure 1CAKE secure	n	n-1 b.c. n-1 XOR
AONT	CPA insecure (n-1) CAKE secure	n	2(n-1) b.c. 3(n-1) XOR
Bastion	CPA secure (n-2) CAKE secure	n	n-1 b.c. 3n-1 XOR

b.c. is number of block cipher operations and XOR is number of XOR operations

CTR encryption

CTR mode is customary CPA encryption mode which gives CPA security however 1CAKE anchored.

Subsequently, a foe furnished with the encryption key should just bring two ciphertext squares to break information secrecy.

AON encryption

AON isn't CPA secure which can get to all figure content squares. Here AON encryption mode [29] pre-process a message with an AONT and after that encode its yield with a CPA-secure encryption mode. This worldview is alluded to in the writing as AON encryption and was first proposed by [23]. Existing AON encryption plans require no less than two rounds of square figure encryption with two diverse keys: the first round is the real AONT that implants the principal encryption enter in the pseudo-figure message, a second round utilizations another encryption key that is kept mystery to ensure CPA-security. AON encryption builds the capacity measure by a solitary square. Be that as it may, two encryption rounds constitute a significant overhead while scrambling and unscrambling extensive documents.

Performance comparison:

The above table demonstrates the execution of bastion in different angles which incorporate security, calculation overhead when contrasted with existing encryption plans CTR and AONT.

At the point when given a plain content of m squares, CTR encryption mode created n=m+1 figure content squares experiencing (n-1) square figure activities and (n-1) XOR tasks. CTR encryption mode is CPA secure however 1 CAKE secure.

AONT yields figure content of n=m+1 figure content squares with 2n-1 square figure activities and 2(n-1) XOR tasks. AONT is CPA uncertain since encryption key is inserted inside the yield itself and is (n-1) CAKE secure.

Bastion produces a yield n=m+1 figure content squares with (n-1) square figure activities and (3n-1) XOR tasks. Bastion is effective plan which accomplishes both CPA security and (n-2) CAKE security.

Here the execution of Bastion is assessed logically and exactly in contrast with various existing encryption systems. Our outcomes demonstrate that Bastion significantly enhances the execution of existing AON encryption plans, and just brings about an immaterial overhead when contrasted with existing semantically secure encryption modes (e.g., the CTR encryption mode).

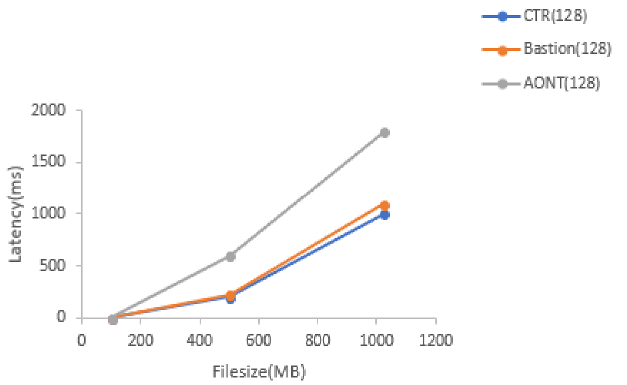


Fig. Latency of encryption/encoding for different file sizes

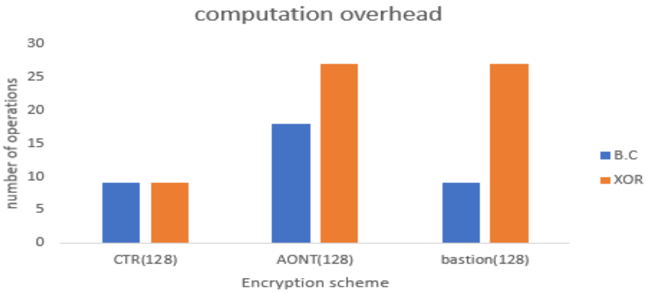


Fig. Computation overhead of different encryption schemes (number of storage blocks n=10)

Clearly, all existing solutions are either not satisfactory in terms of security or incur a large overhead and may not be suitable to store large files in a multi-cloud storage system. In what follows, we introduce our solution, Bastion, which considerably improves the performance of existing solutions.

V Related work

Anand Desai [5] proposed All-or-nothing transformations(AONT) which includes preprocessing of information took after by encryption. It includes two rounds of encryption. In the preprocessing round, the plain content is scrambled with a key and this is enter is added in the pseudo plain content got toward the finish of first round. In the second round the pseudo plain content is encoded with genuine key. In AONT, the scrambled key is implanted in the yield figure squares. At the point when all the yield squares are gotten to by enemy, it can without much of a stretch get the key.

Boyang Wang et al. [7] proposed numerous key encryption of cloud information to guarantee cloud information privacy and guaranteeing productive cloud information stockpiling.
Sneha singha and S.D Satav[11]have presented the idea of de duplication procedure of information wherein the

inherent key introduction flexible framework will check the duplication of information and wipe out the excess one utilizing MD5 hashing.

The thought of Provable Data Possession (PDP) was initially proposed by Ateniese et al. [12] for guaranteeing information ownership on untrusted servers. This plan checked the uprightness of outsourced information by the systems of arbitrary example and homomorphic straight authenticators.

Juels and Kaliski [14] investigated the model named as Proof of Retrievability (PoR) which can guarantee both ownership and retrievability of the records on untrusted servers. They utilized the systems of blunder revising codes and spot-checking to build the PoR plot. Shacham and Waters [15] furnished an enhanced PoR display with stateless check. They proposed a private confirmation plot in view of pseudorandom capacities and an open check conspire in view of BLS signature conspire.

A novel idea of OAEP (ideal uneven encryption cushioning) was proposed by V.Boyko[16] giving more security than the AONT plot.

S. Micali [17] proposed the plan of spillage flexible cryptography points which at outlining cryptographic natives that oppose enemy which learns halfway data about the mystery condition of a framework. Diverse models were proposed for thinking the releases in any case, every one of these models can't constrain the enemy from taking in the mystery state.

VI Conclusion

The idea of accomplishing information privacy under key presentation is tended to in the paper. A novel plan, Bastion is proposed against foe which accomplishes information classification under key introduction. The enemy would need to secure the encryption key and the greater part of the figure content squares to recuperate the plain content.

Bastion significantly enhances the execution of existing encryption plans and offers enhanced security in the new aggressor display and just brings about an insignificant overhead (under 5%) when contrasted with existing encryption modes (e.g., the CTR encryption mode).

VII. References

[1] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues". *Future Generation computer systems* 28.3 (2012): 583-592.

[2] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing*", IEEE Transactions on Parallel and Distributed Systems (TPDS).*

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing", *The 17th IEEE International Workshop on Quality of Service* (IWQoS'09), July 13-15, **(2009),** Charleston, South Carolina.

[4] Swapnali More, Sangita Chaudhari "Third Party Public Auditing scheme for Cloud Storage" *Proc.7th International Conference on Communication, Computing and Virtualization* 2016.

[5]" The Security of All-Or-Nothing Encryption: Protecting Against Exhaustive Key Search" , Anand Desai *adesai@cs.ucsd.edu*

[6] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409-428, 2012.

[7] Boyang Wang, Ming Li, Sherman S. M. Chow "Computing encrypted cloud data efficiently under multiple keys", *2013 IEEE Conference on Communications and Network Security (CNS)*

[8]S. Swaminathan, A. Karthick, S. Suganya, "A secure and robust crypto system based on unique dynamic key generation scheme", *Computing Communication and Networking Technologies (ICCCNT) 2014 International Conference on*, pp. 1-7, 2014.

[9]Jitender Grover, Shikha, Mohit Sharma "Cloud computing and its security issues — A review **"** *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* 2014

[10]A. Desai, "The security of all-or-nothing encryption: Protecting against exhaustive key search," in *Advances in Cryptology (CRYPTO)*, 2000, pp. 359–375.

[11]Sneha singha and S.D Satav "An Effective Approach for Key Exposure Resistance in Cloud using De Duplication and Tile Bitmap Method" *International Journal of Computer Applications* (0975 – 8887) Volume 146 – No.9, July 2016.

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM *Conf. Computer and Comm. Security*, pp. 598-609, 2007.

[13] G. Timothy and M. M. Peter, "The NIST definition of cloud computing," Vol. NIST SP - 800-145, September **(2011)**.

[14] A. Juels, and B. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th *ACM Conf. Computer and Comm. Security,* pp. 584-597, 2007.

[15] H. Shacham and B. Waters, "Compact Proofs of Retrievability," *Advances in Cryptology-Asiacrypt'08,* pp. 90-107, 2008.

[16] V. Boyko, "On the Security Properties of OAEP as an Allor-nothing Transform," in *Advances in Cryptology (CRYPTO),* 1999, pp. 503–518.

[17]S. Micali and L. Reyzin, "Physically observable cryptography," in *Theory of Cryptography Conference (TCC),* 2004, pp. 278–296.

[18] D. Cash, A. K¨upc¸ ¨u, and D. Wichs, "Dynamic proofs of retrievability via oblivious ram," *Advances in Cryptology-Eurocrypt'13*, pp. 279-295, 2013.

[19]R. L. Rivest, "All-or-Nothing Encryption and the Package Transform," in *International Workshop on Fast Software Encryption (FSE),* 1997, pp. 210–218.