ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

Providing Security to Cloud Data using key Exposure

Divesh Kumar[1], Dinesh Kumar [2], Kawaljeet Singh[3] , Kumar Piyush[4], Madhu Shree[5]

UG Students, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Bangalore, Karnataka, India[1,2,3,4]

Assistant Professor, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Bangalore, Karnataka, India[5]

ABSTRACT: Cloud computing is the technology of using a network of remote servers on the internet . It further avoids the use of a local -server. Customer can use applications without installations and access their personal files at any computer with internet access. Day to day usage of cloud has attracted attackers to break data security in the cloud data storage system. Security of cloud data is ensured by means of cryptographic keys which when exposed facilitates the attackers access the ciphertext. This paper reveals an overview and study of providing security to cloud data using key exposure.

KEYWORDS: Cloud, Data, Key exposure, Data confidentiality, Dispersed storage

I.INTRODUCTION

Cloud Computing is the fundamental change happening in the field of Information Technology .It is a representation of a movement towards the intensive large scale specialization. On the other hand it brings about not only convenience and efficiency problems but also great challenges in the field of data security and privacy protection. Currently security has been regarded as one of the greatest problems in the development of Cloud Computing .This paper describes the great requirements in Cloud Computing security key technology standard and regulation etc. and provides a Cloud Computing security framework using key exposure .This paper argues that the changes in the above aspects will result in a technical revolution in the field of information security.

Cloud system can be used to enable data sharing capabilities this can proven abundant of benefits to the user. There is currently a push for IT organization to increase their data sharing efforts. In enterprise settings, there is the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. With current technology user can access almost all of their files or emails by mobile phone or computer from any corner of the world.

In the cloud storage efficient public key encryption scheme which support flexible delegation in the sense that any subset of the cipher texts is decryptable by a constant-size decryption key.

Cloud computing has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, virtualization security, application integrity, and identity management. Data protection is one of the most important security issues, because organizations won't transfer its data to remote machines if there is no guaranteed data protection from the cloud service providers. Many techniques are suggested for data protection in

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

cloud computing, but there are still a lot of challenges in this subject. The most popular security techniques include SSL (Secure Socket Layer) Encryption, Intrusion Detection System; Multi Tenancy based Access Control, etc.

So, security challenges of data protection when using cloud computing must be appropriately solved and minimized. When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more doubts about the security issues when they are using this technology. So, a lot of different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are a lot of security techniques for data protection that are accepted from the cloud computing providers, and they all provide authentication, confidentiality, access control and authorization.
This will mention now the most important recommendations in order to have secured cloud environment. One of the recommendations is a cloud consumer to be ensured that efficient governance, risk and compliance processes exist. This means that security controls must exist in cloud. We implement it using key exposure.

II.RELATED WORK

First in the sharing of secret scheme, which show how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces. Here, knowledge of any k or more Di pieces makes D easily computable and knowledge of any k- 1 or fewer Di pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
This scheme is highly unreliable since a single misfortune (a computer breakdown, sudden death, or sabotage) can make the information inaccessible.

All or Nothing transformations leverage a secret key that is embedded in the output block. The key can be recovered and single blocks can be inverted after all the output blocks are available. All or Nothing transformations has the key material without the decryptor. Therefore All or Nothing is an encryption scheme.

Concern in using cloud storage is that sensitive data are confidential and not being exposed outside. In Shannon model the security of constructions is corresponded to double and (two-key) triple DES. Here, we consider Fk1(Fk2 ()) and Fk1(F1k2(Fk1())) with the component functions being ideal ciphers. This models the resistance of there constructions to “generic” attacks like meet in the middle attacks. We compute a bound on the probability of breaking the double cipher as a function of the number of computations of the base cipher made, and the number of examples of the composed cipher seen, and show that the success probability is the square of that for a single key cipher. Meeting in the middle is the best possible generic attack against the double cipher. To realize our concept, we equip the broadcast encryption with the dynamic ciphertext update feature, and give formal security guarantee against adaptive chosen-ciphertext decryption and update attacks.

Leakage resilient cryptography designs cryptographic primitives resisting on adversary and learning partial information about the secret state of a system . The models limit the knowledge of secret state of a system by the adversary. In our model the secret material is given to the adversary .

Evaluate the performance of Bastion in comparison with a number of existing encryption schemes. Our results show that Bastion only incurs a negligible performance deterioration (less than 5%) when compared to symmetric encryption schemes, and considerably improves the performance of existing AON encryption schemes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

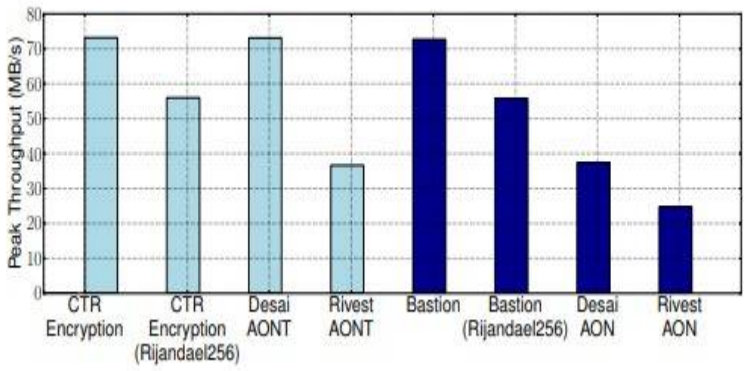
Vol. 7, Issue 5, May 2018

III. METHODOLOGY

In our survey, study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the ciphertext blocks. The adversary can acquire the key either by exploiting flaws or backdoors in the key-generation software, or by compromising the devices that store the keys (e.g., at the user-side or in the cloud). To counter such an adversary, we propose Bastion, a novel and efficient scheme which ensures that plaintext data cannot be recovered as long as the adversary has access to at most all but *two* ciphertext blocks, even when the encryption key is exposed.

Bastion achieves this by combining the use of standard encryption functions with an efficient linear transform. In this sense, Bastion shares similarities with the notion of all-or-nothing transform. An AONT is not an encryption by itself, but can be used as a pre-processing step before encrypting the data with a block cipher. This encryption paradigm— called AON encryption— was mainly intended to slow down brute-force attacks on the encryption key. However, AON encryption can also preserve data confidentiality in case the encryption key is exposed, as long as the adversary has access to at most all but one ciphertext blocks.

IV. EXPERIMENTAL RESULTS



(a)

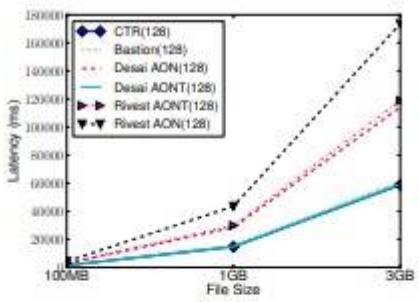
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

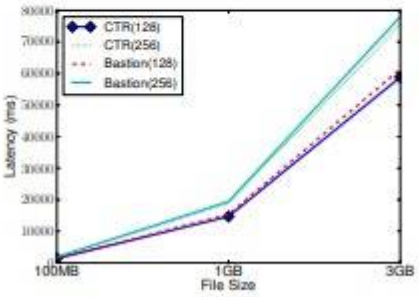
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018



(a) Latency of encryption/encoding for different file sizes.



(b) Latency of encryption/encoding for different block sizes of the underlying block cipher.

(b)

	Computation	Storage (blocks)	Security
CTR Encryption	$n-1$ b.c. $n-1$ XOR	n	1*CAKE* ind-secure
Rivest AONT [26]	$2(n-1)$ b.c. $3(n-1)$ XOR	n	N/A ind-INsecure
Desai AONT [12]	$n-1$ b.c. $2(n-1)$ XOR	n	N/A ind-INsecure
Rivest AON Encryption [26]	$3n-2$ b.c. $3(n-1)$ XOR	n	$(n-1)$*CAKE* ind-secure
Desai AON Encryption [12]	$2n-1$ b.c. $2(n-1)$ XOR	n	$(n-1)$*CAKE* ind-secure
Encrypt-then -secret-share	$n-1$ b.c. $2n-1$ XOR	n^2	$(n-1)$*CAKE* ind-INsecure*
Bastion	$n-1$ b.c. $3n-1$ XOR	n	$(n-2)$*CAKE* ind-secure

(c)

FIGURE (A) SHOWS THE EXPERIMENTAL REULTS COMPARED WITH ALLTHE EXISTING SCHMES. FIGURE (B) SHOWS THE LATENCY GRAPH .FIGURE (C) IS THE REPRESENTATION OF ALL THE COMPUTATION AND SECURITY SCHEMES.

V. CONCLUSION

In this survey we studied different cryptographic techniques for data sharing security. One trivial solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Thus it considers how to compress secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. Our approach is more flexible than hierarchical key assignment.

REFERENCES

[1] Cheng-Kang Chu et.al, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.
[2] M. J. Atallah et.al, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

[3] J. Benaloh et.al, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
[4] S. S. M. Chow et.al, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," in ACM Conference on Computer and Communications Security, 2010, pp. 152–161.
[5] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.
[6] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.