CloudStash: An Efficient Technique to Provide Security to Multi-Clouds

[1]Suman V Chinivar, [2]Sirisha G N, [3]Sushma K V
Department of Computer Science & Engineering
Sambhram Institute of Technology, India
[1]sumanchinivar@gmail.com
[2]sirismailbox@gmail.com
[3]gangasush@gmail.com

Abstract - **Cloud computing is rapidly growing in many organizations. Cloud computing has many features of storing and sharing their data over the cloud network. The various ways of storing and sharing the data has made cloud computing very popular among various organizations. According to IDC survey; security is the major issue that the cloud is facing. Protecting the cloud using normal key management technique opens the risk of attackers hacking the key and confidential data. To address these issues, we propose the CloudStash scheme. Here, we apply the secret sharing scheme directly on the file to store multi-shares of the file. Then we apply hash and sign techniques to provide highly secure cloud by addressing the issues like confidentiality, data integrity, availability and key management.**

Index Terms - **CloudStash, hash and secret sharing, DepSky.**

I. INTRODUCTION

Cloud computing is a computing prototype, where a bulky pool of systems are connected in private or public networks, to provide scalable infrastructure for application data and file storage space. Cloud computing is growing eventually due to it advantageous cost and also faster access of data.

As cloud holds much important information about the users which may contain credit card details and even personal information about the users it should be protected from the malicious insiders who may hack the data. As the confidential data has to be moved between large data centers there is a risk of data being exposed which becomes easy for the attackers to hack the sensitive data. Encryption is not alone adequate to protect the data;unique techniques have to be used in order to achieve high security. So the cloud providers should addressprivacy and security issues as a matter of high priority.

Fig. 1: Cloud Stash

People want to access data in various ways. Some access data through monthly memberships; some purchase and download data for offline viewing on their devices; while some others want to purchase data but do not intend to keep it on their devices. For those users who wish to access data without preserving the data in their devices CloudStash provides aenormous opportunity. For example using Cloud Stash users can purchase a video and it is stored in the cloud and available to watch from anywhere they user want provided with internet connection. Here users can watch or purchase the files from any device that has a browser including tablets,mobile phones and desktops.

As single cloud is facing lot of issues like data damage during transmission to or from cloud, malevolent insiders hacking the password of service provider and termination of service at anytime. To overcome these disadvantages and provide better usability of service; multi-cloud techniques is being used[6]. Use of multi-cloud avoids dependency on individual clouds. Shamir secret sharing scheme has been used to provide highly secure cloud. Here, the secret is divided into parts giving each client his own unique share where some of the shares or all of the shares are needed to rebuild the secret. Shares are obtained from original secret but they are not part of secret[10].

In this paper, we propose CloudStash a multi-cloud technique that uses Shamir secret sharing scheme to protect data stored in cloud such that to address issues like confidentiality and availability[1].

II. LITERATURE SURVEY

CloudStash addresses various issues like confidentiality, availability and key management[1].

A. Confidentiality: Confidentiality is achieved by applying secret sharing scheme on the file. Then the secret key is split into multiple shares. The multiple shares are distributed over multiple clouds. Multi-cloud scheme such as DEPSKY(Dependable and Secure Storage Key) distributes encrypted data over multiple cloud[8]. Using such distribution each cloud stores part of the cipherdata thus providing high level of confidentiality.

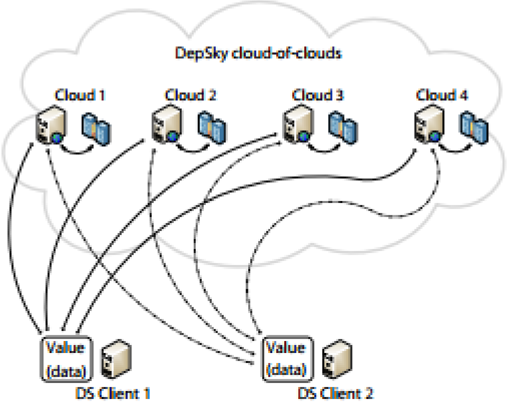

Fig.2: Architecture of DepSky

DEPSKY is a system that improves accessibility, integrity and privacy of data stored in cloud through encryption, encoding and replication of data on device clouds that form cloud-of-cloud[8]. In inter-cloud key is split upon encryption and key shares are attached as metadata to pieces of data destined to individual clouds. The number of shares needed to reconstruct the key is a parameter that depends on number of available cloud and derived resilience and is related to reliability protocols[11].

B.Key Management: Highly secure cloud is based on encryption/decryption of keys that protects the users data in the cloud[1]. The issues w.r.t key management are how to store the keys, how to distribute keys between multi-users and how to protect keys from malicious insiders. Key-Lifecycle Management (KLMS) is a pattern-based method and strict access control to keys and also secure access control policy for a key-management interface. Intercloud used KLMS for its key management[2]. CloudProof relied on broadcast encryption which is qualitative and quantitative assessment of encryption schemes designed for broadcast and for secure transmission to an arbitrary set of recipients listed in ACL while minimizing key management related transmission[12].Cryptonite introduced strongbox file to manage userskeys in Web. Some users used broadcast encryption to distribute read keys to authorized readers and for authorized writers shared keys were distributed[3]. CloudSealeffortlessly integrates symmetric encryption, k-out-of-n secret sharing, proxy-based re-encryption and broadcast revocation mechanism. Both, forward security and backward security are provided by CloudSeal; forward security where clients cannot access the content in the cloud before signinig into the group, and backward security where clients cannot access the content in the cloud after exiting the group[4]. DepSky and Intercloud utilized the secret-sharing scheme and multi-clouds to distribute encrypted data with shares of key over multi-clouds[1]. Proxy re-encryption is a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext[5]. CloudStash bypasses key management issues. Instead of storing/managing keys in untrusted clouds or relying on the users protections of keys; CloudStash directly applies the secret-sharing scheme[1].

C. Availability: In CloudProof customers cannot only detect violations of write serializability, integrity and freshness,it also proves the occurrence ofinfringement to the third party. CloudProof uses cryptographic tools to allow customers to detect and prove cloud misbehavior. HAIL (High Availability and Integrity Layer) a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable[7]. HAIL utilized RAID (Redundant Array of Inexpensive Disk) like techniques to distribute data over multiple clouds in order to provide more availability and integrity of the data stored in the cloud[9].

III. CLOUDSTASH STRATEGY

In CloudStash the secret sharing scheme is being used. CloudStash splits a file into multi-shares and distributes these multi-shares over multi clouds. Every share is a part of secret. These shares do not give any information about the file which is being used. In CloudStash, no single cloud stores the threshold shares to address insider attacks.

In the previousmulticloud approaches like DepSky,Intercloudand N-Cloud the attacker can obtain a part of data if they can compromise the cloud. But in CloudStash the attacker must attack all the clouds to get the required number of shadows[1].Compromising all clouds in CloudStash makes it difficult to achieve.

CloudStash provides availability by using secret sharing scheme. When one cloud storage is attacked or terminated, clients can obtain their data from other available clouds by reconstructing threshold shares.

VI. DESIGN AND ANALYSIS

In the paper two systems have been compared: DepSky and CloudStash.

DepSky uses secret sharing scheme to provide confidentiality. Here, the service provider distributes the secret of 'n'users; but each user gets only one share of secret.

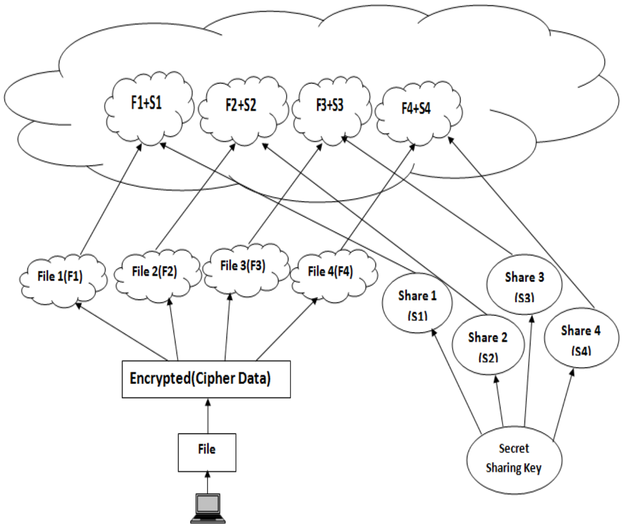

Fig. 3: Structural Design of DepSky

In DepSky, the data is encrypted using some symmetric encryption. The cipher data is dispersed into multiple files. Shamir's secret sharing scheme is used to generate the secret key which is shared among the file. For each file the secret is employed. The file is shared among each cloud along with the shared key[10]. DepSky uses symmetric encryption algorithm which leads to many issues like exchanging of secret keys, securing the keys and providing authentication to the users[8]. A secure channel is needed to exchange the key. The keys have to be exchanged in the way that they remain secret. Different shared key has to be generated for communicating with every different party. Both sender and receiver use the same key; authentication has to be provided between the communicating parties.

Thus, to overcome these issues we are migrating to CloudStash which uses secret sharing scheme which protects a secret from possible loss, damage and malicious insiders. For this technique there is a protocol known as Secret Sharing protocol[10]. Distributing secret is a cryptographic process that allows us to obtain a series of values or shadows from given secret, so it will only be possible to recover the original secret using a previously specified number of those shadows, but impossible if these are fewer shadows. Shadows are derived from original secret but are not part of secret.

A. CloudStash Architecture

CloudStash uses secret sharing scheme to generate the secret key directly on the file. This key splits the file into multi shares. The technique then uses cryptographic hash functions which are practically impossible to retrieve the data from the hash value.

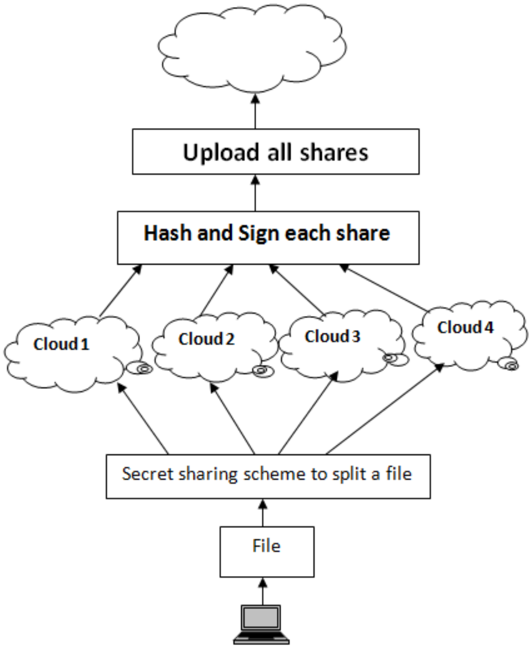

Fig.4: Structural Design of CloudStash

The advantage of using hash function is that it is easy to compute the hash value for any data. It is very difficult to generate the message that has a given hash. It is impossible to modify message without changing hash. It is also impossible to find two differentmessages with same hash. Hash functions provide confidentiality to CloudStash. The integrity is achieved by using Digital Signatures. After applying hash and sign techniques to the shares; all the shares are uploaded to the cloud. Usage of hash functions along with digital signature makes the CloudStash more secure

B. Algorithm forCloudStash using Shamir Secret Sharing scheme and Hash Functions

Step 1: Determine number of shadows 'n'

Step 2: Determine 'k' to recover secret

Where, k is threshold value and (k, n) is threshold protocol.If less than k shadow then it is impossible to recover to recover the secret. If k = n then all the shadows are required to recover the secret.

Step 3: Hide the secret in the polynomial

p(x) = a_0+a_1x + a_2x^2 + a_3x^3+……. + $a_{k-1}x^{k-1}$(1)

Using equation (1) 'n' shadows are generated

Step 4: Recovering secret from generated shadows. Consider 'k' shadows out of 'n' shadows.

Step 5: Use Lagrange Interpolation method for 'k' points

(x_1, y_1), (x_2, y_2), ... ,(x_k, y_k)

Step 6: Determine q_j(x) = $\pi_{i=1,i\neq j}^{k}$ (x - x_i) /(x_j- x_i) with j=1,2,…,k

Where q_j(x) is an auxiliary polynomial which is calculated for each point

Step 7: For each shadows' n' **do** hash and sign

Step 8: Determine original polynomial using auxiliary polynomial

$p(x) = \sum_{j=1}^{k} y_i q_j$(x)

Where p(x) gives the original secret entered.

VII. CONCLUSION

As security is the major issue in the cloud; CloudStash is one of the approach which provides high level of confidentiality, data integrity, availability and provides better key management techniques by making use of Shamir's secret sharing scheme along with hash and sign functions. We also compared CloudStash with the previous multiclouds approach like DepSky to show that CloudStash provide better security thus making the cloud very secure.

VIII. FUTURE WORK

In future work, Diffie-hellman model and Elliptical Curve Cryptography can be implemented in CloudStash which provides the best way of providing data integrity.

REFERENCES

[1] FahadAlsolami and Terrance Boult, "CloudStash: Using Secret Sharing Scheme to Secure Data, Not Keys, in MultiClouds", 11th International Conference on Information Technology: New Generations, 2014, pp 315-320

[2] M. Bjorkuvist, C. Cachnin, R. Haas, X.-Y. Hu, A. Kurmus, R. Pawlitzek, and M. Vukolic, "Design and Implementaionof a Key Life Cycle Management System", in Financial Cryptography and Data Security. Springer, 2010, pp. 160-174.

[3] A. Kumbhare, Y. Simmhan, and V. Prasanna , "Cryptonite: A secure and Performant Data Repositoy on Public Clouds", in Cloud Computing(CLOUD), 2012, IEEE 5th International Conference on. IEEE, 2012, pp 510-517.

[4] H. Xiong, X. Zhang, D. Yao, X. Wu and Y. Wen, "Toward end-to-end Secure Contetn Storage and Delivery with Public Cloud", in Proceedings of the Second ACM Conference on Data and Application Security and Privacy. ACM, 2012, pp. 257-266

[5] G. Atenieese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage", ACM Transactions on Information and System Security(TISSEC), 2006, Vol. 9, No. 1, pp. 1-30.

[6] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences, 2012.

[7]\K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16thACM Conf. on Computer and communications security, 2009, pp. 187-198.

[8]A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6th Conf. on Computer systems, 2011, pp. 31-46.

[9] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10: Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[10]A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.

[11] C. Cachin R. Haas, and M. Vukolic, "Dependable Storage in the Inter Cloud," IBM Research, Vol. 3783, pp 1-0, 2010

[12] R. A. Popa, J.R. Lorch, D. Molnar, H. J. Wang and L. Zhuang, "Enabling Security in Cloud Storage Slas with Cloud Proof," in Proc. USENIX ATC, 2011