ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey of Hidden and Encoded Cloud Storage technique with Anonymous Access

Mohd Sadim[1], Dr. R. K.Sharma[2]

Research Scholar, Department of Computer Science and Engineering, Al Falah University, Faridabad, India[1]

Assistant Professor, Department of Computer Science and Engineering, FET, Agra College, Agra, India[2]

ABSTRACT: Cloud computing is a standard in which information is placed over the internet on the virtual servers which is extracted by the users at the front end. It is one of the today's most enticing technology areas which is efficient in cost as well as flexible. Cloud Computing promotes sharing of resources as one does not need to install a particular software or hardware to access the information from the cloud. Companies provide the services of cloud computing which will charge by the users and they subscribe via internet. Due to certain features such as low cost, low maintenance and easy access, various organizations store their data on the cloud or not. In this paper, we deal with all the security concerns in order to promote the common level of understanding between the users, organizations which must be considered by them before adopting cloud services.

KEYWORDS: Cloud Computing, Security, privacy, Attestation, Intelligence

I. INTRODUCTION

Cloud computing is the latest technology and a new prototype for solving complex and large scale problems. This technology is acquired its due importance in a very short period of time. This provides unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are merely accessing or renting or consume resources as a service and paying instead for what they use.
The biggest security concern with Cloud computing is the issue of Trust [10]:

1. How do you know for certain that the key people who manage your data and applications on the cloud are completely trustworthy?
2. Who else besides you has access to sensitive information?

As we all know that our data is shared on local networks with servers that may be clustered and sharing storage. This approach is having time to stable its architecture and provide decent redundancy when it is deployed. Cloud services are alike known as Grid services, these services are used to solve large scale problems is various fields such as Science and technology. These services are less capable of implementing enterprises services. In terms of technologies, the vision of cloud computing and grid computing is same as they both have same goals such as reduction in cost, increase reliability and increase flexibility but this is not a new idea however the solution is changed according to the requirement of new massive data.

1) Security and privacy

Concerns[2] such as data protection, operational integrity, vulnerability management, business continuity (BC), disaster recovery (DR), and identity management (IAM) make up the list of security issues for cloud computing[1]. Privacy is another key concern — data that the service collects about the user (e.g., event logs) gives the provider valuable marketing information, but can also lead to misuse and violation of privacy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

2) *Conformity*

Data privacy and business continuity are two big items for compliance. Specific issues such as geo-location of data centers, incident response procedures, rediscovery support, and proper handling of logs and audit trails all come to focus here.

3) *Legal and agreement issues*

Legal issues are the least well-understood areas of cloud computing. Though I will not be giving out legal advice, I will be looking at what legal issues may arise in the context of cloud computing.
For instance, liability and intellectual property are two examples of legal issue that often being discussed. Other contractual issues include end-of-service support — when the provider-customer relationship ends, customer data and applications should be packaged and delivered to the customer and any remaining copies of customer data should be erased from the provider's infrastructure, etc.

II. CLIENT'S PERTAIN

According to Gartner, while assessing the Security Risks of Cloud Computing following Subsequent concerns should be well justified in case of client:

A. Honoured User Access

The important and confidential information [3] which is processed outside the organization on the cloud is involved with a lot of risks, because it has no direct control over it. All the information is in the hands of administrators that are hired by the cloud service provider organization and we have no idea about those people.

B. Regulatory Compilance

Customers are only responsible for the security and integrity of their own data, even when it is held by a service provider. External audits and security certifications are subjected by traditional service providers. According to Gartner, Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions".

C. Data Location

Users have no clue at all where they have stored their data and do not have any idea about the geo-location of his information. So in this case they have to depend on service provider if it agrees on processing and storing information according to some local privacy requirements.

D. Data Seperation

Data is present on the loud in an environment that is shared by all the customers. It is one of the great concerns according to the user what is done for the segregation of the data. In this case some proofs should be given by some service provider that the encryption scheme is designed and tested thoroughly by experts.

E. Recovery

In case of disaster or damage to the cloud or if there is a total failure of infrastructure then the provider should tell any method for complete recovery of data and how much time will it take.

F. Long Term Feasibility

According to the ideology, client's confidential and important data should not disclose by the service provider to any other person or organization. And the clients must be sure that the data will remain available in case of disaster. Client should ask the providers about the security of their information in such a manner.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

III. SECURITY ISSUES

There is a number of security concerns associated with cloud computing but these concerns fall into two broad categories: Security issues faced by cloud and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.
Security concerns are arising because both customer data and program are residing in provider premises.

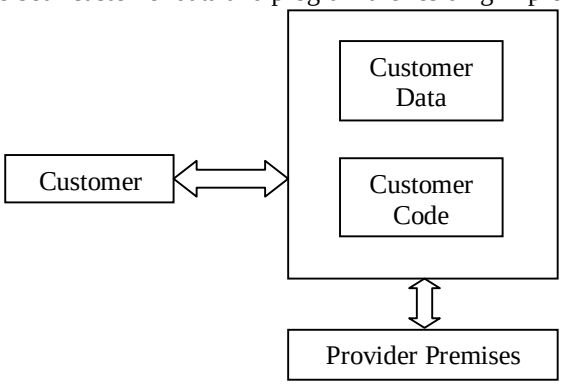
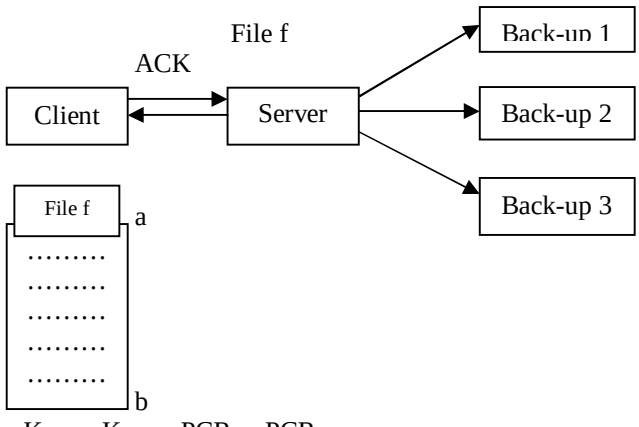


Figure 1

No. Of Data Back-ups

We deal with the case where the server stores a given number of redundant copies of the client's data for the purpose of data backup and efficient retrieval. The problem is to verify at the client with a high probability that the server is actually storing the number of copies of the client's data in its database all the time, for which it is charging the client.



ACK = K_{PM1}, K_{PM2}, K_{PM3}, PCR_1, PCR_2, PCR_3

Figure 2

a) Attacker Model

A malicious server tries to fake the fact that it is storing a larger number of copies of the client's data than it actually does.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

b) Assumptions

We assume that each data backup site has a TPM installed whose private key is certified by a trusted third party. We assume that there is software with the functionality described below and which is trusted by the client, run on all the back-up machines all the time. We also assume that the server cannot launch any sophisticated hardware modifications to the storage locations which can make the system clock go at a significantly faster rate. We also assume that the BIOS and RAM at the backup sites have not been tampered with.

c) Analysis

We observe that the effort spent by the client in verification is O (N*b) where N is the number of times for hash was Calculated by the trusted software during the billing period and b is the number of chunks. We must choose the values of b and N in order to ensure a high probability of collision of randomly chosen words at the client and trusted software, and low periods of uncertainty between two consecutive hash Calculations, while at the same time having the client effort for Verification to be reasonably low. We show that probability of at least one collision of randomly chosen words at client and rusted software is

$$P = (1 - (a - 1)/a) b) N,$$

where a is the size of a chunk in unit of words (32 bit) b is the number of chunks and N is the number of hashes in the Billing period.

IV. CONVENTIONAL SECURITY

These concerns involve computer and network infringement or strikes that will be made possible or at least easier by moving to the cloud. Cloud purveyors respond to these concerns by debating that their security principles and processes are more mature and tested as compared to those of the average company. Another argument, made by the Jericho Forum is: "It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls."

A. Third Party Control

The legal suggestions of data and applications being held by a third party are multifaceted and not well understood. There is also a major lack of transparency and control when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but actually regulatory compliance needs transparency into cloud. All this is publicizing some companies to make up private clouds to prevent such issues and thereby, retain some of the benefits of cloud computing.

B. Assortments In Security

The attractiveness of cloud computing for a broad range of users may require differing approaches for use and security. At the one extreme, low-end users, such as start-ups, can use clouds for just about everything. The cloud provider's security and reliability generally exceeds that of a small enterprise. At the other extreme, high-end users such as large enterprises are more likely to employ a hybrid model. For legal and risk management reasons, they will keep especially sensitive data and applications in-house and may use an internal cloud. In between, mid-size enterprises can use clouds for many purposes including compute cycles for R&D projects, online collaboration, partner integration, social networking, new business tools and more.

V. NEW PATH FOR ENHANCED SECURITY

With the emergence of cloud, the cloud provider also controls the user's data. In this way there is always a risk of security and authenticity of data. So to avoid this problem, some services or features must be added to improve the services of the cloud and to limit the control of cloud service provider. The aim here is to increase the benefit and reliability of the cloud for the users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A. Intelligent Data Security

As in the present scenario, a client enterprise has to depend on the cloud provider for the security of the entire information. So to increase the control over the data the enterprise needs to have to adopt a different strategy for the data security. In this, we make the data intelligent so that it saves itself from potential threats. We call this approach of data and information protecting itself as Intelligent Data Security. The data in this type of approach is saved over the cloud in an encrypted form and a policy for its usage is applied over it. The data is made so intelligent and self dependent in this way so that it is not relied on any other scheme, no matter how tough is the environment is that in which it is used. When data is accessed, it should check its usage policy and a secure-virtual environment should be created by the data around itself .Information should be revealed only if the environment is verified as trustworthy (using Trusted Computing). Intelligent Data Security will lead towards a hassle-free protection of data.

B. High-Assurance Remote Server Attestation

In the cloud computing the method of storing and accessing information over the cloud is not very secure. These security constraints prohibit the enterprises to utilize the services of cloud. There is a lack of transparency in this phenomenon. The enterprises wants there to have a 24X7 check on their data, to find how is it handled at the cloud and to get a satisfaction that it is not altered or modified in any way, or it is not intercepted by spies. They wish their data to be in the same state as it was at the time of sending to the cloud. Currently the customers see for the manual auditing procedures like SAS-70 provided by the cloud service providers.

An approach which can handle this problem effectively is Trusted Computing. With Trusted Computing, the computer will consistently behave in expected ways, and those behaviors will be enforced by hardware and software. Trusted Computing uses cryptography to help enforce a selected behavior. The main functionality of TC is to allow someone else to verify that only authorized code runs on a system [4]. (Imagine a trusted monitor installed at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide “proofs of compliance” to the data owner, stating that certain access policies have not been violated. To ensure integrity of the monitor, Trusted Computing also allows secure bootstrapping of this monitor to run beside (and securely isolated from) the operating system and applications. The monitor can enforce access control policies and perform monitoring/auditing tasks. To produce a “proof of compliance”, the code of the monitor is signed, as well as a “statement of compliance” produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run and that the cloud server has complied with access control policies).

C. Privacy-Enhanced Business Intelligence

As suggested above to increase the control of an enterprise over its information encryption should be used. Only the encrypted information should be stored over the cloud. But this encryption has a limiting factor on the usage of data. It is obvious that searching an encrypted data by unencrypted keywords is a difficult task. As in general, if the data is stored in simple text, anyone can search by using some specific keywords. But this is not possible with the encrypted text because, the operation and computation will be done on the encrypted text. But the cryptography has a solution to this problem. A new encryption scheme is invented which allows operation and computation on the cipher text.

For example: (predicate encryption) is a keyword-searchable encryption scheme, which allows a user to extract even the encrypted data containing the particular keywords over a remote server. This scheme has proved to be very important in solving security problems of confidential data and information. However, most existing schemes support only a single keyword for searching, but do not allow for Boolean combinations of keywords.

D. Computation Over Encrypted Data

Computation over the encrypted is information is not an easy job. So there is need to decrypt the information and then perform computation, but again it is not safe. So to remove this limitation we have some other encryption techniques that can be of great use in maintaining security over the cloud. These are homo-morphic encryption and Private Information Retrieval (PIR).

Homo-morphic encryption scheme [5] provides us the facility to perform computations over the cloud without decrypting the information. This encryption technique has limitations that it can be used only in cases where computation is simple. For example, the popular encryption scheme ROT (13) is partially homomorphism. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

calculations can be performed over the encrypted information and if we decrypt the results, we get the result as it would have come if the operation was performed on simple plain information.

Let us encrypt two strings, concatenate them and decrypt the result. In pseudo-code, this is:

```
Var   v1 = Encrypt(13,"AFU");
 // v1 = OFNVGZ
Var v2 = Encrypt(13,"FARIDABAD"); //v2=SNEVQNONQ
Var v3 =  Concat (v1, v2);
//v3 =OFNVGZSNEVQNONQ
Var z  = Decrypt (13, v3);
// z = AFUFARIDABAD
```

Because it was not necessary to first decrypt the two fragments of cipher text before performing the concatenation operation, we can say that rot-13 is homomorphism with respect to concatenation. In other words, it is possible to take two pieces of cipher text and perform an operation on them which results in the cipher text of the concatenation of the two respective pieces of plaintext.

E. Private Information Retrieval

In cryptography, a private information retrieval (PIR) protocol [6] allows a user to retrieve an item from a server without revealing which item she is retrieving. It is also required that the user should not get information about other database items. In PIR, receiver receives one of the inputs (and possibly more), without sender getting to know what receiver asked for. As these encryption techniques are in emerging state, so in the near future they may open up new possibilities for cloud computing security.

VI. CONCLUSION

Cloud computing is most up-to-date development that provides straightforward access to high performance computing resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. It also offers a unique opportunity to developing countries to get closer to developed countries. In this paper we have discuss the issues related to hidden and encoded clouds access with anonymous access.

VII. ACKNOWLEDGEMENT

We wish to acknowledge faculty of Department of Computer Science and Engineering, Al Falah University, Faridabad, India and other contributors to prepare this paper. We would like to thank Er. Sanjeev Kumar Gupta, founder Director, Devansh Softech Consultancy Services Pvt. Ltd., Agra, INDIA for his most support and encouragement for their technical support in performing this task. He kindly read my paper and offered invaluable detailed advices on organization, and the theme of the paper. We could not imagine this paper possible without the help of all contributors.

REFERENCES

[1] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug. 2010.

[2] R. Maggiani; (2009), "Cloud computing is changing how we communicate," 2009 IEEE International Professional Communication Conference, IPCC 2009,Waikiki, HI, United states ,pp 1, 19-22 July.

[3] Grobauer, B.; Walloschek, T.; Stocker,E.;(2011), "Understanding Cloud Computing Vulnerabilities",5487489 searchabstrSecurity & Privacy, IEEE, Vol 9, pp 50.

[4] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010),"Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.

[5] Yuefa D; Wu B; Yaqiang G; Zhang Q; Tang C; (2009), " Data Security Model for Cloud Computing", Proceedings of the 2009 International Workshop on Information security and Applications (IWISA 2009)

[6] Jansen, W.A.; (2010), " Cloud Hooks: Security and Privacy Issues in Cloud Computing5719001 IEEE 2011 44th Hawaii International Conference on System Sciences (HICSS), pp1, 4-7 Jan. 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

[7] Tian L.Q; NI Y,LING; (2010) , "Evolution of user Behavior Trust in Cloud Computing", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010),Vol. 7,pp V7-567, 22-24 Oct. 2010.
[8] Mathur, P; Nishchal, N.; (2010), "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), pp 223.
[9] Dikaiakos, M.D; Katsaros, D.; Mehra, P.; Pallis, G.; Vakali, A.; (2010), "Cloud Computing Distributed Internet Computing for IT and Scientific Research".Vol.13 ,pp 10, Sept.-Oct. 2009.
[10] Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), "Cloud Computing Research and Development Trend", 2nd International conference on Future Networks, 2010. ICFN ' 10. pp 23, 22-24 Jan 2010.
[11] Dean and S. Ghemawat; (2010), "MapRduce: Simplified data processing large clusters", communication of the ACM, Vol.51, pages 107-113.
[12] Xue J; Zhang J.J; (2010),"A Brief Survey on the Security Model of Cloud Computing",2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.
[13] B.Michael,"In Cloud Shall We Trust?" IEEE Security & privacy,sept./oct.2009,p.3
[14] J.Boles,"Security and the Cloudy:A Revolution for the Infrastructure,"computer world oct.2008; http://blogs.computerworld.com/security-in-the-cloud.
[15] Establishing Truust in Cloud Computing Khaled M.Khan And Qutaibah Mulluhi,Qatar University
[16] D.Gambetta,"Can We Trust Trust?" Trust:Making and Breaking Cooperative Relations,Basil Blackwell,1988,pp.213-237
[17] S.perez,"In Cloud We Trust?" ReadWriteWeb, Jan.2009;www.readwriteweb.com/enterprise/2009/01/in-cloud-we-trust.php