Combined Security and Service Overloading Fusion Model for Cloud Environment

Ramesh Prasad Vishwakarma[1], **Dr. Sitendra Tamrakar**[2], **Rishi Kumar Sharma**[3]

1st IT Department, AISECT University, Bhopal, India

2nd CS Department, AISECT University, Bhopal, India

3rd CS Department, AISECT University, Bhopal, India

Abstract: ***Cloud computing is a field which has been rapidly developing over the past few years. The fact that cloud can offer both storage and computation at low amounts makes it popular among corporations and IT industries. This also makes it a very attractive proposition for the future. But in spite of its promise and potential, security in the cloud proves to be a cause for concern to the business sector. This is due to the outsourcing of data onto third party managed cloud platform. These security concerns also make the use of cloud services less flexible. In this paper, we propose a secure service overloading framework that allows data to be stored securely in the cloud while at the same time allowing operations to be performed on it without any compromise of the sensitive parts of the data.***

Keywords: Cloud Computing; Cloud Security; Searchable Encryption; Service overloading

Abstract: ***Cloud computing is a field which has been rapidly developing over the past few years. The fact that cloud can offer both storage and computation at low amounts makes it popular among corporations and IT industries. This also makes it a very attractive proposition for the future. But in spite of its promise and potential, security in the cloud proves to be a cause for concern to the business sector. This is due to the outsourcing of data onto third party managed cloud platform. These security concerns also make the use of cloud services less flexible. In this paper, we propose a secure service overloading framework that allows data to be stored securely in the cloud while at the same time allowing operations to be performed on it without any compromise of the sensitive parts of the data.***

Keywords: Cloud Computing; Cloud Security; Searchable Encryption; Service overloading

1. Introduction

Cloud computing has become the synonym of anything that involves delivering of services over the internet. The impact of cloud services on the business sector is tremendous. With the increase in the end-users, there is an increasing growth in the number of Cloud Service Providers (CSP) as well. The CSP is a third party that maintains and manages information about another entity. As users of both private and public sectors become more and more aware of cloud and it's plethora of services, they are searching for ways of making it more flexible and cost efficient. The strength of the cloud lies in that it offers both storage and computational power: a necessity for any company. Ideally, a company would want to use the CSP that provides the best package in their field of service. But as it happens, each CSP has different prices and strengths for each of their services and hence, a CSP who offers cheap storage may not offer good computation power. In such cases, a customer would opt to use multiple CSPs to make the best use of resources. Hence, in this scenario, one important factor that perhaps is given less importance is the security of data but the help of cloud service overloading technique (CSOT) we can reduce this problem.

Ironically, the main reason for customers still opting out of cloud is the potential vulnerability of cloud when it comes to security. The Cloud Security Alliance (CSA) [1] in a report has concluded that security threats like malicious insiders, data breaches, etc. still hamper the popularity of cloud. Major security concerns are privacy, integrity and confidentiality. Even in a single cloud, security is a major concern. However, this risk is multiplied when multiple clouds are involved. If there is data breach of a cloud user using multiple clouds for operations, it would be near impossible to determine at which CSP the data breach occurred or which malicious insider at which CSP sold this data. Hence, a possible solution is needed such that user can make use of multiple CSPs without fear of security breaches. In this paper, we propose a new approach (CSOT) to enhance security in cloud that particularly suits this scenario, ensuring that user can be sure of the security and confidentiality of their data.

The major problem in cloud is that when the user's data is stored on the cloud, the data could be physically located anywhere in the globe and it is not possible for the user to keep track of who has access to their data. Added to this is also the fact that storing raw data in the cloud implies an easy access to hackers and rivals, as the CSP's security offering would be the only barrier between these entities and the raw data. Since the cloud hosts millions of other users, it could be possible that one CSP could collude with any other person and sell users' data stored on the cloud. Unfortunately, this stored data may contain sensitive information, which is vital to the user's company or clients. The user loses direct control of his data and due to the raw nature of the data trusting the CSP becomes a rather forced choice.

Data in cloud could be broadly tagged as either static or computational. On the storage cloud, the data is at rest and in order to protect this data, the obvious option is to encrypt it. Encrypting this static data means, jumbling it up into gibberish that is unreadable or non-understandable. Several encryption algorithms have been proposed to be used for this purpose, the most popular being AES-256 bit. However, the disadvantage of conventional encryption standards is the need to decrypt the data before searching the same for partial retrieval. This search may be based on a small part of the data, such as any word or record. However, if decryption at the CSP is to be avoided, the only option left to the user is to retrieve the whole encrypted dataset, decrypt it, search and retrieve the necessary data, encrypt the data and store the same back in the cloud. In situations where it is necessary to retrieve a single user record from a database, this method would cause high overhead, since it requires the transfer of the data twice with additional cost for encryption and decryption. This overhead can only be avoided if there is a way to search on the encrypted data. Normal encryption schemes do not have the ability to search on encrypted data. To solve this problem Searchable Symmetric Encryption (SSE) [2] [3] [4] [5] was introduced. The advantage of this idea is to allow users to search for a word or record on encrypted text and retrieve that record. This saves a huge amount of time and effort taken by user.

When computation is required to be performed on the data, data is said to be dynamic, in other words, the value changes with every operation. In such cases, the data is expected to be raw for calculation. But as discussed, raw data is highly volatile. Conventional encryption encrypts the data, making it obtuse for hackers. However, it does not allow operations on it. A huge breakthrough while hunting for a solution was the introduction of Service overloading Encryption . The idea is that, data can be encrypted in such a manner that allows computation to be done on it. This computed encrypted data upon decryption, returns the same answer as computations done on raw data. Example: Elgamal is a partially Service overloading encryption that allows multiplications to be done on cipher texts. It has been proved that Elgamal can be extended to addition as well, although with some practical constraints.

Although solutions have been separately proposed for data at rest and data to be manipulated upon, it is important to identify a single system that handles both these cases simultaneously. This ensures the privacy of data in a multiple cloud environment. In this paper, it is proposed that it is enough to obscure only the sensitive part of the data, provided the protection mechanism is strong. By doing so, even if a malicious user gets hold of the data, the document’s integrity is not wholly lost, since the encrypted fields are not accessible.

We propose a solution that allows a user to search on encrypted data, retrieve and perform some computations on it. This approach lets the users decide what parts of the data they are willing to reveal to the cloud while securely hiding the sensitive parts. A combination of Searchable Encryption along with Partial Service overloading technique to support our proposal.

2. Related Work

In this section, literature survey is done for various Homomorphic Encryption methods and Searchable Encryption schemes.

Searchable encryption can be achieved in two ways: using an index or by sequential search. Dan Boneh et al. [2], Yanjiang Yang et al. [8] proposed related research in the Searchable Encryption field. Most of the work is based on creating an index of keywords for the searchable encrypted file and mapping the indexes to the words when searched. When data users input a keyword, a trapdoor is generated for this keyword and then submitted to the cloud server. A comparison between the trapdoor and index is executed by the cloud server when it receives the trapdoor. All the files/records, which this keyword is a part of, are sent to the data user. Sequential scan of encrypted data allows for controlled searching [9]. All practical implementations can be built using this scheme since it offers less complexity in search. Wang et al. [10] proposed an encryption technique using a secure ranked keyword search by combining inverted index with order - preserving symmetric encryption (OPSE). They employed numerical relevance scores technique to order the retrieved files. Although this method enhances system usability and saves communication overhead, it supports only single keyword ranked search and hence is not very useful for many applications.

Homomorphic cryptosystems can be broadly divided into two types: Partial Homomorphic systems and Fully Homomorphic systems. Fully Homomorphic systems are those systems, which do not have any limitation on the type of operation nor the number of operations that can be performed on the cipher texts. This is an ideal type of system and was considered impractical and was not even theoretically proved until in 2009, Craig Gentry [11], using lattice-based cryptography showed that fully Homomorphic system are theoretically achievable. However, this scheme did not allow for its implementation to be used practically as the complexity and length of cipher texts keeps increasing with increase in security levels. The key generated is also, too large. Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan [12] proposed the second Fully Homomorphic encryption scheme. This scheme uses many of the tools proposed in Gentry's construction, but does not require ideal lattices. This technique has almost the same efficiency as Gentry’s original proposition. The HElib, a library released in GitHub [13], implements the Brakerski-Gentry-Vaikuntanathan (BGV) [14] Homomorphic encryption scheme, along with many optimizations to make Homomorphic evaluations run faster.

A Homomorphic system having a limitation on the type of operation or the number of operations that can be performed on the cipher texts is called Partially Homomorphic. Examples of some such systems are RSA [15], Paillier [16] and Elgamal [7]. When an allowed operation on the encrypted data is restricted to only multiplication, it is said to be multiplicatively Homomorphic. Both Elgamal and Unpadded RSA are such systems. On the other hand Paillier is additively Homomorphic since addition operation can be performed on the encrypted data. Although original Elgamal is multiplicative, a variant of Elgamal [17] is proposed where it could be made additive. Likemost Homomorphic encryption mechanisms this also has a restriction on the size of the data that can be encrypted. This characteristic of Homomorphic encryptions essentially restricts the use of these mechanisms. However, it is observed that these mechanisms work well when applied on a smaller size of the data. In our work, we have used Elgamal Encryption and we have included the change to make Elgamal additively Homomorphic.

3. Service Overloading Fusion Model

In this model explains service overloading which is used to reuse different service in one situation. cloud is implemented by using service overloading. The pure virtual and non-virtual networks are used in static and dynamic service. These services overloading technique is used by base cloud. Service overloading is flexible as the multiple service can be used in single aspect.

- Overloaded cloud give network the flexibility to call a similar cloud for different types of service.
- Service overloading is done for service reusability, to save efforts, and also to save cost and provide more secure network.

It is a concept of service oriented network(SON). Service overloading is a SON concept that allows datacenter to define two or more service with the same name and in the same scope. Each service has a unique signature (or header), which is derived from: service / service ID name.

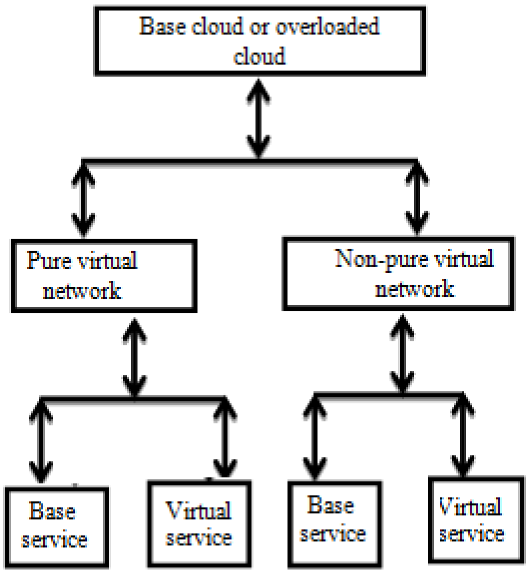

Figure 1: Service overloading architecture

4. Service overloading Technique

If any clouds have multiple services with same names but different parameters time then they are said to be overloaded. Service overloading allows you to use the same name for different range, to perform, either same or different service in the same cloud network.

“When you have a chance of defining the same cloud more than one time, so that you can use each individual cloud for a particular service, it is called service overloading.’

Service overloading is usually used to enhance the readability of the cloud security. If you have to perform one single operation but with different number or types of user or cloud, then you can simply overload the cloud.

"Overloading is the reuse of the same service name or network for two or more distinct user or operations". Service overloading is the general concept of service oriented network .A service can be declared more than once with different operations. This is called service overloading. It is the datacenter job which one is the right to choose. If it cloud service provider sense to you then I should say that one service name for different operations have the advantage of good readability of a cloud.

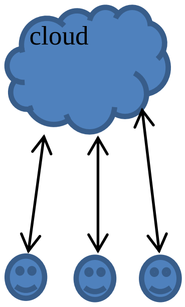

Figure 2: Simple cloud with data base services

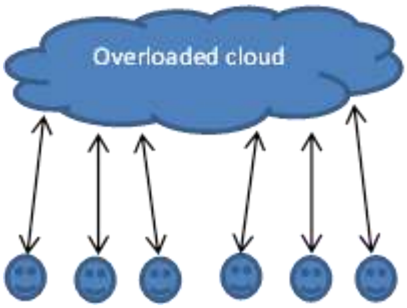

Figure 3: Cloud service overloading

Service overloading can be defined as same service or network will show different behaviors when different types of user.

5. Conclusion

In this paper we have presented a new areas of interest for the design of the cloud computing, service overloading. Service overloading area modern mechanisms that make it easier for a user to save data on cloud. Service overloading is a refinement and replacement technique for cloud network. A virtual network can also be declared and defined like any other service, but should be preceded by Base cloud but base service can also be done without virtual network or function.

References

[1] N. Saravanan and A. Mahendiran, “An Implementation of RSA Algorithm in Google Cloud using Cloud SQL,” *Res. J. Appl. Sci.Eng. Technol.*, vol. 4, no. 19, pp. 3574–3579, 2012.

[2] G. Aceto, A. Botta, W. de Donato, and A. Pescapè, “Cloud monitoring: A survey,” *Comput. Networks*, vol. 57, no. 9, pp. 2093–2115, Jun. 2013.

[3] W. Jansen, T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” *Natl. Inst. Stand. Technol. Spec. Publ. 800-144*, 2011.

[4] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[5] Daniel E. Geer, “Complexity Is the Enemy,”*IEEE Secur. Priv.*, vol. 6, no. 6, pp. 88–88, 2008.

[6] C. Rong, S. T. Nguyen, and M. G. Jaatun, “Beyond lightning: A survey on security challenges in cloud computing,” *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, Jan. 2013.

[7] J. Yang, and Z. Chen, “Cloud Computing Research and Security Issues,” in *IEEE Conf. Computational Intelligence and Software Engineering (CiSE)*, 2010, pp. 10–12.

[8] S. Surianarayanan, T.Santhanam, “Security Issues and Control Mechanisms in Cloud,” *Proc. Int. Conf. Cloud Comput., Tech., App. & Management*, 2012.

[9] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, “Multi-tenancy in cloud computing,” *Proc. - IEEE 8th Int. Symp. Serv. Oriented Syst. Eng. SOSE 2014*, pp. 344–351, 2014.

[10] G. Russell, R. Macfarlane, “Security Issues of a Publicly Accessible Cloud Computing Infrastructure,”*IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, *IEEE Computer Society*, pp. 1210-1216 , 2012.

[11] Craig Gentry, Fully homomorphic encryption using ideal lattices, Symposium on the Theory of Computing, pp. 169-178, 2009.

[12] vandijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V. Fully homomorphic encryption over the integers, 2009. http://eprint.iacr.org/.2009.

[13] Halevi, Shai. "An Implementation of homomorphic encryption", GitHubRepository, https://github.com/shaih/HElib, 2013.

[14] ZvikaBrakerski and Craig Gentry and VinodVaikuntanathan, Fully Homomorphic Encryption without Bootstrapping , Cryptology ePrint Archive, Report 2011/277, http://eprint.iacr.org/, 2011 .

[15] Rivest, R.; A. Shamir; L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. Feb 1978, vol. 21, no. 2, pp. 120-126, 1978.

[16] P. Pallier. Public-key cryptosystems based on composite degree residuosity classes. In Proc. of Eurocrypt vol. 1592 of LNCS, pages 223–238, 1999.

[17] Markus Jakobsson, Ari Juels, Addition of ElGamal Plaintexts, In Proc.
of the 6th International Conference on the Theory and Application of Cryptology and Information Security & Advances in Cryptology, pp. 346-358, 2000.

[18] Elgamal, Taher. "The Secure Sockets Layer Protocol (SSL)", http://www3.ietf.org/proceedings/95apr/sec/cat.elgamal.slides.html, 1975.