A Smart Encryption System for Cloud Evolving Security on Cloud

Priyanka[1], Khushboo Yadav[2]
M.Tech Scholar, Computer Science & Engineering, RPSGOI Mahendergarh[1]
Assist Prof, Computer Science & Engineering, RPSGOI Mahendergarh[2]
priyankamishracs@gmail.com[1], khushbooyadav000@gmail.com[2]

Abstract: Cloud Computing proposes a way to access applications over internet as utilities. It allows online creation, configuration and customization of applications. Data in world is increasing day by day and due to lack of space to store it, cloud computing is generated. The most basic issue in cloud computing is of security. As our Data is very precious to us and we don't want it to be hacked by someone else we need to secure it using some security algorithms. Sensitive data which is to be protected has to be encrypted before outsourcing to public cloud environment. This may be the only method to provide best security to our data even from the cloud provider. Encrypting our data may protect it up to some extent but this may cause problem in data storage efficiency and it's retrieval on server. In my thesis, some of the searchable encryption schemes are analyzed where the owner of the data i.e. the customer is self responsible for the security of his/her data. This scheme not only guarantee high security and efficiency but also allows fast and efficient data retrieval of the encrypted data. This paper describes a completely new method to safely save our data on cloud and easily retrieve it as analyzed in our thesis. This method may help to secure data on cloud in future.

Keywords: AES (Advanced Encryption System), Cloud Computing, Cloud Security, Encryption, SHA 512.

1. INTRODUCTION

With the rapid increment of data and databases, it is becoming a big task to secure and save data. So to solve the problem of space to store our data cloud computing is introduced. **Cloud Computing** proposes a way to access applications over internet as utilities. It allows online creation, configuration and customization of applications. The term Cloud refered as a Network or Internet or it can also be explained as something which is present at remote location is cloud. On public and private networks services can be provided using cloud. i.e. WAN, LAN or VPN. Cloud Computing is online manipulation, configuration, and access of the applications. Cloud computing offers applications, infrastructure and storage to data online. Now days, cloud computing is widely used to store data for longer time. The main issue is of security of data stored on cloud.

For securing our data many security algorithms may be used but the problems is that hackers decode it and our data becomes available to them. Other than this the cloud provider is the one who may access our data without our permission as he is the one who manages our data. So, we need a secure algorithmic method to make our data safe.

In the paper a completely new method is reveled to secure the data. This method includes encryption of data before uploading it on cloud environment so that the cloud provider will not be able to access our real data and in this way our data becomes safe even from the cloud provider. This method includes some presteps for security before encrypting it on user database, so that it become very hard for the intrupter to encode it without our

DOI: 10.141079/IJITKM.2016.915

permission. After that the encrypted data will be again encrypted at cloud uploading time and this way it becomes more secure. The complete process may be understood by the contribution part within the paper.

2. CLOUD COMPUTING & SECURITY:

Cloud computing indicates virtual servers available on the internet. It is the usage of computing resources like software, hardware or both. These resources are not owned by the application owners, but are hosted in data centers owned by a third party provider, in a consolidated manner. This frees the application owners of the computing resources from worring about the underlying technology and implementation details. They can ask for more or less resources on demand, and it is the responsibility of the third party provider to dynamically adjust to these requirements. Thus, application owners can just concentrate on the application on the application logic, and do not have to keep scaling up or down in terms of hardware infrastructure, personnel or software licensing. Instead, they can pay per use to the third-party provider.

Cloud Computing is online manipulation, configuration, and access of the applications. Cloud computing offers applications, infrastructure and storage to data online. Platform dependency issues are solved using cloud computing as using this there is not any need to install any software on your local PC. This way it is making our business applications collaborative. Deployment model and service model are the two types of models used to make cloud computing more reliable and feasible. Deployment models defines which type of access is provided to the cloud, i.e., how the cloud is located? There are four types of accessing cloud any one of them may be used for providing access to cloud: Public, Private, Hybrid and Community.

Public Cloud: To make systems and services easily available and accessible to the general public, public cloud is used. Public cloud may be less secure as it has a feature like openness, for example, e-mail.

Private Cloud: To make systems and services accessible within an origination, private cloud is used. It has increased security then public cloud as having private nature.

Community Cloud: To allow access of system and services to a group of organizations community cloud is used.

Hybrid Cloud: Mixture or Combination of public and private cloud is hybrid cloud. The difference is that the critical activities are accessed using private cloud and the non- critical activities are accessed using public cloud.

Service models- The reference models on which the Cloud Computing is based - can be categorized into the following three basic service models:

1. Infrastructure as a Service (IaaS)

2. Platform as a Service (PaaS)

3. Software as a Service (SaaS)

Different characterstics of cloud computing are as follows:

ON DEMAND SELF-SERVICE

On demand users are allowed to use web services and resources using cloud computing. One can logon to a website at any time and use them.

BROAD NETWORK ACCESS

Completely based on web so can be accessed from anywhere at any time.

RESOURCE POOLING

multiple tenants are allowed to share a pool of resources using cloud computing. Single physical instance can be shared of multiple resources like hardware, database and basic infrastructure.

DOI: 10.141079/IJITKM.2016.915

RAPID ELASTICITY

Scaling up and scaling down of resources is very easy and can be done at any time. Currently assigned or previously used resources of the customers are monitored automatically using cloud computing.

Technologies like virtualization, SOA (service oriented architecture), grid and utility computing are used in cloud computing. CSA model is used for data storage in cloud computing.

The subject of cloud security is still evolving, since cloud computing itself is still evolving. Collectively, a set of policies, technologies, and approaches that are needed to protect data, applications and cloud infrastructure is the area of cloud security. At a very high level, cloud security involves two parties: the cloud provider/host and the cloud client/user. The cloud platform could be provided by the host as an infrastructure, as a service, or as an application. Security is necessary in each case. Client's data and applications must be secure in cloud computing, especially because the client relies on the cloud provider much more than in a non-cloud application. Consequently, cloud security must deal with all aspects of securing data access, storage, application hosting and storage, user information, and authentication.

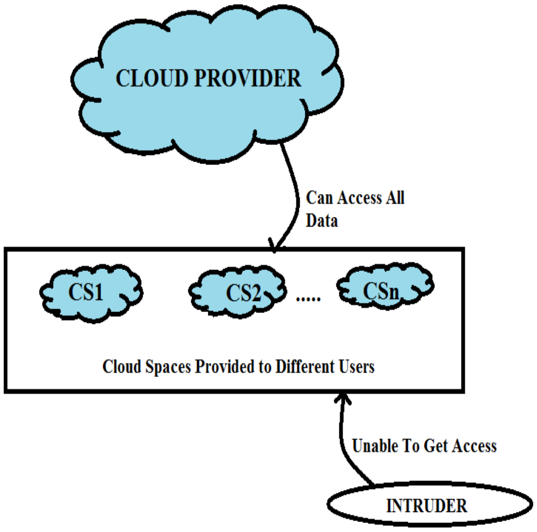
Cloud security deals with identity management, physical and personal security availability of data and applications, application security, and confidentiality.

3. CONTRIBUTION:

3.1 Problems Analyzed:

With the help of our study in the field of Cloud Computing we have found that there are several issues of security in cloud computing. These security issues are a big problem in the evolution of cloud computing. Security is the most basic thing every end user needs while sharing his/her data in the cloud environment or may be somewhere else. But if a cloud provider is not able to provide complete security to our data, we have to think twice before saving our data on that cloud database. It is necessary to provide more advancement while talking about the concept of cloud computing so that it may become more useful in future technology.

As if a data is previously encrypted on the customer's database it will be much secure providing it to the cloud provider. While uploading a file in cloud environment, this environment assures you that your data will be completely safe. No one else can get access to your data without your permission. Security to our data is provided by the cloud provider who is handling cloud management and providing space to our data on cloud. This security helps our data to become safe and not to be accessed by any intruder. But still there is a security issue. There is someone who may get access to our data without our permission and this is the cloud provider managing our all data.



When you store your data in cloud environment within a specific cloud provider, the cloud provider manages the security of our data and provide its access to you only i.e. the customer is the only person who may access his data. But it is possible that the cloud provider himself may read, delete, change or you may say that hack your data and mat misuse it. This data may get leaked and your personal data will not be personal anymore. This may be a big issue while uploading your data in cloud environment as your data may be very precious to you and you do not want it to be leaked in front of anyone as it may include any type of data like your financial information, your property or your bank's business property. You never want to share it to anybody. This may cause a big problem if this information get reveled in front of someone else even if it is a cloud provider. So before providing your data within a cloud environment, it is necessary to resolve these issues.

To resolve these issues we have generated a method which is discussed in "OURSOLUTION" part.

3.2 OUR SOLUTION:

We have analyzed the issues came in the field of cloud computing and tried to resolve this problem. This method may help to solve security issue. The paper proposes a completely new method to secure our data on cloud. Using this method may help to secure data on cloud in future. Even a cloud provider will not be able to get the original data and hence your data will be completely safe. This process is as follows:

There are some encryption steps helping in providing security to the file to be uploaded in cloud environment before and at the time of uploading the file. Performing this step by step will defiantly create a secure cloud environment.

Firstly, before uploading the file on the cloud we perform database encryption so that it may get secure from the cloud provider. In this process the data or the file goes through the following security method:

1) Tokenizer : Tokenizer creates tokens of the data i.e. tokenization is a process to create tokens of the whole data so that the next step of security may be performed on these tokens. The whole file is divided into small parts and these parts are then passed through the next security level.
2) Stock word removal: In this step, we have stock words already saved in our database and the tokens created in first step are traversed and compared with these stock words. If the token have those words which are in the stock word list then these words are removed from the token otherwise if not present the whole token remains as it is and passed to the next security level. For example we have a stock word list containing words: "is, life, always, be, some". This list is saved in the database of the customer who wants to upload his data on cloud environment. Now when a token "life is to stay happy always". This token is passed through the list stored in database and the words exist in the list are removed from the token and it becomes "to stay happy" which will be useless if got hacked. But if not any word matches to the words in the stock word list then the token is passed to the next level as it is. But normally we use to take those words in the stock word lists which are common in all sentences so that much security may be provided by removing these words from the list and making the sentence meaningless as removing these words the meaning of the sentence changes completely which is much difficult for the intruder to hack.

After these two steps, some more steps are used to enhance the security level of our data on user database and on cloud environment. These steps improve security up to a safe level where not even a cloud provider can access

DOI: 10.141079/IJITKM.2016.915

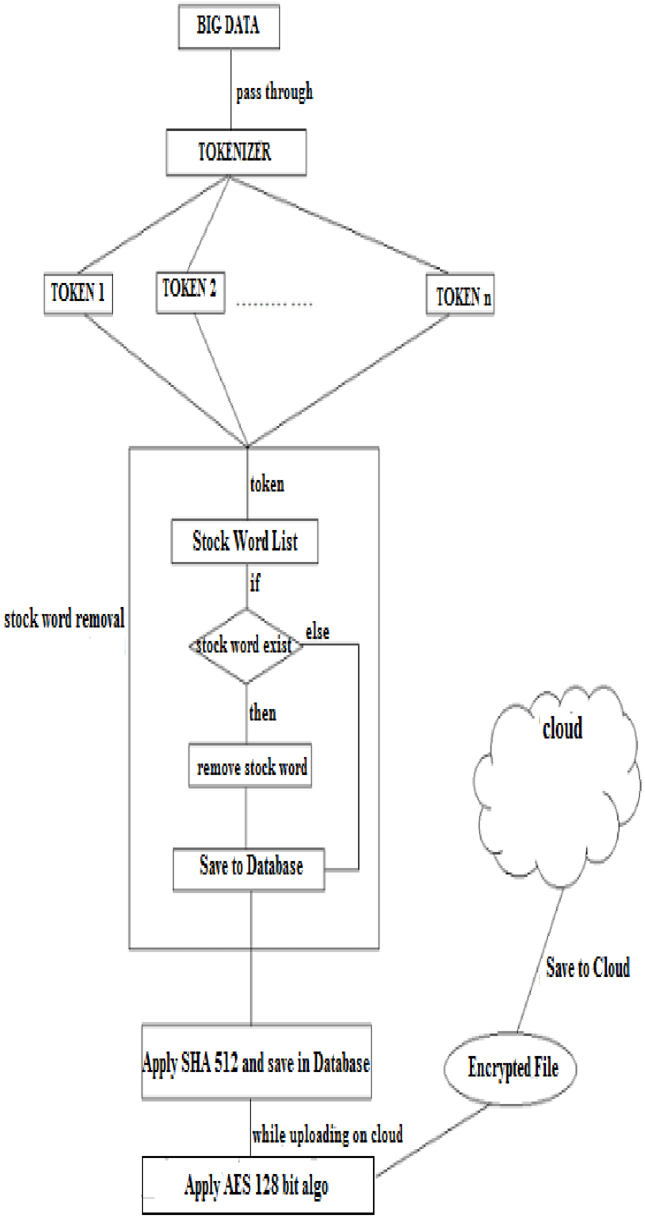
your original data. Within these steps the data goes through the following process:

The tokens are now encrypted using SHA 512 algorithm and then these are stored in the database. After encryption by SHA 512, the hash table is saved in the database and at the time of uploading the file on the cloud AES 128 bit encryption algorithm is applied on it and the encrypted file gets encrypted again. This encrypted file is uploaded on the cloud and will be safe to be hacked by anyone. No one else will be able to decrypt it as if he/she decrypt the file from cloud he will take only the encrypted tokens not the encrypted file and even if the cloud provider will access our data he will get the encrypted data and not the original data. The file needs the same decryption method to be in readable form and is possible only on the uploading system or by the person who knows the method to encrypt it and knows the stock words list removed from the file. The file on the server use AES and then uploaded on the cloud.

For more detailed information about SHA-512 & AES algorithms please refer to [2], [3] and the references therein.

Actually this system can be regarded as a prominent solution for the security of data on the cloud. This not only provides the method to save data securely on cloud but also makes a user possible to easily retrieve the data from the cloud knowing the time to retrieve it.

Here provided a proposed architecture for easily understanding all the work proposed by our thesis and is included in our paper. This architecture may help you understand the paper easily and within no time:



Proposed Architecture

The above architecture explains step by step process applied in the thesis to improve the security level of the data in cloud environment.

4. Future Work:

Cloud security is still evolving and there is a security issue in this. Cloud environment is best for data service outsourcing but there is security problem. Even if our data is safe from intruder, it is not still safe from the cloud provider. This is a completely new way to secure the data on cloud which includes data security from the cloud provider also and will help a lot to have safety of your data as it include both database and cloud server encryption. The main issue of security from the cloud provider may be solved using this method in future so it will be very helpful in cloud security evolution. Using this it will be very difficult or you may say next to impossible to crack the security of your data. Using this method may secure your data in future.

5. REFERENCES

[1]. SeongHan Shin, and Kazukuni Kobara. "Towards secure Cloud Storage." Available at http://googleweblight.com/?lite_url=http://engpaper.net/

[2]. M.Pitchaiah, Philemon Daniel and Praveen. " Implementation of advanced Encryption Standard Algorithm." International Journal of Scientific & Engineering Rsearch(IJSER) Volume 3, Issue 3, March-2012 ISSN 2229-5518

[3]. Priyanka Vadhera and Bhumika Lall. . "Review Paper on Secure Hashing Algorithm and its Variants." International Journal of Science and Research(IJSR) Volume 3, Issue 6, June 2014 ISSN:2319-7064

[4].Webpage: https://en.m.wikipedia.org/wiki/cloud_computing.

[5]. Harry Katzan, Jr.,Savannah State University, USA. " On An Ontological View Of Cloud Computing." Journal of Service Science-2010, Volume 3, Number 1.

[6]. Er. Ubeeka Jain , Ritika Trivedi. " A Review on the Security Issues in Cloud Computing Models." International Journal of Advanced Research in Computer and Communication Engineering, Volume 4, Issue 11, November 2015.

[7]. Brunette, G. and R. Mogull (ed)2009. “Security Guidence for Critical Areas of Focus in Cloud Computing” Cloud Security Allience, V2.1, December 2009.

[8]. Cavoukian, A. 2009. “Privacy in the Clouds” Toronto: Information and Privacy Commission of Ontario. www.ipc.on.ca.

[9]. Mell, P., Badger, L., and T. Grance. 2009b. “Effectively and Securely Using the Cloud Computing Paradigm.” National Institute of Standards and Technology, Information Technology Laboratory. 10-07-09.

[10]. Youseff, L., Butrico, M., and D. Da Silva. 2009. “Towards a Unified Ontology of Cloud Computing”.

[11]. Subashini, Subashini and V. Kavitha. “A survey on security issues in Service delivery models of cloud computing.” Journal of network and computer applications 34, no. 1 (2011): 1-11.

[12]. Idziorek, Joseph, and Mark Tannian. “Security analysis of Public cloud computing”. International Journal of Communication Networks and Distributed Systems 9, no. 1-2 (2012): 4-20.

[13]. Kaufman, Lori M. “Data Security in the World of cloud computing.” Security and Privacy, IEEE 7, no. 4 (2009): 61-64.

[14]. Ren, kui, Cong Wang, and QianWang. “Security Challenges for the public cloud.” IEEE Internet Computing 1 (2012): 69-73.

[15]. Sakr, Salam, An Liu, Daniel M. Batista, and Mohammad Alomari. “A Survey of large scale data management approaches in cloud

environments." Communications Survey & Tutorials, IEEE 13, no. 3(2011):311-336.

[16]. Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." In Services Computing, 2009. SCC'09. IEEE International Confernce on, pp. 517-520. IEEE,2009.

[17]. CSA (Cloud Security Allience), "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", December 2009.

[18]. ENISA (Europian Network and Information Security Agency), "Cloud Computing: Benefits, Risks and Recommendations for Information Security", November 2009.

[19]. CSA (Cloud Security Allience), "Top Threats to Cloud Computing V1.0", March 2010.

[20]. Rajesh Piplode, Umesh Kumar Singh. "An Overview and Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.