International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

An Approach for Efficient Utilization of Public Cloud Storage and Securing Data

Megha Prabhu[1], K Paramesha[2]

[1]*M. Tech Student, Department of Computer Science and Engineering, VVCE, Mysuru, India.*
[2]*Associate Professor, Department of Computer Science and Engineering, VVCE, Mysuru, India.*

Abstract - *Technology is evolving at a rapid speed. The infrastructure requirement of the enterprises is also changing with the evolution. One way to cope up with this is to make use of the cloud services rather than investing on the infractures and its maintenance. But we cannot outsource all our storage as we cannot trust the service provider completely. In this paper, we propose an approach for utilizing the public cloud storage space for storing our data in encrypted form. We also make use of secure servers maintained by the organizations or enterprises which can be trusted completely for the key management. By the combination of public cloud storage for storing data and use of secure servers for key management and authentication we propose an approach to achieve data security.*

Key Words: **public cloud storage, data security, secure server, cryptography, AES**

1.INTRODUCTION

We are in a world where each person generates a large set of data in his day to day life and would like to preserve the same and share it. With the growing amount of data, it is becoming difficult to store the data in the personal systems or hard drives. Each person comes across a point where he/she feels that the data they possess are important and should be preserved as it may need to be retrieved or shared with some other person at some point in time. As we all know the most precious thing in this digital world is the data and hence its storage and security are the main things to be considered.

Cloud computing is one such domain which provides solution for data storage and security concerns. Cloud provides services like IaaS, PaaS and SaaS. For data storage, we make use of infrastructure as a service. Cloud comes with three basic types namely private cloud, public cloud and the hybrid cloud. As we know, a lot of security measures will be at place in the private cloud. But when it comes to public cloud, security becomes a major concern for the data owner. Even though the public cloud storage provider offers a lot of safety and security measures, we cannot completely trust the public cloud. So, we need to make sure that the data that is stored in the public cloud is secure. We suggest an approach wherein we make use of the cryptographic techniques to secure our data, public cloud infractures for data storage and secure servers for key management and authentication. We come across many approaches where in different encryption mechanisms are used to encrypt the data and store it. Data encryption can be done using symmetric encryption technique or asymmetric encryption technique [1]. The decision on which technique must be used depends on the application in which it is implemented and the level of security expected. Initially, data encryption was done using DES techniques. It was used for a long duration by many organizations and agencies as an efficient and secure method for data encryption. Currently technologists are turning towards AES encryption methods [2] as it has been observed as efficient and secure method for data encryption. In our approach, we upload the encrypted data to the cloud and the key management is done at the secure server. We make sure that the server is secure by imposing certain policies on it. In this way, we can utilize the benefit of cloud storage at the same time be sure that our da-ta is secure as the keys required for decrypting the data files on the cloud resides with the system owner or the enterprise as it is stored in the secure server and is not uploaded in the cloud. This approach makes sure that the data in the cloud is secure even if it becomes accessible by other unauthorized authority because it cannot be decrypted unless they obtain the decryption key which is not available in the cloud.

2. RELATED WORK

Lot of work has been done and are going on in the field of cloud computing to make it robust against security attacks and at the same time improve performance. Mai Dahshan and Sherif Elkassass [3] suggested a framework for data protection on cloud. In this paper, they design a framework for confidentiality and fine grain access control. They make use of trusted third party service in their approach. In their approach, they made use of multi-authority cipher text policy attribute-based encryption method and attribute based signature method. They suggest double encryption of data before sending to cloud. Readers and writers have different access permissions. Writer can create, update and download the file whereas the reader can only download the file.

Ms. S. Vijaya Lekshmi and Mrs. M.P. Revathi [4] in their work suggest a method for implementing a secure data storage method for multiauthority access. They make use of proxy re-encryption and CP-ABE method. They also prove that their method is secure against chosen cipher text attacks. They suggest using database as a service and use certificate authorities in their approach.

Sujata Kattimani and Shikha Pachouly [5] in their approach suggest multi authority access control method for accessing data in cloud. They make use of threshold secret sharing and CP-ABE method for their approach. They made use of MD5 AES 128 with 16-bit encryption and certificate authority for authentication of data owner and user.

3. PRELIMINARY

In this section, we focus on core concepts used in this paper. We discuss about AES encryption, cloud, Infrastructure as a Service and secure communication techniques that are used in our approach.

3.1 AES Encryption

AES (Advanced Encryption Standard) algorithm is most widely used encryption technique for data security in todays connected world. It is a symmetric encryption algorithm which means same key is used for both encryption and decryption process. Even though same key is used for both the process, it provides the required level of security by the way it encrypts the data. It supports block length of 128 bits and key size of 128,192 and 256 bits. Joan Daemen and Vincent Rijmen in their work [6] clearly describe the AES encryption method. Implementation process, motivation for the design, its strength against know attacks and many other aspects are explained with great details.

3.2 Cloud

Cloud computing provides a set of scalable homogenous resources. It is a boon for many start-up organizations as it eliminates the need of huge initial investment on physical resources. They can go for pay-per-usage policy and avoid the initial set-up cost of large infractures. Cloud computing offers different types of cloud [7]. We can classify them as private cloud, public cloud and hybrid cloud. In private cloud, all the infrastructures are utilized and maintained for a dedicated organization. This is the most secure type of cloud as no resource is shared with external entities. When we say public cloud, it's obvious that we are sharing the physical resources with some other person or an enterprise. Even though virtually we are not sharing any of the resources or devices with unauthorized user, at the core level there are chances that an external person may get access to our data accidently or intentionally. This can occur because the security of the public cloud leis solely with the service provider and they might be providing service to different customers in the same cloud which can lead to security issues. This makes the public cloud semi-trusted. We can make use of the storage space provided by public cloud but at the same time we need to be rest assured that our data is safe even if some unauthorized user gets access to our data or a hacker tries to get hold of our data and try to decrypt it. Hybrid cloud is a combination of private and public cloud.

3.3 Infrastructure as a Service

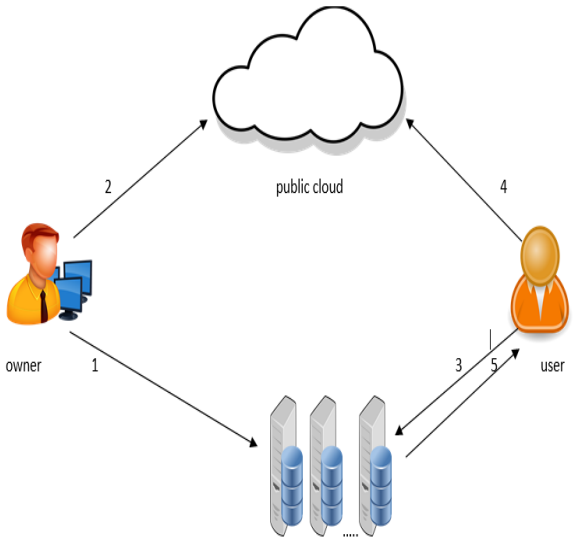
In Infrastructure as a service [8], the service provider provides storage, networks, processing capabilities and other vital resources. The users of this service will be able to deploy and run their application on the resources provided by the cloud service provider. Maintenance of the infrastructure used is the responsibility of the service provider. Users do not have any control on the infrastructure maintenance. But, the user has complete control on the applications and softwares they run on the infrastructure provided by the cloud vendor. Main advantage of using IaaS is that it supports dynamic scaling and the feature of pay only for the usage policy. Today's business needs demand for dynamic scaling of storage space. Large amount of data is gathered for analysis and processing which ultimately demand large storage space. We may not need a bulk storage space at all time. This makes the pay per usage option attractive. Thus, IaaS fits as a best choice considering these factors.

3.4 Secure Communication

As we are passing our data through internet, we need to check that our data is secure not only at storage but also when it is transmitted through different channels. To achieve this, network security parameters should be considered. Firewall and gateways should be setup appropriately to avoid hackers entering and stealing valid data [9]. We also need to make use of secure communicating layers and protocols to avoid data loss by intruders. We can make use of secure socket layer for communicating [10]. Other options include HTTP over SSL which is called HTTPS. Other alternative to HTTPS is secure HTTP(SHTTP). Depending on what kind of security mechanism we need to deploy for our application, we should decide on the communication protocols considering its pros and cons.

4. SYSTEM MODEL

In our paper, we suggest an approach through which we can securely pass our data to the cloud. We need to make sure that only encrypted data is passed to the cloud. The keys used for encryption process are stored on the secure serve locally. This assures that even if someone tries to get our data from cloud, it becomes impossible for them to decrypt the data as all the required information to decrypt the data is stored in the secure server. We also need to have complete access control over the secure server and we can call it as a trusted entity. If a person wants to access the data uploaded through this model, then he must get the token/key to login to cloud and view the available file. If a user wants to download or view any of the files, then he should obtain the corresponding decryption keys from multiple authorities from the secure server. User can decrypt the data only when he gets all the parts of the keys. This makes sure that even if one authority is compromised; it is not possible for an intruder to get hold of the actual data.



1. Owner registers with the secure server and obtains credentials to upload data to cloud.
2. Owner uploads encrypted data to cloud.
3. User registration and authentication.
4. User access cloud storage space and finds required data.
5. User obtains key to decrypt the data.

Fig -1: represents secure data storage and access model

Our model consists of 4 entities namely: user module, owner module, cloud, secure server.

1) Owner module: This module allows the authorized user to upload data to the public cloud storage space. Only users who are registered as owner can upload the data to cloud. The encryption details like the encryption algorithm and the keys used are not disclosed to the owner. This is handled by the application internally. The owner need not be available at all time as there is no dependency on the owner to allow access to other user to view and download data.
2) User module: This module allows user to register and login to view and download required data from the public cloud storage. The owner can only view the list of files available in the cloud. If that file must be viewed or downloaded, then the user should obtain the corresponding key from the secure server. The data can be decrypted only when all bits of the key are available. This makes sure that even if a single authority is compromised it is not possible to get hold of the content of the data.
3) Public cloud: This is a storage space on the cloud. It is always available and can be accessed by authorized user at any point in time. The security of the cloud solely lies with the cloud service provider. So, we assume that we cannot completely trust the public cloud service provider. There might be chances that our data from the cloud can be accessed by some third party intentionally or accidentally. We make sure that only encrypted data is uploaded to cloud and no details regarding decryption is stored in any part of the cloud.
4) Secure Server: This server plays a very crucial role in the entire system. We make sure that it's impossible to compromise security features of this server. It is always online. All the registration and authentication process are carried out in this server. This server must be maintained by the enterprise who want to use the cloud infractures purely for storage purpose. This approach will help any start up to save their investment on re-sources. They just need toned to maintain a couple of servers such that all the tables required for key management can be stored in this server. We use this approach because in cryptography keys play a vital role. If we make sure our decryption keys are placed in a secure place, we can be rest assured that our data is secure. To achieve this, we avoid storing keys in the cloud. We can secure our servers by imposing lot of security policies on it. We can go for application white-listing and black-listing [10], disabling different ports and by specifying what set of devices can be used for accessing this server along with user authentication [11].

5. DESIGN CONSIDERATIONS

In our approach, we want to make sure that confidentiality of the data is preserved. It is very important in to-day's competitive world to preserve the confidentiality of the data. Compromising with the data confidentiality factor can cause major damage to the data owner. We suggest an approach such that even if the data is obtained by a malicious user through the public cloud storage, it should not be possible to decode the data easily. Our encryption mechanism should be such that the time and money spent to acquire and decrypt the data by a malicious user should surpass the benefit they can attain by accessing the data. In this approach, all the individuals who access this system should register them-selves with the secure server where the application will be hosted. The authorities in the secure server have all the privileges to accept or reject any individual trying to register. The owner of the data must login with his credentials to upload a file to the public cloud storage. As soon as the data owner opts for uploading a file to public cloud, the data is encrypted using AES technique be-fore it is transmitted through secure channel to the cloud storage. This makes sure that the data security process starts before the data leaves from the owner system to enter the cloud environment. As the data is encrypted before transmission and as we make use of secure communication protocols, it becomes difficult for an intruder to get hold of the actual plain text. When a user wants to know the available file in the cloud, the user should first enter a token key which

would be unique for each user. The authorities should send a token key to the registered email id of the user. The user must enter this token key to view the list of files available in the cloud storage. Next, if the user wants to access any file from this list then he should request for the key from the authorities of the secure server. The multiple authorities or the secure server hold all the keys, registration details and the privilege to accept or reject any new registration. So, it is assumed that the secure server is a trusted entity and is always available. The decryption keys will be sent to multiple applications in parts which are registered by the user. This will make sure that even if any-one application credentials of a user are compromised, it's not possible to access the data. The user should enter all the bits of the key sent to multiple registered applications to decrypt and view the data. This method is considered to avoid data confidentiality loss due to com-promise of any application credentials.

6. CONCLUSION

In this paper, we have proposed an approach for developing a secure way to store data in public cloud storage using cryptographic techniques. We also make use of security concepts like application blacklisting and whitelisting to secure our server that performs the vital tasks of key management and authentication. We also suggested the use of AES encryption technique for encrypting our data. Our approach suggests to maintain all authentication and key management details at a server which is completely secure and not part of the public cloud infractures. We do not make use of any certifying authority to authenticate the data owner or the data consumer. All the rights to provide access to the public cloud storage solely lies with the multiple authorities who take care of the secure server through the pre-defined set of policies. Future work in this topic will reflect the actual implementation details. It can also show the simulation result on performance and security aspects.

REFERENCES

[1] William Stallings, Cryptography and Network Security, Pearson 6th edition, 2013.

[2] M.Pitchaiah, Philemon Daniel and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

[3] Mai Dahshan and Sherif Elkassass, "Framework for Securing Data in Cloud Storage Services", published in 2014 11th International Conference on Security and Cryptography (SECRYPT), Year: 2014, pp: 1 - 8

[4] Ms. S. Vijaya Lekshmi and Mrs. M.P. Revathi, "Implementing Secure Data Access Control for Multiauthority Cloud Storage Sys-tem Using Ciphertext Policy-Attribute Based Encryption", pub-lished in International Conference on Information Communication and Embedded Systems , Year: 2014, pp: 1 - 6, DOI: 10.1109/ICICES.2014.7033749

[5] Sujata Kattimani and Shikha Pachouly, "A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", 2016 International Conference on Computing Commu-nication Control and automation (ICCUBEA), Year: 2016, pp: 1 - 4, DOI: 10.1109/ICCUBEA.2016.7860064

[6] Joan Daemen andVincent Rijmen, "AES Proposal: The Rijndael Block Cipher" , NIST Computer Security Resource Center

[7] Rajkumar Buyya, James Broberg and Andrzej M. Goscinski, "Cloud Computing: Principles and Paradigms", john wiley and sons, inc., publications.

[8] Dan C Marinescu, Cloud Computing Theory and Practice, Else-vier(MK)2013.

[9] https://security.berkeley.edu/resources/best-practices-how-articles/securing-remote-desktop-rdp-system-administrators

[10] http://searchsecurity.techtarget.com/definition/application-blacklisting

[11] John E. Canavan, Fundamentals of network security