International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 02
February 2020

Cloud Security Ecosystem for Data Security

Rajesh Kumar S[1]

[1]Assistant Professor, Department of Computer Science and Engineering, Cambridge Institute of Technology, Bangalore, Karnataka, India.

Abstract: *In the past couple of years Cloud Computing has become an eminent part of the IT industry. Because of its economic benefits more and more people are heading towards Cloud adoption. In present times there are numerous Cloud Service providers (CSP) allowing customers to host their applications and data onto Cloud. However, Cloud Security continues to be the biggest obstacle in Cloud adoption and thereby prevents customers from accessing its services. Various techniques have been implemented by cloud service providers in order to mitigate risks pertaining to Cloud security. In this project, we present a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption thus resulting in a secure Cloud environment. The project focuses on creating a secure Cloud ecosystem wherein we make use of multifactor authentication along with multiple levels of hashing and encryption. The proposed system along with the algorithm are simulated using the CloudSim simulator. To this end, we illustrate the working of our proposed system along with the simulated results.*

1. Introduction

In today's times, Cloud computing has a significant impact on the IT industry[1]. With growing popularity, more and more organizations are making use of cloud services. Although cloud services have widespread acceptance of the fear pertaining to the security and privacy of these services continues to be an open challenge. With rapid technological advancements, these services could be easily accessed through smartphones thus allowing users to share pictures, videos, documents, and other important data across various platforms on a real-time basis. However, a security breach in their cloud account could lead to stolen data which would indeed result in huge losses.

Security has always been a concern in the domain of information technology. With Cloud services handling critical data that can be accessed from anywhere through the internet makes security a prominent concern. The pervasive nature of Cloud and its disbursal of data across various geographical locations amounts to high-security risks[1]. While talking of Cloud Security there are many aspects which one needs to consider such as, trusted authentication, appropriate authorization, data security, and privacy. These are some of the basic security goals which are extremely essential for every cloud provider to incorporate. Since security has been seen as an attribute for information technology, data encryption has been one of its key measures in ensuring data security protection. Many algorithms in the past have been proposed for conducting efficient data encryption. These algorithms range from Diffie-Hellman, RSA, DES to AES, RC4, and 3DES. Each of these algorithms has its own advantages along with its demerits. These algorithms are broadly classified as being symmetric or asymmetric in nature.

2. Existing System

Several security threats are associated with cloud data services, not only traditional security threats, such as network eavesdropping, illegal invasion, and denial of service attacks, but also specific cloud computing threats, such as side channel attacks, virtualization vulnerabilities, and abuse of cloud. Many solutions have been proposed to provide security measures using one or the other algorithms listed below.

2.1 Systems using RSA

It is an asymmetric cryptography algorithm. Asymmetric is it works on two keys i.e. Public key and Private Key[2].

Example:

- A client sends its public key to server and requests for some data.
- Cloud server encrypts the data using public key and sends the encrypted data.
- The private key with client is used to decrypt the data.

2.2 Systems using AES

It is the most popular and widely adopted symmetric algorithm, Stronger and faster than 3DES, when it comes to cyber security, AES is one of those acronyms that you see popping up everywhere. That's because it has become the global standard of encryption and it is used to keep a significant amount of our communications safe.

The Advanced Encryption Standard **(AES)** is a fast and secure form of encryption that keeps prying eyes away from our data[2].

3. Drawback of Existing System

Each algorithm has its own drawback and none of the existing solutions provide security measures at all the levels of user/system operations.

3.1 Drawbacks of RSA

- RSA Algorithm can be very slow in cases where large data needs to be encrypted by the same computer.
- It requires a third party to verify the reliability of public key.
- Data transferred through RSA algorithm could be compromised by middleman who can tamper with the public key.

3.2 Drawbacks of AES

- It uses too simple algebraic structure.
- Every block is always encrypted in same way. AES in counter mode is complex to implemented in software taking both performance and security into considerations.

4. Proposed System

The focus of this paper would be to create a Secure Cloud Ecosystem that leverages from the benefits of both symmetric and asymmetric encryption. Make use of RSA (Asymmetric) and AES (Symmetric) algorithms for carrying out data encryption. We aim at creating a comprehensive Cloud. An environment that has security measures at all levels from creating and storing username and password, multifactor authentication, transmission of user data and data encryption, It uses RSA (Asymmetric) and AES (Symmetric) algorithms for carrying out data encryption. It creates a comprehensive Cloud Environment that has security measures at all levels from creating and storing username and password, multifactor authentication, the transmission of user data and data encryption.

5. System Architecture

System Architecture contains several subdivisions as show in Fig. 5.1, where the modules in the rightmost contain the important architecture. The modules are Security Services, Trusted Authentication, Authorization, Data Encryption, Key Management, Hashing, and Data Privacy.

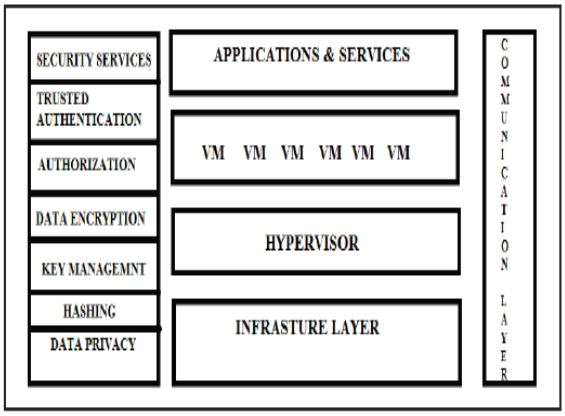

Fig. 5.1: Architeture of cloud security ecosystem.

The infrastructure layer contains the major hardware components that are required to run the program. Applications & Services is the upper layer that runs the project in our project the application is accessed through a web browser. The Security services provided by the project contains encryption of data before storing the data into the cloud, there contains login as well as two-factor authentication for an additional layer of security for the ecosystem.
Hashing module is used to hash the password before storing the password into the database within the server which is also considered as a security measure. The key management module is used for managing the encryption keys used to encrypt the data. The Keys can be added as well as removed by the user[3].

5.1 System Design

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. If the broader topic of product development "blends the perspective of marketing, design, and manufacturing into a single approach to product development," then design is the act of taking the marketing information and creating the design of the product to be manufactured. Systems design is therefore the process of defining and developing systems to satisfy specified requirements of the user.
System design is one of the most important phases of software development process. The purpose of the design is to plan the solution of a problem specified by the requirement documentation.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 02
February 2020

In other words, the first step in the solution to the problem is the design of the project. The design of the system is perhaps the most critical factor affecting the quality of the software. The objective of the design phase is to produce overall design of the software.
It aims is to figure out the modules that should be in the system to fulfill all the system requirements in an efficient manner. The design will contain the specification of all these modules, their interaction with other modules and the desired output from each module. The output of the design process is a description of the software architecture.

5.2 Modules in the Proposed System

The figure shows a general block diagram describing the activities performed by this project. The entire architecture has been implemented in nine modules as shown in the Fig. 5.2.

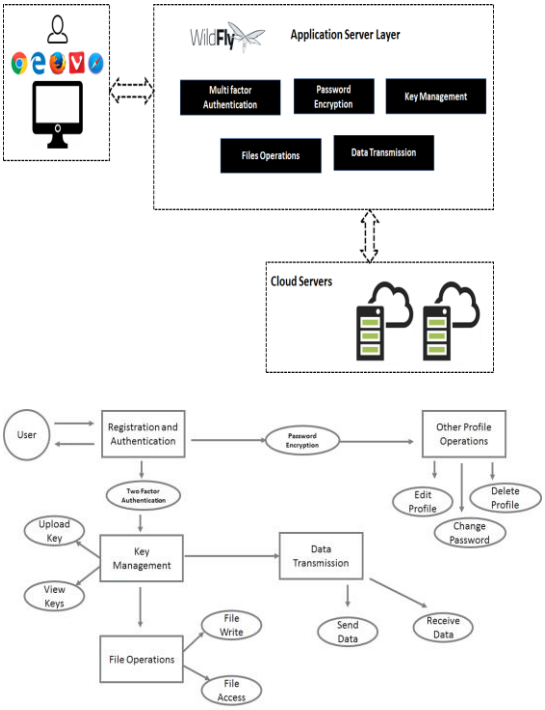

Fig. 5.2 Modules in Proposed System.

User Account Module: This module provides the users of our project with a user interface to get access to our project. A user can create an account after which he will be able to access his/her account. Other operations a user can perform on his account are log in, Logout, edit profile, delete profile, change password and retrieve the password in case he/she forgot. Only the admins of the project whom we consider as the owners of the SQLiID portal will be performing this operation. Even the users who own the project can be able to change their profile password, email and other details.

File Write: This module allows the users to perform the file write operation on the cloud. The user will be provided with an HTML interface where they can browse the file to be uploaded to the cloud. It is mandatory for the users to upload at-least one of their secret keys before accessing this module. The users will then be provided with an option to select any of the keys uploaded by them which has to be used for performing the hybrid cryptography on the file he/she has uploads as show in the Fig. 5.2.1.

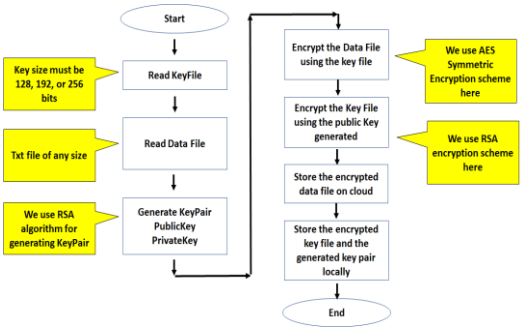

Fig 5.2.1: File Write Operation.

File Read: This module performs the file read operation from the cloud and performs the decryption operation using the hybrid cryptographic system with the same key used for encryption.

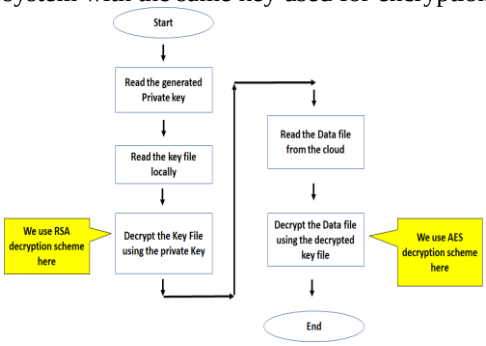

Fig 5.2.2: File Read Operation.

Data Transmission: This module is implemented for demonstration purpose only. When the end users send any confidential data from their devices: typically a laptop or desktop, to the cloud application, there are some possibilities that the hacker or the third party can steal the confidential data during the data transmission from the client

device to the cloud application. To avoid this, the confidential data must be encrypted from the client end (laptop/desktop) itself before the data transmission begins. This module allows the users of our portal to experience how this kind of security has been implemented.

Password Security: During the registration phase, the end users are going to select their passwords for their accounts. All the profile information including the password will be stored in the relational database management system like MySQL. However, there are chances that the attacker might compromise the RDBMS. In such situations, the attacker will also get an access to the user's password and hence bypassing the security layer of the cloud application. To avoid this, the user's password will not be stored as a plain text on MySQL, instead it will be stored as an encrypted text[4].

Two-factor authentication: Often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password. Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords[2].

Key Management: This module helps the users of our portal to manage their secret keys. The users will be provided with an interface to upload their secret keys. The secret key must be in multiples of 128 bits. The users will also be provided with an interface where they can view the list of all the keys uploaded by them and also they can perform other operations like downloading the keys and deleting the keys in case they no longer need it. It is mandatory for the users to upload at least one key before they proceed further for data write operation. However, there is no limit on the number of keys the user can upload in our portal.

Conclusion

In the past couple of years Cloud Computing has become an eminent part of the IT industry. Because of its economic benefits more and more people are heading towards Cloud adoption. In present times there are numerous Cloud Service providers (CSP) allowing customers to host their applications and data onto Cloud. However, Cloud Security continues to be the biggest obstacle in Cloud adoption and thereby prevents customers from accessing its services. Various techniques have been implemented by cloud service providers in order to mitigate risks pertaining to Cloud security. In this paper, we presented a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption thus resulting in a secure Cloud environment. The paper focused on creating a secure Cloud ecosystem wherein we make use of multifactor authentication along with multiple levels of hashing and encryption.

Future work

In future we wish to incorporate definite steps that would enhance the efficiency and generality of our system. This could be in form of extending our system to work for a multi cloud environment and add certain backup and recovery features which would prevent data loss in case of an attack.

References

[1] Khanna, Abhirup, Sarishma. (2015). Mobile Cloud Computing: Principles and Paradigms. IK International.

[2] Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).

[3] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[4] Singh, Aarti, and Manisha Malhotra. "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review." International Journal of Computer Networks and Applications 2.2 (2015): 41-45. 292 2017.

[5] Suli Wang, Ganlai Liu. "File Encryption and Decryption System based on RSA algorithm" 2011 International Conference on Computational and Information Sciences 10.1109/ICCIS.2011.150