

Cloud Computing Security Using RSA & AES

Sweta H Meshram¹ Manisha D Badwaik² Chetana N Kore³ Reshma S Neware⁴ Deepak Bhiogade⁵

^{1,2,3,4}Student ⁵Assistant Professor

^{1,2,3,4,5}Department of Computer Engineering

^{1,2,3,4,5}MPCE Bhilewada, Bhandara, India

Abstract— Presents Hybrid (RSA & AES) encryption algorithm to safeguard data security in Cloud. Security being the most important factor in cloud computing has to be deal with great precautions. This paper mainly focuses on the following key tasks:

1. Secure Upload of knowledge on cloud such even the administrator is unaware of the contents.
2. Secure Download of data in such a way that the integrity of data is maintained.
3. Proper usage and sharing of the general public , private and secret keys involved for encryption and decryption.

The use of one key for both encryption and decryption is extremely prone to malicious attacks. But in hybrid algorithm, this problem is solved by the utilization of three separate keys each for encryption as well as decryption. Out of the three keys one is the public key, which is made available to all, the second one is the private key which lies only with the user. In this way, both the secure upload as well as secure download of the data is facilitated using the two respective keys. Also, the key generation technique used in this paper is unique in its own way. This has helped in avoiding any chances of repeated or redundant key.

Keywords: Cloud computing, AES, RSA, Computing Services

I. INTRODUCTION

Cloud computing is that the results of the evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to al technologies, without the necessity for deep knowledge about or expertise with all of them. The cloud aims to chop costs, and helps the users specialize in their core business rather than being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the method through which the user can provision resources on-demand. By minimizing user involvement, automation accelerates the method, reduces labor costs and reduces the possibility of human errors. Cloud Security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

The conception of cloud computing is associated closely with the infrastructure as a services (IaaS), platform as a services (PaaS), System as a services (SaaS).

Cryptography, in modern days is considered combination of three types of algorithms.

They are

- 1) Symmetric-key algorithms
- 2) Asymmetric-key algorithms and
- 3) Hashing. Integrity of data is ensured by hashing algorithms.

A. Public Cloud:

The most recognisable model of cloud computing to many consumers is the model, under which cloud services are provided in a virtualised environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

B. Private Cloud:

Private clouds are those that are built exclusively for a single business. For many companies considering cloud computing, private clouds are a good starting point. They allow the organization to host applications, development environments, and infrastructure in a cloud, while addressing concerns regarding data security and control that can arise in the public cloud environment.

C. Community Cloud:

The cloud foundation is imparted by numerous associations and backings a specific group that has imparted issues (e.g., mission, security necessities, arrangement, and consistence contemplations). Hybrid cloud: A hybrid cloud is generally best-of-breed. It combines the comfort level of a private cloud with the flexibility and versatility of the public cloud. Hybrid platforms use either public clouds or off-site Hosted Virtual Private Clouds for some applications and processes. They merge these with on premises private clouds for high security application environments to leverage the best of both worlds.

II. SECURITY ISSUES OF DATA PRIVACY IN CLOUD

The six issues that must be addressed are:

- 1) Breach notification and data residency:
- 2) Data management at rest
- 3) Data protection in motion
- 4) Encryption key management
- 5) Access controls
- 6) Long-term resiliency of the encryption system
 - a) Host security issues The host running the job, the job may well be a virus or a worm which can destroy the system from malicious users
 - b) Network security issues Denial of Service: where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a