



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

A Secure Framework for User Data Storage in Public Cloud Systems using Symmetric Cryptography

Reetika Singh¹, Rajesh Tiwari²

¹Research Scholar, Faculty of Engineering & Technology, ²Faculty of Engineering & Technology
Department of Computer Science & Engineering, Shri Shankaracharya College of Engineering & Technology,
Chhattisgarh Swami Vivekanand Technical University, Bhilai - 490006, Chhattisgarh, INDIA

Abstract: Cloud computing is a paradigm shift over the Internet which provides instant access to software, hardware and computing information resources for use when they needed. Cloud Computing is the access of data, software applications and computer processing power through a “cloud” of online resources. Cloud computing involves storage of user data in the cloud. Cloud architectures will constitute cost efficient mechanism that will support the storage, transmission and processing of the user application contents. A user can access cloud service as a utility service. The diversity of the services delivered through the cloud and sharing the distributed resources via network in the open environment results in a challenge to ensure that only authorized users can gain access to it. Thus, there is a critical need to have a secure framework for ensuring confidentiality and integrity of stored data in cloud. To ensure the data security, we proposed a method for efficiently storing and data in a cloud infrastructure by building secure channels for data communication.

Keywords: Cloud Computing, Data Storage Security, Symmetric Encryption, Data Confidentiality and Integrity

I. Introduction

To meet ever changing business needs in computing resources and advances in networking technologies, organisation needs to invest time and money to scale up their infrastructure to outsource their storage and computing needs. On – premise IT infrastructure results in low scaling. Cloud computing is a paradigm in which resources in the computing infrastructure are provided as a service over the Internet. Organization simply connect to the cloud and can use computing resource on pay-per-use method which reduces organization’s capital expenditure and can scale up or down the IT infrastructure as per the business need. Cloud computing is a result of gradually development of providing services by forming clusters and grids of computers. Cloud computing primary significance lies in allowing the end user to access computation resources through the Internet and it is gaining popularity because of its scalability, instant access and can save money. Cloud computing is an innovative technology that facilitates the networked nodes to share the pooled resources on demand in pay per use model. Resources could be a simple software application, a platform needed for project development or the infrastructure itself using Internet as the backbone. The various security issues of cloud computing due to its service delivery models. Some of the fundamental security challenges are data storage security, data transmission security, application security and security related to third party resources [4]. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible [8]. All the data security technique is built on confidentiality, integrity and availability of these three basic principles of information security [1]. Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [5]. The common solution for data confidentiality is encryption. The novel method of selecting the encryption algorithm is to have an algorithm that has speed and computational efficiency for handling encryption of large volumes of data which is in this paper is symmetric encryption algorithm. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand. The primary purpose of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud, by separating applications from operating systems, from the hardware that runs everything from themselves. This capability is provided by a web application through which one can access the application on another system through web browser. In this paper, we address the main security challenge to cloud – Data Storage Security. The paper covers some aspects of major challenging problems for implementing security for networked storage from the perspective user in cloud environment which includes –

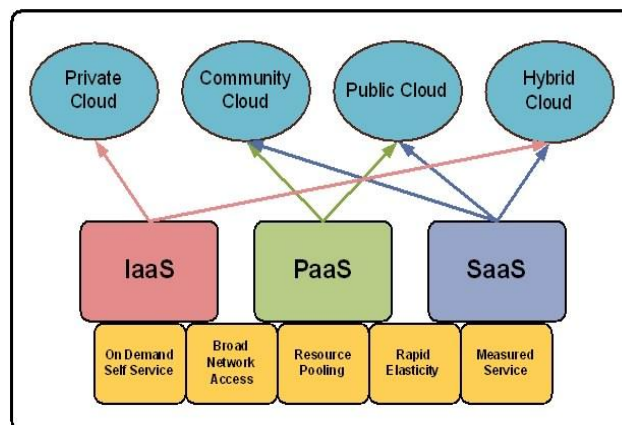
- The problem of incorrect storage of data in cloud.
- The data stored in cloud may be updated by the user.
- The sensitivity of data needs to be maintained.
- To enable users to perform storage correctness checks with minimum overhead.

II. Cloud Computing

A. Introduction to Cloud Computing

Cloud computing is creating a fundamental change in computer architecture, software and tools development and in way for storage, distribution and consumption of information. Cloud computing is like a hosted services where servers, storage and networking infrastructure are shared across multiple tenants and over a remote connection with the ability to scale. A cloud is a powerful combination of cloud computing, networking, storage, management solutions, and business applications that facilitate a new generation of IT and consumer services. These services are available on demand and are delivered economically without compromising security or functionality. Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing is broken down into three segments: application, storage and connectivity. End users access cloud-based applications through a web browser or a light-weight desktop or mobile app while the business software and user's data are stored on servers at a remote location [10]. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and the system software in the data centers that provide those services [6]. A computing Cloud is a set of network, enabled services, providing scalable, QoS guaranteed, normally personalized inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way [7]. Cloud computing is conceptually viewed as a paradigm where software applications, data storage and processing capacity are accessed over the Internet by thin or thick client platforms. As per National Institute of Standards and Technology, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (Rapid Elasticity, Measured Service, On-Demand Self-Service, Ubiquitous Network Access, Location-Independent Resource Pooling), three delivery models (Software as a Service, Platform as a Service, and Infrastructure as a Service), and four deployment models (Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud)." Figure 1 shows the five essential characteristics of cloud, three building blocks of cloud and its three deployment models.

Figure 1 Three Aspects of Cloud Computing.



B. Problem Identification

Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network. In public cloud infrastructure, storage services provides customer with scalable and dynamic storage. Data Security for Storage-as-a-service cloud service encompasses several aspects including secure channels, access controls and encryption. In cloud storage model, data is stored on multiple virtualized servers. Physically the resources will span multiple servers and possibly can even span storage sites. Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites. Since cloud computing share distributed resources via network in the open environment thus it makes security problems. Security, availability and reliability are the major quality concerns of the cloud user. Authentication and identity, access control, encryption, secure deletion, integrity checking, and data masking are all data protection methods that have applicability in cloud computing. Cloud computing facilitates storage of data at a remote site to maximize resource utilization. As a result, it is critical that this data be protected and only given to authorized individuals. Within the cloud computing world, the virtual environment lets user access computing power that exceeds which is contained within their own physical worlds. Cloud computing environments are multi-domain environments in which each domain can use different security, privacy, and trust requirements [3]. One of the most significant problems is data security in the field of Cloud Security. In the Cloud Computing environment, important data, files and records are entrusted to a third party, which enables data security to become the main security issue of Cloud Computing. Despite the potential

benefits and revenues that could be gained from the cloud computing model, the model still has a lot of open issues (obstacle/opportunity) that impact the model creditability and pervasiveness [2]. Obstacles are listed in Table 1 as under:

Table 1 Top 10 obstacles to and opportunities for growth of cloud computing [2].

Obstacle	Opportunity
1 Availability/Business Continuity	Use Multiple Cloud Providers
2 Data Lock-In	Standardize APIs; Compatible SW to enable Hybrid Cloud Computing
3 Data Confidentiality & Auditability	Deploy Encryption, VLANs, Firewalls
4 Data Transfer Bottlenecks	FedExing Disks; Higher BW Switches
5 Performance Unpredictability	Improved VM Support; Flash Memory; Gang Schedule VMs
6 Scalable Storage	Invent Scalable Store
7 Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs
8 Scaling Quickly	Invent Auto-Scaler that relies on ML
9 Reputation Fate Sharing	Offer reputation-guarding services like those for email
10 Software Licensing	Pay for use license

The problem of data security consists of providing secure channels, access controls and ensuring the secure data storage in the cloud hosted environment. The effective and flexible distributed scheme should be designed for cloud data storage, which aims to ensure storage correctness, fast localization of data error, dynamic data support, dependability and lightweight. The scheme assumes that the point to point communication channels between every cloud provider and customer is authenticated and reliable.

III. Cloud Computing Security Challenges

Cloud Computing and web services run on a network structure so they open to network type attacks. Data Security is a crucial element that warrants scrutiny. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. The cloud services present many challenges to an organization. When an organization mitigates to consuming cloud services, and especially public cloud services, much of the computing system infrastructure will now under the control of cloud service provider. Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization. Although proper security controls must be implementing based on asset, threat, and vulnerability risk assessment matrices, Cloud computing security risk assessment report is mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud. Data security (Privacy & Confidentiality) at public deployment of cloud includes security risks lists for:

- Privileged User Access.
- Data in Transit.
- Data at Rest.
- Data in Processing.
- Data Segregation.
- Data Integrity.
- Data Recovery.
- Long term viability.

The cloud computing is a virtual environment that requires data transfer throughout the cloud. To ensure data confidentiality, authentication, integrity, and availability, the provider should include the following: Encryption, Physical Security, Authentication and access control, Separation of duties and Intrusion Detection and prevention. In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. Thus security imposed on data by encryption prior to storage of data, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [1], [6]. Table 2 shows the proposed data security aspect at each phase of data life cycle from its generation to destruction as under:

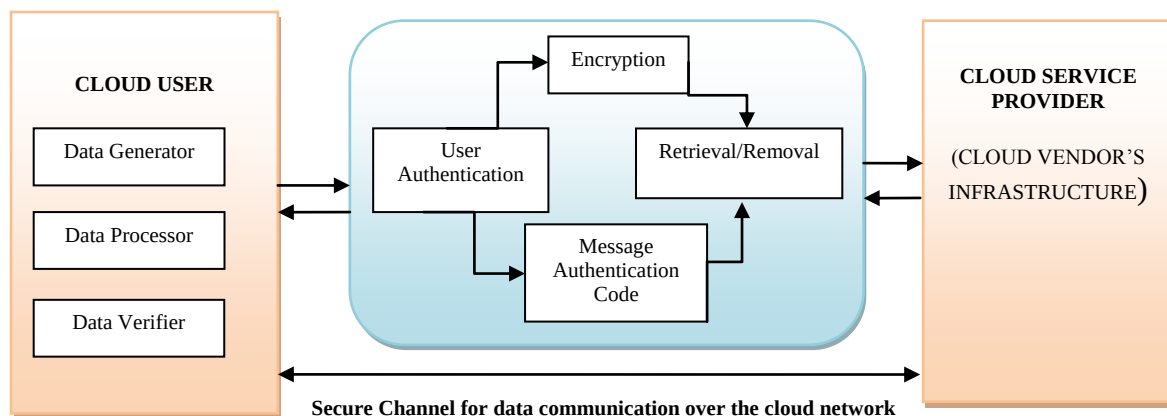
Table 2 Proposed Data Security Mechanism for user data in Cloud.

Data Attributes	Storage	Processing	Transmission
Confidentiality	Symmetric Encryption	Homomorphic Encryption	SSL
Integrity	Message Authentication Code (MAC)	Homomorphic Encryption	SSL
Availability	Redundancy	Redundancy	Redundancy

IV. Proposed Data Storage Security Model

Cloud computing is Internet based computing whereby shared resources, software and information are provided to computers and other services on demand like the electricity grid. Cloud computing proposes new model for computing and related issues like compute, storage, software. It provides development environment, allocation and reallocation of resources when needed, storage and networking facility virtually. It satisfies the on-demand needs of the user. It facilitates the sharable resources “as-a-service” model [9]. Cloud computing is making it possible to separate the process of building an infrastructure for service provisioning from the business of providing end user services. Cloud storage model is a network storage model which is backed by distributed storage providers offers storage capacity for user to lease. In public cloud, the infrastructure is owned by cloud service provider & it offers the highest level of efficiency of the shared resources. For achieving the data storage security we need security mechanisms for data at transit and data at rest while storing the user data in cloud storage and also to build a secure cloud storage service on top off a public cloud infrastructure where the cloud service provider is not completely trusted. For data stored in the cloud (storage-as-a-service), this refers it to as IaaS and security concerned with the stored data includes - confidentiality, integrity and availability. Secure storage in cloud computing may be achieved through cryptographic access control which is cryptography. The techniques used in cryptography are encryption and decryption of data. In the proposed model, Data confidentiality and Data integrity are ensured by data encryption (Symmetric Cryptosystem) and Message Authentication Code (MAC) respectively. In this, AES Encryption technique is proposed for ensuring data confidentiality and Security Hash function (SHA - 256) is proposed for data integrity.. In the process of storing to the cloud and retrieving data back from the cloud, there are mainly three elements that are involved – client, server and the communication channel between them. The proposed security framework provides user centric interface where all operations are performed on the client side, which gives the users more control on the security of their data, and thus the data are not dependent on the security solutions provided by the servers. As studied from [8], the proposed model consists of data security mechanism at data storage and transmission. Figure 2 shows the proposed security framework architectural components for user data storage in cloud.

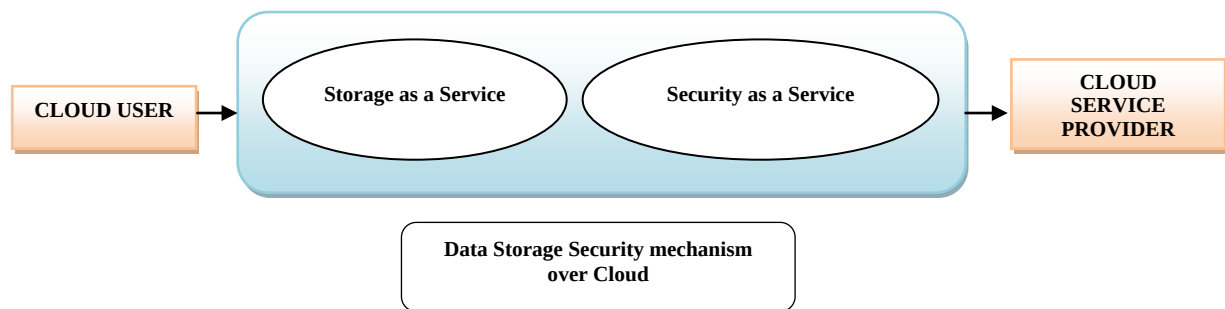
Figure 2 Proposed Security Model for User data storage in public cloud.



The proposed architecture consists of components- a Data Generator (DG), which owns the original user data, a Data Processor (DP), which processes data before it sent to the cloud for storage means responsible for user authentication and encryption of the data and a Data Verifier (DV), which checks whether the data in the cloud has been tampered with by using cryptographic hash function (MAC) and a credential generator which issues access rights to other users if they want to access the stored data in cloud by providing its credentials. In proposed methodology, firstly for data encryption and decryption, a symmetric cryptography (AES Encryption) is used. A client user encrypts the data locally by using symmetric algorithm and then stores the encrypted data in the cloud. If this client or any other client, who is authorised, wants to access the data, has to use the corresponding key to decrypt the data locally. Secondly, besides encryption and decryption of data, two other operations are also performed namely data verification and secure data transmission. For data verification operation, an algorithm (Secure Hash Algorithm-SHA) takes the block of data and generates a fixed size value called message digest and this digest helps in checking the data integrity. By using cryptographic access control, confidentiality and integrity of data is ensured. The data is encrypted locally, and then stored in the cloud. So anyone can get the encrypted data, but no one can read the content of the data, except the authorised clients, who are provided with the key(s). This ensures confidentiality of the data. On the other hand the encrypted data is signed. When an authorised client gets the data, he tries to verify the signature. If the verification of the message digest fails, he knows that someone has tampered with the data, but if the message digest verifies successfully, he knows that the data is untouched. This ensures the integrity of the data. Figure 3 shows proposed workflow diagram of data storage security model which consists of – Data Owner, Cloud User (Service Consumer/Client),

Cloud Service Provider (IaaS/PaaS/SaaS/-Server), Storage as Service, and Security as service (Encryption and Hash function).

Figure 3 Workflow Diagram for Data Storage Security.



A. Advanced Encryption Standard (AES) Cryptography

Encryption algorithm, or cipher, is a mathematical function used in the encryption and decryption process - series of steps that mathematically transforms plaintext or other readable information into unintelligible cipher text. A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a block cipher with a block size of 128 bits. The key length for AES is not fixed, so it can be 128, 192, 256 and possibly more bits. The encryption techniques such as substitutions and transpositions are mainly used in AES. AES algorithm begins with Key Expansion which is the round keys derived from the cipher key. The algorithm is executed with 9 rounds of four stages namely – SubBytes, ShiftRows, MixColumns and AddRoundKey.

B. Cryptographic Hash Function

Cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. Cryptographic hash function is notably used in digital signatures and message authentication code. A message authentication code (MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. The Secure Hash Algorithm (SHA) is a family of cryptographic function published by National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS) that includes- SHA-0, SHA-1, SHA-2 (256/512) and SHA – 512.

V. Conclusion

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. Cloud computing offers many benefits, but it also is vulnerable to threats. According to service delivery models, deployment models and essential features of the cloud computing, data security is the prime aspect of cloud computing. Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network. There are three types of main problems in Cloud Computing, including Data Security, Data Storage Security and Hostile Attack. In this paper, we focused on data security in cloud storage which is essentially a distributed data storage system. The main goal is to securely store and manage data that is not controlled by the owner of the data. To ensure the correctness of users' data in cloud data storage, and correctness of users who can access to the cloud server, we proposed an effective and flexible distributed scheme with explicit dynamic data support using symmetric cryptosystems with user authentication to maintain the confidentiality and integrity of data. The proposed model aims at providing a secure mechanism for data storage in public deployment of cloud by implementing symmetric encryption technique for data confidentiality and hash function for data integrity in achieving user data security. The proposed model provides an integrated framework Data – as – a – service, Storage – as – a – service and Security – as – a – service for the user data in the public cloud infrastructure for the cloud user.

References

- [1] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing", 2009 International Workshop on Information Security and Application (IWISA 2009) – Nov 2009.

- [2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, David Patterson, and Matei Zaharia “A View of Cloud Computing”, Communications of the ACM, April 2010, Vol.53, Issue. 4.
- [3] Hassan Takabi and James B.D. Joshi, “Security and Privacy Challenges in Computing Environment”, IEEE Computer and Reliability Societies, Nov-Dec, 2010.
- [4] S. Subashini n, V.Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, Elsevier, 2010.
- [5] Joshi Ashay Mukundaro, Galande Prakash Verma, “Enhancing Security in Cloud Computing”, Information and Knowledge management, IISTE, Vol.1 No.1, 2011.
- [6] Gargee Sharma and Prakriti Trivedi. “A Model for Data Protection Based on the Concept of Cloud Computing”. International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012.
- [7] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, JieTao, “Cloud computing: A Perspective study”.
- [8] Dyen Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, 2012, International Conference on Computer Science and Electronics Engineering.
- [9] N. Saravanan, A. Mahendrian, N.Sairam and N. Venkata Subramaniam, “An Implementation of RSA algorithm in Google Cloud using Cloud SQL”, Research Journal of Applied Sciences, Engineering and Technology, Oct-2012.
- [10] http://en.wikipedia.org/wiki/Cloud_Computing.