Abstract

To improve the productivity in IT organizations and educational institutions, transition to Mobile cloud environment seems to be necessary. Mobile cloud faces many challenges and issues in concern with security and privacy. In this paper, we design a security framework to overcome threats and attacks by providing security mechanisms such as authentication, encipherment and data access to ensure the confidentiality and availability of data. As, data stored in mobile cloud environment can be accessed by many users, sensitive information of an individual should be protected by security framework. The information is preserved by symmetric encipherment and asymmetric encipherment. In the proposed security framework, the mobile cloud service provider enables privileges to mobile cloud users to classify the sensitive data, authorization to access data and revocation of rights. If the data is compromised by adversary then data sanitization process is provoked by the proposed security framework to ensure the privacy protection of data in mobile cloud.
I. INTRODUCTION

In real world, many functions follow the concept of virtualization. Likewise under information technology, this concept means delivering useful function while hiding how their internal work. Mobile cloud computing allows such computing in a fully virtualized manner by aggregating resources and offering a single system view. Mobile cloud computing unfolds the numerous pluses to IT corporate and organization. Mobile cloud computing is based on its distributed and utility computing, and it brings the incredible growth and benefits of reason for migration to the mobile cloud. It also ensures the end users of mobile cloud to utilize the software applications remotely [1], where the data can be stored and computed dynamically.

The other benefits of mobile cloud are easy to use, on demand service, resource pooling, elasticity and pay for user based on good internet bandwidth. Mobile cloud computing is empowered by the key technology “Virtualization” on which hypervisor creates several virtual module. The maximum benefit of virtualization hypervisor is to simulate the hardware, software and network serves for high quality utilization of resources. Mobile cloud computing is the combination of hardware and software that provide pervasive and utility computing to deploy the resources. Day by day the fame of mobile cloud computing is increasing exponentially. On the other, various issues about the security and privacy have been raised. These issues of securing should be identified, analyzed, investigated and solutions need to be proposed by privacy framework to overcome those challenges. The privacy problem in mobile cloud is mainly caused by multi-tenancy users. The other important concern of privacy is data storage and its maintenance in mobile cloud. So, the service provider must maintain the mobile cloud standards by securing the client’s data and satisfying the service level agreement (SLA).

The mobile cloud offers the following service model [2]

- Software as a service: Saas provides the user to access the application and software on mobile cloud infrastructure via web browsers.
- Platform as a service: Paas provides the user to deploy the application, language and tools provided by mobile cloud service.
- Infrastructure as a service: Iaas enables the processing, storage, network, hardware and resources.

The service models are displayed in mobile cloud infrastructure through,

- Public mobile cloud: It is managed by mobile cloud service provider. It is operated as external storage.
- Private Mobile cloud: It is operated and managed by internal organization.
- Hybrid mobile cloud: It is the combination of both public and private mobile cloud. Its storage is maintained by either external or internal storage based on requirement of service agreement of customers.

In this paper, we design a proved mobile cloud framework which helps to satisfy the requirements against threats and attack for an individual or as a whole for organizations. In section 2 we have detailed review about various issues in mobile cloud. Section 3 elaborates...
the system designing of mobile cloud framework. Section 4 describes about the implementation of framework. Finally, section 5 is about the conclusion and future.

II. RELATED WORKS

This paper is mostly about the data integrity and availability in mobile cloud computing. In [3] flexible and efficient storage scheme is discussed (i.e., homomorphism encryption of data where by issuing the token which in turn erasure the coded data to ensure the behavior of servers such as modification of block, deleting and appending). This scheme thus by enforces against byzantine failure, malicious attack of data at the server end.

Recently in [4] the author proposes a secured management framework to mobile cloud service provider which define and enforces policies. This framework in turn helps to defeat and cease the different types of attack defined through various policies and it allows easy interaction with management framework. The data storage can be easily and efficiently protected by blob-seer platform. The added advantage in here is that DOS attacks are evaluated towards blob-seer platform on grid test bed.

In [5] the work is analyzed about assuring the data correctness in mobile cloud. The user should be able to check whether the data integrity is maintained or compromised due to data migration to the service provider. The mobile cloud user should ensure the data integrity at both service provider and customer end based on service level agreement. This system also proposes thin clients which are more beneficiary because the data storage at the client side is minimal.

In addition to that [6] it has been discussed about four categories of mobile cloud security and privacy.

1. Role based access control where the mobile cloud user needs to get access permission for each session and by classifying the role based to each user which in turn prevents the malicious attackers

2. Dynamic control mechanism handles multi policies and dominant policy on data processing.

3. Identity management method to identity- unauthorized mobile cloud privacy label (CPL) to protect the data.

By using the technique “Virtualization” the user may lose the control over data. To overcome such problem, it uses Third Party Auditor (TPA) to provide the balance between service provider and user.

In [7] the author proposed a new mobile cloud security management framework is introduced, based on FISMA standard to maintain the mobile cloud security. This framework consists of three layers 1) Management layer 2) Enforcement layer 3) Feedback layer. Mobile cloud providers can manage their data by using this framework and as a security as a service by security management process to mobile cloud.

In [8] identified four categories of security issues mobile cloud infrastructure, data access and compliance. The standardization activities of security anonym and privacy preserving techniques are essential requirement to ensure the security risk profile.
III. ATTACKS AND SERVICE MODEL

In Software as a service the common attacks [9] are
1. Wrapping attack:
The attacker can alter simple object access protocol (SOAP) messages between the web browser and server XML Signature element wrapping which is known as wrapping attack.
2. Browser based attack:
The intruders alter the signature and encryption of simple access protocol messages. Phishing attack, SSL certificate snooping and browser caches are the other browser based attack.

In Platform as a service attacks are
1. Mobile cloud injection attack:
The attacks involve creating malicious service activities on models (or) on virtual machines. SQL injection, operating system injection and cross scripting injection are the attacks that concern with mobile cloud injection attacks.
2. Meta data snooping attack:
The attack includes reengineering web server on metadata description. To overcome this attack the verification on web service need to be implemented.

In Infrastructure as a service attacks are
1. Denial of service attack:
When an attacker sends a lot of malicious request to access the resources on server and when the server reaches the maximum request but not able to respond into the request, denial of service attacks occurs. In mobile cloud computing multi-tenancy user accesses the mobile cloud infrastructure which causes greater impact on Distributed Denial of Service (DDOS) attacks.
2. Buffer overflow attack:
The attack occurs due to buffer overflow on the data overwrite of the malicious program.

IV. SYSTEM DESIGN AND ARCHITECTURE

Public mobile cloud has desirability of cost cutting factor and low maintenance but it has drawback. The resources in mobile cloud need to be stored with unknown profile. An intruder can act as subscriber and access the system. It is the responsibility of service provider to ensure the authenticity of user.

4.1 Security Issues

The international standards organization have discussed number security issues

4.1.1 Authorization

Mobile cloud users access the mobile cloud globally from different location based on the privilege provided by mobile cloud service provider. The main body action such as control access, ownership of the users monitors the great challenges in mobile cloud. The solution provided in such mobile cloud environment between the mobile cloud service provider and user is to ensure each entity should have trust on each user.
4.1.2 Authentication
It provides the identification to multi-tenancy user by providing username and password while utilizing the mobile cloud through web browser. The two factor authorization [10] is an efficient way for preventing intruders in the mobile cloud environment.

![Figure 1: Secure Framework for Mobile cloud Computing](image)

4.1.3 Compliance and Audit
The regulation and law plays vital role in ensuring the security requirement in mobile cloud. The auditing should be done on internal and as well as external activities. But customers does not allow the service providers to adhere the compliance and thereby auditing most of the organization such as Health Insurance Portability and Accountability Act (HIPAA) [11] and Payment Card Industry Data Security Standard (PCIDSS) [12] holds the privacy data of the clients. The data needs to be encrypted and migrated over the public mobile cloud. So the mobile cloud service provider should allow the clients to control requirements internal monitory and analyze their audit report.

4.1.4 Transparency
The operation process in mobile cloud computing should be clear between the mobile cloud service provider and user. User should able to understand the architecture i.e. how the data is stored and handled. The service level agreement should be tracked and reported properly. If the data is compromised, who holds the responsibility for data and where the responsibility ends need to be tracked.
4.1.5 Governance

It ensures the data processing against the malicious attacks. And also it makes sure the operation in mobile cloud policy and procedure are implemented properly to secure the data vulnerability as the data is stored and process remotely.

4.2 Secure framework for mobile cloud computing

The mobile cloud computing has many challenges and issues. To overcome the issues, the proposed framework will support the service providers and consumers to protect the data to great lengthen.

The framework deals with the secure environment where the clients need to communicate with the service provider through Virtual Private Network (VPN). The framework ensures the user authentication by validating and verifying the credentials provided by the user. Once the credentials are verified, the framework allows the user data to be encrypted and stored in the mobile cloud.

4.2.1 Security policies

The framework ensures security policies like mobile cloud service provider should have plan and documentation to ensure the data storage properly. The employee who works in the data centre at service provider end should be given proper training on the technologies. The employee should be loyal enough to the organization and also the organization has to cross check the background of the employees. The staff should be given access restriction and privilege settings by the administrator in the data centre. The organization should enforce password changes with period of time. The hardware and software provided password should not be used by the employees of mobile cloud service provider.

4.2.2 Security Schemes

Encryption and key management [13] are the core mechanism for protection of sensitive data in mobile cloud computing. There is raise in need of encryption for privacy of data such as passwords, credit card numbers, and finance and bank details over the internet. Mobile cloud customer’s data need to be guard against data theft and loss. The feasible solution for ensuring the data sensitivity in mobile cloud is by encrypting the data for unauthorized information access. So it is necessary to provide the privacy of organizational data shared in trusted mobile cloud over the internet. By combining the symmetric and asymmetric encryption, we can provide better performance of data in mobile cloud.

4.2.3 Data Backup and Recovery

Data backup has to be carried out in regular period of time. The mobile cloud service provider should roll back, ensure the acid level and recover the data for any disaster that may occur. Data replication should be done on RAID [14] level and sensitivity of data on which separation of data should be done on basis of customer clarification. The alternate plan should be prepared to meet the business continuity of customers. The service provider should be armed to plan data recovery in case of any emergencies. If the customer ends
their services with service provider, then all the data need to be deleted from server and backup drives.

4.2.4 *System logs*

The system logs need to be maintained properly for all multi-tenancy users to access the data. All the session utilized by the user need to be monitored. If any users override the privileges, then the system logs should record the unauthorized changes.

4.2.5 *Penetration Test*

The intruders may cause the mobile cloud environment to be vulnerable at some point of time. Penetration test need to be carried on in regular intervals to ensure that the malicious attack does not occur by using the framework. The firewall must be installed and policies need to be updated regularly. The framework ensures the privacy and security breach to great extent.

4.2.6 *Data sanitization*

Data sanitization is the process that allows the mobile cloud to implement critical factor for security. Sanitization is the removal of sensitive information from storage device or moved to other location. Data Sanitization also takes care of backup copies, residual data’s until service termination between service provider and customer. Research on privacy and security are discussed and presented in [15].

V. **CONCLUSION**

In here, we proposed a Distinctive framework for ensuring privacy and security in mobile cloud computing considering the users trust on mobile cloud service provider in mobile cloud storage. The framework addresses the challenges and issues and brought by various attacks on service model in order to store the data safe and secure. In future, we will be discussing more on homomorphic encryption, two factor authentication and digital signature.

VI. **REFERENCES**


TO CITE THIS PAPER