CHAPTER - III

A BROKER BASED SECURITY MODEL FOR TRUSTED CLOUD SERVICE

3.1 INTRODUCTION TO CLOUD BROKER

A cloud broker is a third-party individual or business entity that acts as an intermediary service provider between the cloud vendor and cloud user. As enterprises increasingly adopt the model of cloud computing, the enterprise IT environment is progressively transformed into a matrix of interwoven infrastructure, platform and application services which are delivered from diverse service providers. To help enterprises deal with the overwhelming complexity of consuming large numbers of cloud services from diverse providers, future enterprise cloud service delivery platforms will need to implement a wide array of sophisticated brokerage-enabling capabilities that will lead rise of services which goes beyond currently offered by cloud service providers. The proposed work delivers a brokerage framework which will allow cloud intermediaries to equip their platforms with advanced methods and mechanisms for continuous quality assurance and optimization of software-based enterprise cloud services.

3.2 CLOUD SERVICES BROKERAGE (CSB)

Is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles including aggregation, integration and customization brokerage.

A Cloud Service Brokerage Enabler provides technology to implement CSB, and a Cloud Service Brokerage Provider offers combined technology, people and methodologies to implement and manage CSB related projects.
In the increasingly complex cloud computing scenario [20], there exists a dire need to amalgamate all cloud-based services and offerings on an integrated platform, to ensure seamless delivery to the end-user. With a wide array of offerings spanning across infrastructure-as-a-service (IaaS), Software-as-a-service (SaaS), Platform-as-a-service (PaaS), Business Process as a Service (BPaaS), and many alike, the cloud marketplace is progressively becoming more diverse and hence, incoherent at the same time. In order to address this seemingly large gap between different standards, platforms, services, and offerings, a unified platform seems to be the only resort, and is ascertained to bridge the gap.

The Cloud Brokerage and Enablement market is set to redefine the cloud environment, with its inherent integration, aggregation, and inter-operable capabilities. Cloud Services Brokerage (CSB), as a concept, has evolved over the years; however, its potential and existence has come to light very recently. Cloud Brokerage and Enablement market refers to the cloud enablement and brokerage market, collectively. Both these markets have been defined, segmented, and estimated, separately; wherein cloud brokerage enablement refers to integration...
platforms which aggregate, customize, and/or integrate cloud offerings on a single platform, thereby enabling other players to become cloud brokers. Cloud Brokerage, on the other hand, is defined by market players who use the enablement platforms as brokers, serve Small and Medium-sized Businesses (SMBs) and enterprises, for their respective cloud-based needs.

Presently, this market comprises of various players who are dedicatedly offering and building on their enablement platforms, with internal and external offerings. While internal enablement is widely being adopted by large enterprises and financial organizations; external enablement is being adopted by players such as telecom providers, system integrators, hosting providers, Independent Service Vendors (ISVs) and resellers, to become cloud brokers.

The Cloud Brokerage and Enablement market is at a very nascent stage and stands highly fragmented. It pioneers the integration of the entire cloud ecosystem, connecting hardware players such as IBM, HP, Dell; software players such as Microsoft, Citrix; PaaS, IaaS, SaaS providers such as Google, Salesforce, Amazon, and Rackspace, among many other prominent players in the IT and Telecom industry.

3.2.1 The use of a cloud broker

The usage and functionalities of the cloud broker is mentioned below

- Help agencies screen their applications for cloud feasibility and prioritizing cloud migrations accordingly
- Address the challenges of cloud model comparisons due to the variables in product offerings, including the business models, service levels, and package inclusions
- Translate capacity requirements into provider line items, thus allowing for accurate estimation of cloud cost
- Provide a cloud service order review or approval workflow facility, a function not normally provided by cloud service providers and
- Provide a means to regulate payment across the different government entities.
3.2.2 Cloud Aggregator

A cloud aggregator showing in Figure Fig 3.2 is a type of cloud broker that packages and integrates multiple cloud computing services into one or more composite services.

The cloud aggregator's business model is still evolving. Some may only offer a finite number of fixed packages, whereas others may incrementally create new bundles by mixing and matching features from existing services. An example of a bundle that a cloud aggregator might offer would be Unified Communications as a Service (UCaaS). By definition, UC is composed of several technologies. A cloud aggregator may combine and integrate cloud-based voice, messaging, rich presence technology and conferencing services from multiple UC vendors into one UCaaS package.

The success of a cloud aggregator is partly dependent on the cloud federation capabilities of the providers whose services the aggregator resells. Ideally, the federation is transparent to the customer, who consumes the aggregated services from one logical user interface. If cloud providers are poorly federated, the cloud aggregator may have to work harder to integrate the services for customers and for its own operational support system (OSS) architecture.

![Figure 3.2 Cloud Services and Actors](image-url)
3.2.3 Cloud Federation

Cloud federation is the practice of interconnecting service providers' cloud environments to load balance traffic and accommodate spikes in demand.

3.2.4 Cloud Integrator

A cloud integrator is a product or service that helps a business negotiate the complexities of cloud migrations.

3.3 INCLUSION OF CREDENTIAL SERVICE IN BROKER ARCHITECTURE

The proposed security model based on cloud service broker uses the Third Party Auditor (TPA) attestation between the tenant virtual machine and the customer before performing the transactions. To enable in the process of attestation, all hardware and software components in the trusted platform are measured using hash values at the time of boot and measurements are stored securely to prevent modification. When a third party presents an attestation request, the trusted platform provides an attestation report as response. This response includes the measured hash values, and a set of expected hash values that are supported in the form of measurement certificates by trusted certifiers.

The basic idea is that, a match between the measured and expected values usually indicates that the components are in a known and trusted state. A fundamental question that arises is – how much can an Attestation Requester (AR) trust the properties that are presented by an Attesting Platform (AP). In other words, when a tenant virtual machine reports its system state with a set of properties to a tenant customer, how certain can be that these reported values are accurate and that AP actually satisfies these claims. Recently different attestation techniques such as binary attestation and property based attestation techniques have been proposed. However uncertainties can arise with these attestation techniques. This can in turn reduce the trust on the property attestation process and leads to situations where attestation requester cannot be completely certain if AP truly satisfies the properties presented to it. The reasons for such uncertainties in attestation are as follows: [43].
First, in binary attestation, the measurements in binary attestation indicate
the state of the components at the time of boot and not at the time of request.
Today's systems are highly dynamic in nature and system components are
constantly upgraded with updates from manufacturers. Also systems can go on
without being rebooted for a very long time. This combination of a dynamic
system with not being rebooted means that values measured at boot time do not
necessarily represent the state of the system at the time of attestation. This leads to
time-of-check time-of-use (TOCTOU) vulnerabilities: values reflect the state of the
system when it was measured, not when the attestation report is generated based on
the measurements. This makes the attestation report less useful for decision
making. As the time between boot and attestation report increases, tenant customer
is uncertain about how much it can use this attestation report for effective decision
making.

In property attestation, the process of property assessment and property
certification do not happen on the run but much in advance before an attestation
challenge is issued to AP. Furthermore, property certificates are generated for each
standalone application component and not for TVM system as a whole. This means
that the environment under which the component's property is verified by the
property certification could be different to the environment under which the
component is measured.

Furthermore, like in any system that involves third party certification
authorities, trust on the property certification authority is subjective and can vary
depending on the context. The trust worthiness on the properties depends on the
trust- worthiness of the authority and verification mechanisms used by the
authority to evaluate a component for a property. Therefore, trust on property
attestation and the properties certified are directly dependent on AR's trust on the
authority that certifies that property. Furthermore AR could trust one authority to
certify one type of property but not other types.
3.4 PROPOSED ARCHITECTURE FOR TRUSTED CLOUD MODEL

The entities available with the current architecture are users, cloud service providers, cloud storage servers and the optional third party. The data will be stored in various data centers through the Cloud Service Provider. The user has to know the correctness of the data at equal feasible time interval. If the user have no enough time to verify the correctness of the data, then the user will request and the delegate the work to the optional Third Party Auditor to ensure the correctness of the data.

![Diagram of Existing System Architecture](image)

Fig.3.3 Existing system architecture

The traditional architecture of trusted cloud model is shown in figure 3.3 accordingly will be done directly from the users and the Cloud Service Provider directly. From the Cloud Service Provider the data will be stored in the data centers which one having the available facilities. This model lacks the support of the public audit to ensure the data stored in the remote data centers because they are placed as optional only. In various work [13][14] the Third Party Auditor can be defined as an entity, that have more capable and expertise than the clients and is trusted to assess the risk of cloud storage services for the clients upon request.
The proposed model for improvised trusted third party is being depicted in figure 3.4 we are introducing the Trusted Third Party (TTP). Because the biggest problem faced by the computer technology is data security, due to the users works with very sensitive information. For that we are going to make a new model called Trusted Computing Technology (TCT) using TTP. In the cloud environment various numbers of users want to join, it means join into the cloud computing environment, due to the elastic nature of the architecture.

![Architecture diagram for OTP Generation System](image)

Fig.3.4 Architecture diagram for OTP Generation System

The proposed system consists of the following four directions to improve the quality of the Cloud Environment

3.4.1 Enhanced Security

3.4.2 New Data Displacement Strategies

3.4.3 User oriented Service Level Agreement

3.4.4 Improving the Quality of Service(Qos)
3.4.1 Enhanced Security

Here we introduce a Trusted Third Party (TTP) like a ticket granting server. If a user want to access the data stored in a cloud server or a data center the user must get authentication key from the TTP, then the user first interact with the Cloud Server, the authentication key will be verified then only the user will be allowed to access the data which is stored in the cloud server or the datacenter. The user must get the authentication key for each and every time. By this we can avoid the misbehaved nodes.

If a user wants to join into the cloud, first step the user have to prove their identity. In this system the user first communicates with the TTP and reveals their identity. Then the TTP check with the identity provided by the user and verify for the trust worthy of the user. If found the trustworthy then it gives a secure key. The key may be combined with the system IP address, and the key given to the user will also be informed to the CSP and Cloud Data Center. Then the user has to enter into the cloud data center through the CSP with the secret key which was given by the TTP. If the key match with the key given by TTP to the CSP, then the user will be allowed to access the Data Center.

3.4.2 New Data Displacement Strategies

By data displacement strategy the user will be allowed to choose the data centers where he wants to store the data. The cloud service provider will also use the pattern matching technology to make decision in the storage area.

3.4.3 User Oriented Service Level Agreement

In this area we are impose new user oriented service level agreement which will give more safer to user side like. The service provider will provide Availability of the service to customer needs. The service provider should follow the NIST standards and security practices.

The CSP will provide confidentiality agreement. The CSP will disclose the contract termination date and policies of termination, and open strategies to move
from one service provider to another one. The CSP will provide the details of the storage where the customer data is stored on the request by this the user will know the position of their data; it gives safest mind set to the user.

3.4.4 Improving the Quality of Service:

By the implementation of the above sections, we are analyse current improvement in the Quality of the service both the view of user side as well as in the service provider side.

In the proposed model, we are introducing the Trusted Third Party (TTP). Because the biggest problem faced by the computer technology is data security, due to the users works with very sensitive information. For that we make a new model called Trusted Computing Technology (TCT) using TTP. In the cloud environment various numbers of users want to join, it means join into the cloud computing environment, due to the elastic nature of the architecture.

3.5 AUTHENTICATION MODEL

The proposed model includes an authentication mechanism on the basis One Time Password generation. A one-time password (OTP) is one, in which password is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional password based authentication. A number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has as well as something a person knows.

The most important advantage that is addressed by OTPs is that they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A second major advantage is that a user, who uses the same password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot
easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further. OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work.

OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. The approaches for the generation of OTPs are listed below:

- Based on **time-synchronization** between the authentication server and the client providing the password
- Using a mathematical **algorithm** to generate a new password **based on the previous password**
- Using a mathematical **algorithm** where the new password is **based on a challenge** and/or a counter.

This one-time password system works as follows:

1. A seed (starting value) \( s \) is chosen.

2. A hash function \( f(s) \) is applied repeatedly (for example, 1000 times) to the seed, giving a value of: \( f(f(\ldots.f(s)\ldots)) \)). This value, which we will call \( f^{1000}(s) \) is stored on the target system.
3. The user's first login uses a password \( p \) derived by applying \( f^{999} \) times to the seed, that is, \( f^{999}(s) \). The target system can authenticate that this is the correct password, because \( f(p) = f^{1000}(s) \), which is the value stored. The value stored is then replaced by \( p \) and the user is allowed to login.

4. The next login, must be accompanied by \( f^{998}(s) \). Again, this can be validated because hashing it gives \( f^{999}(s) \) which is \( p \), the value stored after the previous login. Again, the new value replaces \( p \) and the user is authenticated.

5. This can be repeated another 997 times, each time the password will be \( f \) applied one fewer times, and is validated by checking that when hashed, it gives the value stored during the previous login. Hash functions are designed to be extremely hard to reverse, therefore an attacker would need to know the initial seed \( s \) to calculate the possible passwords, while the computer system can confirm the password on any given occasion is valid by checking that, when hashed, it gives the value previously used for login. If an indefinite series of passwords is wanted, a new seed value can be chosen after the set for \( s \) is exhausted.

### 3.6 OTP GENERATION – A SCENARIO IN BANKING SYSTEM

In the current scenario all the banking [54] sectors provide the online services for their customers for easy banking as well as the fastest banking solutions. For the online transactions they relay on the one time password for the approval of each and every transaction. By that we know the OTP is the proved technology for the securing transactions. So that in our proposed system also we use the OTP for the purpose of authenticate the user who made transactions on the data which are stored in the third party premises. The CSP is also maintaining the each and every transactions the each user for the future verification process.
3.7 FUNCTIONALITIES OF PROPOSED CLOUD BROKER

Functionalities of cloud broker are being derived as the following research assumptions.

A cloud broker is a third-party individual or business that acts as an intermediary between the purchaser of a cloud computing service and the sellers of that service. A cloud broker is a third-party individual or business that acts as an intermediary between the purchaser of a cloud computing service and the sellers of that service. In general, a broker is someone who acts as an intermediary between two or more parties during negotiations.

The broker's role may simply be to save the purchaser time by researching services from different vendors and providing the customer with information about how to use cloud computing to support business goals. In such a scenario, the broker works with the customer to understand work processes, provisioning needs, budgeting and data management requirements. After the research has been completed, the broker presents the customer with a short list of recommended cloud providers and the customer contacts the vendor(s) of choice to arrange service.

A cloud broker may also be granted the rights to negotiate contracts with cloud providers on behalf of the customer. In such a scenario, the broker is given the power to distribute services across multiple vendors in an effort to be as cost-effective as possible, in spite of any complexity that negotiations with multiple vendors might involve. The broker may provide the customer with an application program interface (API) and user interface (UI) that hides any complexity and allows the customer to work with their cloud services as if they were being purchased from a single vendor. This type of broker is sometimes referred to as a cloud aggregator.

In addition to acting as an intermediary for contract negotiations, a cloud broker might also provide the customer with additional services, facilitating the reduplication, encryption and transfer of the customer's data to the cloud and
assisting with data life cycle management (DLM). This type of broker is sometimes referred to as a cloud enabler. Another type of broker, sometimes referred to as a cloud customizer or white label cloud service, selects cloud services on behalf of a customer, integrates the services to work together and sells the new offering under their own brand.

The business model for cloud brokerage is still evolving. At its simplest, the customer may hire a broker at the beginning of a project and pay the broker an hourly fee for their time. A broker providing more robust services, however, may charge the customer on a sliding scale, depending on what services the customer contracts for. A broker may also partner with one or more cloud service providers and take a small percentage of the cloud provider's profit as remuneration once the customer has arranged service.

A cloud broker is a software application that facilitates the distribution of work between different cloud service providers. This type of cloud broker may also be called a cloud agent. There are different types of CSB use-cases, but at a high level they can be segmented into "Internal CSB" and "External CSB."

Internal CSBs are typically operated by or on the behalf of large enterprise or government IT organizations who want to aggregate private and public cloud services and unify the delivery and life-cycle management on behalf of their internal users. Internal CSBs are typically driven by a centralized IT organization that wants to provide a unified security, compliance, license management, support, and overall usage experience for employees or affiliated members.

External CSBs may share many of the needs of an Internal CSB, but they are also focused on monetizing cloud services delivery. They may want to operate their own private-branded cloud marketplaces as a means of bundling value-added services with their own core product and service offerings.

If you are in the process of evaluating cloud services brokerage solutions, here are some helpful building blocks of cloud service Brokerage. They are Catalog Management, Work flow automation, Service Integration and final one is
Operations and Management. The Catalog Management deals with Current portfolio analysis, which model the user have to chose based on their needs, Cost and pricing, Policy entitlement and dealing with service definitions. The work flow automation deals with Order to settlement process, user on boarding, security, reporting of dashboards and auditability.

3.8 CONCLUSION

The benefits of the cloud computing are to achieve the economics of scale, reduce the spending on technology infrastructure which is globalize your workforce as very cheap, steam line process, reduces capital cost, improves accessibility and monitoring the projects more effectively. Another focus, as a cloud provider, they have to ensure the security of user’s data. The cloud computing security issues are discussed and new algorithm for protecting the data is developed. The test result shows that the new algorithm is used to protect the data more efficiently. The above system tested with various users and collected the feedback about the reliability of the software is compared with the previous one.