A

Dissertation

On

Use of DSS with Station to Station Key Agreement and Cloud Manager to Enhance Security in Cloud Computing

For the Award of the Degree of

Master of Technology

In

Computer Science & Engineering

Submitted By

Kranti Asiwal

University Roll No. 2K12/CSE/10

Under the Esteemed Guidance of

Mr. Manoj Kumar

Assoc. Prof., Computer Engineering Department, DTU, Delhi

2012-2014

DELHI TECHNOLOGICAL UNIVERSITY

DELHI - 110042

CERTIFICATE

This is to certify that the dissertation titled "**Use of DSS with Station to Station Key Agreement and Cloud Manager to Enhance Security in Cloud Computing**" is a bonafide record of work done at **Delhi Technological University** by **Kranti Asiwal, Roll No. 2K12/CSE/10** for partial fulfilment of the requirements for the degree of Master of Technology in Computer Science & Engineering. This project was carried out under my supervision and has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma to the best of my knowledge and belief.

(Mr. Manoj Kumar)
Assoc. Professor & Project Guide
Department of Computer Engineering
Delhi Technological University

Date: ____________

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to all the people who have supported and encouraged me during the course of this project without which, this work could not have been accomplished.

First of all, I am very grateful to my project supervisor Mr. Manoj Kumar for providing the opportunity of carrying out this project under his guidance. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success. I am also grateful to Dr. O. P. Verma, HOD, Computer Science, DTU for his immense support. I am also thankful to my parents for being there for me at all times. Last but not the least, I am grateful to Delhi Technological University for providing the right resources and environment for this work to be carried out.

Kranti Asiwal
University Roll no: 2K12/CSE/10
M.Tech (Computer Science & Engineering)
Department of Computer Engineering
Delhi Technological University
Delhi – 110042

ABSTRACT

Cloud computing provides IT as service. Cloud computing is a budding paradigm having high availability, performance, least cost and many others. Cloud is an IT environment based on remotely providing IT resources. As cloud computing is an internet based computing solution, there are lots of security breaches and vulnerabilities like authenticity, data security, confidentiality and privacy which should be dealt properly to get high performance. Different combinations are used by different researchers to get rid of these security breaches and vulnerabilities, same way we have chosen a combination of authentication technique and key exchange with cloud manager. In this paper we have proposed a model to enhance security of cloud by using Station to Station key agreement for generating session key with a fixed timestamp between User and Cloud Server and then send request for any service by using Digital Signature Standard, the request message would be encrypted by using that session key which was shared earlier and once a session key is been used then that session key would not be used again. So every time for any service new session key is required by user. All of these issues related to authentication and authorization are handled by a cloud manager present between cloud server and user.

Table of Contents

TITLE	PAGE NO.
Certificate	ii
Acknowledgment	iii
Abstract	iv
List of Figures	vii
1. Introduction	1
1.1 Problem statement	2
1.2 Proposed work	2
2. Cloud	3
3. Computing	5
4. Cloud Computing	6
4.1 Key Characteristics of Cloud Computing	7
4.2 Need of Cloud Computing	8
4.3 Cloud Computing reference architecture	10
4.3.1 Actors of Cloud Computing	11
4.3.2 Components of Architecture	13
4.4 Service Models	14
4.5 Deployment Models	15
4.6 Advantages of Cloud Computing	17
4.7 Disadvantages of Cloud Computing	20
5. Digital Signature Standard	22
5.1 Why DSS?	23
5.2 Application	23
6. Station to Station key Exchange Agreement	25
6.1 Algorithm	25
7. Cloud Manager	27
8. Related Work	28

9. Proposed Work	31
10. Conclusion	41
11. Future Work	42
12. References	43

List of Figures

FIG NO.	TITLE	Page no.
Figure 2.1	Symbol used to denote the boundary of a cloud environment	3
Figure 4.1	Cloud Computing Reference Architecture	11
Figure 6.1	Station to Station Key Exchange Agreement	26
Figure 9.1	Proposed Model Entities layout	31
Figure 9.2	Services Provided by Cloud Manager	32
Figure 9.3	Algorithm of Station to Station Key Exchange Agreement	36
Figure 9.4	Digital Signature Standard	39

Chapter 1
Introduction

Cloud Computing is a utility over internet that provides resources on pay per usage basis to users as it is pool of resources which are remotely provided to users. Companies provides services over internet by cloud computing and reduces services cost by this way.

Cloud computing provides it services and resources over internet and that internet act as a cloud that uses computer technology and that technology is computing. In this type of computing, resources are provided dynamically and virtually as a service over internet. It is not necessary for users to have full knowledge, control or expertise over this technology that is Cloud.

Cloud computing is paradigm that is emerging in computer industry and computing is used over cloud. It has become one of buzzing words of this industry nowadays. Concept of cloud computing is pretty simple that all of those resources present in the pool could be used anytime when user needed them and those resources resides somewhere on cloud of computers so actually users uses resources virtually.

Cloud computing is a solution whose range is quite wide that deliver IT on pay per usage basis as a service. It is a kind of computing solution that is based over internet where resources are virtually distributed like distribution of electricity is done through electricity grid. Systems are organised in a way on cloud that they work together and in many applications collective computing power of many systems are used and user thinks all of this computing is done on single system.

Flexibility is one of attribute of cloud computing as it is very much flexible in providing resources to users on their demand. By using cloud computing there is no need to assign specific hardware to any task. Before cloud computing a specific system were assigned for execution of web based and server based applications, but through cloud computing resources are collectively used virtually by a user.

1.1 Problem statement

Cloud computing technology provides services over internet so privacy and security is main concern that's why security issues like authentication, confidentiality, privacy should be handled properly. To deal with these problems a scheme where one to one medium is been generated by Station To Station key exchange agreement for privacy, encryption algorithm are used by cloud manager for data encryption and thus provides confidentiality and Digital Signature Standard is used as an authentication technique.

1.2 Proposed work

Since cloud computing is a utility available on internet so security is main concern. So for Security problems we have used techniques for authentication, verification and a manager which will manage everything to enhance security.

As for secure connection between user and server one to one connection is preferable for security purpose that's why session key is been generated by Station to Station (STS) key exchange agreement. Station To Station key exchange agreement will establish session keys between user and server for a fixed timestamp and only for single use that means once a session key is used by user for any service then again it won't be used again. After establishment of session key it's been used in Digital Signature Standard so as intruders will be unable to decrypt the message send by user this message is the request from user to server for a service. All request-response management, session key generation and management are handled by Cloud Manager.

Chapter 2
Cloud

Cloud is a wide area network like internet or any other network like internet. It is a term like allegory. Cloud name came from cloud like symbol that depicts intricacies of network through schematic diagram. This symbol represents complexity of network which includes everything i.e. used for connection of users, server and other resources.

A cloud refers to a trenchant IT environment that quiet effectively purvey scalable IT resources to users for which it is designed. This term spring up from metaphor of internet i.e. network of networks which purveys resources remotely and virtually from non concentrated IT resources. Cloud computing has became its own validated IT industry sector. Cloud stands for internet in a variety of documentation and specification of web based architectures. Cloud symbol represents cloud environment.

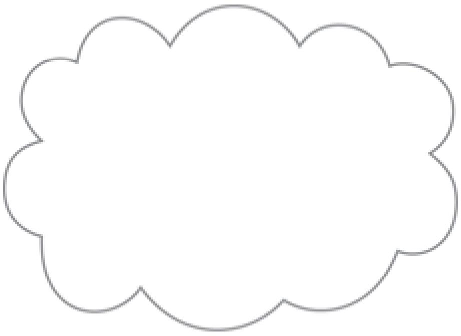

Figure 2.1: Symbol used to denote the boundary of a cloud environment

Term cloud and symbol cloud of internet are very important to discriminate between each other. Cloud has restricted boundary that virtually provide services to users. There are lots of individual clouds present on internet which are very easy to get.

Many web based IT resources have open access over internet but cloud is privately owned and offer private access to IT resources.

Internet is mostly used for accessing content based IT resources through World Wide Web(WWW) whereas cloud computing is devoted to provide IT resources which are supplying back and processing capabilities. Another point is that it is inevitable for clouds to be web based even if it is based on internet technologies and its protocols. Cloud acts as a platform where cloud consumers get services and uses services as per their requirement.

Chapter 3
Computing

Computing started off at the time of mainframe era. At mainframe era there were mainframe computers and those were connected to each other through some kind of terminals and these terminals were known as dumb terminals. It was very frustrating for users at times to sit on those dumb terminals because they were able to do only those things for which they are authorized. They depend on system administrator for permission regarding removal of bugs.

Centralized computing was replaced by personal computers. Users felt freedom in using personal computer rather than centralized computing system. But server architecture replaced personal computers. Server architecture keeps computing in focus and keeps a check if any of its clients are having any resource idle with it. Computing was done at the server site. Internet grew because of these servers. Through cloud computing now we are back to centralized computing infrastructure but now we are having full control over it and anything can be easily accessed over internet using this.

Chapter 4
Cloud Computing

In Cloud Computing any service can be easily used through wide area network having many resources. It believes in logic of minimum input and maximum output i.e. minimum resources and maximum results that is at user end hardware requirement is minimum but maximum computing capability is been used and that is only possible by a technology which uses and requires its services and resources in best way.

Cloud computing can dynamically allocate, reallocate and deploy resources and can monitor their usage. Cloud service providers make profit by charging services to users effectively.

Broader concept of cloud computing is convergence of infrastructure. Through Cloud computing a kind of data centre environment is provided which allows organisation or companies to get their applications on cloud and that run faster, easily manageable and very less maintenance required for business demands.

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. Any user who has a PC, Laptop with Internet facility can acquire the cloud source according to the service provider's policies and norms at any time without any prerequisites, this nature of computing opens several security breaches and vulnerabilities to the cloud environment. The flexibility that allows many users to make use of the cloud leads to various network and information security risks, in cloud environment mostly client data's are moved on to the data centres that are distributed across the network that is data resides in the physical storage of the service providers therefore an enterprisers or user data's are under the service providers concern which paves for unexpected security attacks and vulnerabilities when it is uploaded and offloaded to and from the cloud data centres.

4.1 Key Characteristics of Cloud Computing

- *Cost:* By cloud computing capital expenditure converts into operational expenditure and cost is very much reduced. As third party provide infrastructure so this lowers the barriers to entry and its services can be used online and need not to be purchased.

- *Device and location independence:* It doesn't matter wherever users are, whatever their location is and whatever device they are using (pc, mobile) they can use services of cloud computing over internet by using their web browser. As cloud computing is provided by third party which is offsite and it is accessed over internet so can be used from anywhere.

- *Multi-tenancy:* It enables user to share lots of resources and it allows them following things:

    - Centralization: This allows centralization in many other areas with less cost.

    - Peak-load capacity: Load capacity at peak time increases.

    - Utilization and efficiency improvements: Efficiency and utilization improves for a system that is usually very less.

- *Reliability:* Multiple redundant sites are used and through that a suitable condition is there for business continuity and disaster recovery and this improves reliability.

- *Scalability:* Resources are provisioned dynamically to users on self service basis and users don’t have to be scared of peak loads. Cloud computing performance is very lightly monitored so as to keep it bug free.

- *Security:* As it is advancement of centralization of systems so this improves security but there is one issue also i.e. loss of sensitive data. As there are lots of issues that should be handled properly to increase security. For that auditing is also done.

- *Sustainability:* Cloud computing improves utilization of resources and increase efficiency and this increases sustainability.

4.2 Need of Cloud Computing

What could we do with 1000 times more data and CPU power?
That’s all it took the interviewers to bewilder the confident job applicants at Google. This is a question of relevance because the amount of data that an application handles is increasing day by day and so is the CPU power that one can harness.

There are many answers to this question. With this much CPU power, we could scale our businesses to 1000 times more users. Right now we are gathering statistics about every user using an application. With such CPU power at hand, we could monitor every single user click and every user interaction such that we can gather all the statistics about the user. We could improve the recommendation systems of users. We could model better price plan choices. With this CPU power we could simulate the case where we have say 1,00,000 users in the system without any glitches.

There are lots of other things we could do with so much CPU power and data capabilities. But what is keeping us back. One of the reasons is the large scale architecture which comes with these are difficult to manage. There may be many different problems with the architecture we have to support. The machines may start failing, the hard drives may crash, the network may go down and many other such hardware problems. The hardware has to be designed such that the architecture is reliable and scalable. This large scale architecture has a very expensive upfront and has high maintenance costs. It requires different resources like machines, power, cooling, etc. The system also cannot scale as and when needed and so is not easily reconfigurable.

The resources are also constrained by the resources. As the applications become large, they become Input/Output bound. The hard drive access speed becomes a limiting factor. Though the raw CPU power available may not be a factor, the amount of RAM available clearly becomes a factor. This is also limited in this context. If at all the hardware problems are managed very well, there arises the software problems. There may be bugs in the software using this much of data. The workload also demands two important tasks for two completely different people. The software has to be such that it is bug free and has good data processing algorithms to manage all the data. The cloud computing works on the cloud - so there are large groups of often low-cost servers with specialized connections to spread the data-processing chores among them. Since there are a lot of low-cost servers connected together, there are large pools of resources available. So these offer almost unlimited computing resources. This makes the availability of resources a lesser issue.

The data of the application can also be stored in the cloud. Storage of data in the cloud has many distinct advantages over other storages. One thing is that data is spread evenly through the cloud in such a way that there are multiple copies of the data and there are ways by which failure can be detected and the data can be rebalanced on the fly. The Input/Output operations become simpler in the cloud such that browsing and searching for something in 25GB or more of data becomes simpler in the cloud, which is nearly impossible to do on a desktop.

The cloud computing applications also provide automatic reconfiguration of the resources based on the service level agreements. When we are using applications out of the cloud, to scale the application with respect to the load is a mundane task because the resources have to be gathered and then provided to the users. If the load on the application is such that it is present only for a small amount of time as compared to the time its working out of the load, but occurs frequently, then scaling of the resources becomes tedious. But when the application is in the cloud, the load can be managed by spreading it to other available nodes by making a copy of the application on to them. This can be reverted once the load goes down. It can be done as and when needed. All these are done automatically such that the resources maintain and manage themselves.

There are valid and significant business and IT reasons for the cloud computing paradigm shift. The fundamentals of outsourcing as a solution apply.

- *Reduced cost*: Cloud computing can reduce both capital expense (CapEx) and operating expense (OpEx) costs because resources are only acquired when needed and are only paid for when used.

- *Refined usage of personnel*: Using cloud computing frees valuable personnel allowing them to focus on delivering value rather than maintaining hardware and software.

- *Robust scalability*: Cloud computing allows for immediate scaling, either up or down, at any time without long-term commitment.

4.3 Cloud Computing Reference Architecture

NIST (National Institute of Standard and Technology) provides reference architecture and that's known as cloud computing reference model. This is conceptual model that depicts structure, requirement, operation of cloud computing. This model is not tied to any service, provider or vendor. It describes, activities, actors, functioning that are used at the process of cloud computing architecture development. It describes uses, characteristics and standard for cloud computing.

Five major actors of cloud computing are:
1. Cloud consumer
2. Cloud provider
3. Cloud auditor
4. Cloud broker

5. Cloud carrier

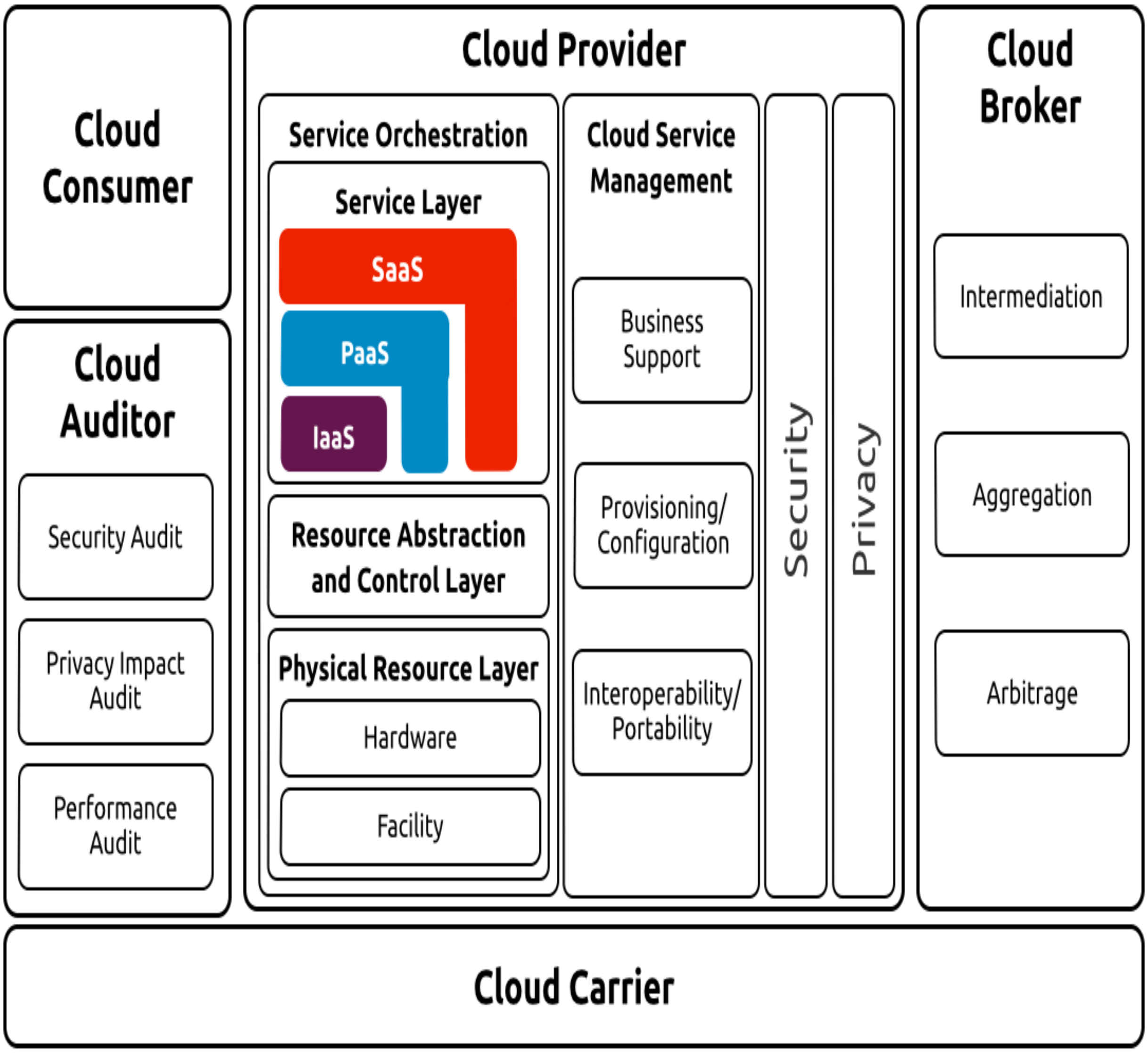

Figure 4.1: Cloud Computing Reference Architecture

4.3.1 Actors of Cloud Computing

Cloud Consumer

For Cloud computing services Cloud consumer are principal stakeholders. It represents those who uses cloud computing services and maintain business relation i.e. organization, user. It contact cloud provider for any service which will provide it a catalogue of services from which cloud consumer will select services required, sets proper contract with cloud provider and finally use service. For every service cloud consumer could be charged and he has to pay for that through one of payment methods given by cloud provider.

Cloud Provider

Cloud provider is responsible for providing services to cloud consumer. It can be any entity, an organization or a person. It manages technical platform required for purveying services, builds requested software and platform, keep all of services secure. Activities done by cloud providers are cloud service management, privacy, security, service deployment and service orchestration.

Cloud Auditor

Cloud auditor is an independent party that keeps assessment of operation, performance, cloud services security related issues and implementation. Evaluation of services provided by cloud provider is done by cloud auditor on the basis of privacy impact, performance, security controls and adherence to service agreement.

Cloud Broker

Cloud broker does the management of cloud services delivery, use, and performance negotiates relation between cloud consumers and cloud providers. As cloud computing spring up, cloud services integration was very much complex task for cloud consumer to manage. Cloud broker can directly provide services to cloud consumer with one interface for many providers by following 3 categories:-

1. **Intermediation**

Cloud broker purveys value added services to cloud consumer and improves some capability by this enhances a service. Improvement can be identity management, enhanced security, performance reporting.

2. **Aggregation**

Cloud broker aggregates multiple services into many new services or one service. Cloud broker ensure that data move pretty securely between multiple cloud providers and cloud consumer. It provides data integration.

3. **Arbitrage**

It is very much similar to aggregation except for one thing that services combined or integrated are not fixed. This means that cloud broker has freedom to choose any service from multiple cloud providers.

Cloud Carrier

It acts as a mediator between cloud consumer and cloud provider that concepts and transport cloud services between cloud providers and cloud consumers. Cloud consumers are provided access by cloud carrier through telecommunication, networks other devices. Likewise cloud consumer also access cloud computing by provider through network access devices like laptop, mobile phone, computers, tablets, and internet connected devices.

4.3.2 Components of Architecture

There are following architectural components according to cloud computing reference architecture:-

Service Deployment

It can be private, public, mobile, community and hybrid.

Service Orchestration

It is composition of components of system for supporting activities of cloud provider in coordination, arrangement and management of resources for providing services to cloud consumers. It has following 3 layers:-

- Service layer
- Resource abstraction and control layer
- Physical resource layer

Cloud Service Management

It comprises of all function related to service which are required necessary for operation and management of required services by cloud consumer. This can be defined from point of view of configuration, business support, portability, interoperability requirements and provisioning.

Security

Cloud computing needs to fulfil security issues like authorization, authentication, identity management, confidentiality, audit, integrity, responses monitoring and policy management. In all layers of cloud computing reference model security is necessary even in application security as well as physical security. Security is necessary even at the functioning of actors of cloud computing.

Privacy

Cloud auditor should audit properly and make sure of privacy in all actors involved as well as in whole cloud computing architecture. Cloud provider purveys privacy in consistent collection, proper, assured, communication, processing, deposition and use of personal information in cloud.

4.4 Service Models

1. **Software as a Service (SaaS)**

In this the feature provided to consumer is to use any of provider application which runs on cloud. Application over cloud provider can be accessed from many client devices even from a small interface like web browser (example- web email) or program interface consumer do not control or manage cloud including servers, storage, system software, network and applications.

2. Platform as a Service (PaaS)

Applications created by consumer or acquired by using programming language, services, library and tools are to be deployed on cloud by consumer in platform as a service. Consumer can't control or manage cloud including servers, network, storage, system software, but it could have control on deployed applications and setting of configuration for hosting application environments.

3. Infrastructure as a Service (IaaS)

Service provided by this is that consumer is provided storage, processing, and other computing resources for consumers to run or deploy arbitrary software which includes other applications as well as operating system. Here consumer can have limited control over network components(example- host/firewall) operating system, deployed applications, storage but does not control or manage cloud.

4.5 Deployment Models

1 Public cloud

This kind of cloud is completely open to be used by general public. It may be operated, managed and owned by academic, government, business organisation or any combination of them. It resides on cloud provider premises.

2 Private cloud

This kind of cloud is privately owned and provisioned for use by organisation which may have many consumers in it. This can be operated by third party, organisation or combination of them. It can exist in 2 forms on or off premises.

On-site: This means that cloud implements on customer site and user who belong to some organisation are allowed to use it.

Off-site: This means that cloud implements on cloud provider site.

3 Community cloud

This kind of cloud is provisioned for specific community of consumer. It can be managed, owned and operated by more or one third party, organisation or any combination. This also exists in two form, these are on or off premises.

On-site: In this cloud implementation is done at customer site and only same organization cloud customers are allowed to access services. In this case cloud customers can be of two or more organisation.

Off-site: It means cloud implementation is done at cloud provider site.

4 Hybrid cloud

Here cloud is composition/aggregation or combination of at least two of these distinct cloud type public, private and community.

5. Mobile Cloud

The kind of cloud computing which is used on mobile devices is known as Mobile cloud. In cloud computing data is present on World Wide Web (WWW) and provided by internet rather than on separate devices, which purvey access on demand. But in mobile cloud applications executes on remote server and after that sent to consumers.

4.6 Advantages of Cloud Computing

- *Lower computer costs:*
  - Low powered and low priced computers can be used for cloud computing web applications so no need to spend high amount of money and get high powered computers.
  - Hard disk space and processing power which was earlier demanded by traditional software are not required here because cloud computing application runs on cheap systems with less hard disk space.
  - No need of installation of software so no need of CD or DVD because they are installed on cloud site.
- *Improved performance:*
  - Booting in computers of cloud computing systems are very much fast and they run also faster because they have very less process and programs.
  - Even very big programs run very efficiently on cloud then if you will run that on your system.
- *Reduced software costs:*
  - You don't have to purchase software because cloud consumers can get most of software for free on cloud. Example- Google Docs
  - Commercial software is very expensive so it's a better option to use that software on cloud for fewer amounts.

- *Instant software updates:*
  - Cloud consumers don't have to give upgrading charges so cloud consumer doesn't have to opt for this choice.
  - For web based applications updates are automatically done.
  - Without even paying for upgrading charges you can get latest version of web based applications.
- *Improved document format compatibility:*
  - We don't have to be worried about compatibility of documents we created whether they are going to work on other systems or not.
  - When all users are sharing documents on cloud then there would be no incompatible format.
- *Unlimited storage capacity:*
  - Limitless virtual storage space is offered by cloud computing.
  - There is hundreds of Pbytes available on cloud and that is way much higher than your computer 1 Tbyte hard disk.
- *Increased data reliability:*
  - A crashing of computer would not lead to loss of your data in case of cloud unlike desktop computing where a computer crashing could lead to loss of data.

  - It is a kind of computing platform which we can call as data safe computing.

- *Universal document access:*

  - Users don't have to keep their documents with them all the time because they can easily get them from cloud by using internet.

  - In other words we can say you just need a system and internet connection and you can use your documents anytime, anywhere.

  - You are instantly provided your documents by cloud.

- *Latest version availability:*

  - Cloud always provides updated and latest versions of services and documents.

  - After editing a document over cloud at home you will be able to use that edited version any other place after that.

- *Easier group collaboration:*

  - Better collaboration is achieved because documents are shared.

  - It is very easy to collaborate for multiple users on documents and projects.

- *Device independence:*

  - Users are not tethered to one network or computer.

- Even in case where we use portable devices, still our application and documents are with us.

4.6 Disadvantages of Cloud Computing

- *Requires a constant Internet connection:*
    - If cloud consumer don't have internet connection then it is impossible for them to work on cloud.
    - If cloud consumers won't have internet connection he won't be able to get services from cloud even won't be able to use his own files so that can make them to loose deals because of that. So for places where connection is very unreliable and few there cloud is not useful.
- *Does not work well with low-speed connections:*
    - When internet connection is slow like dialup internet connection then users won't be able to get best of cloud computing.
    - As mostly web based applications are used by users as an interface for cloud but that require very high bandwidth for uploading as well as downloading purpose like large documents.
- *Features might be limited:*
    - Still after so many years of cloud computing still we don't have web based applications that have all features like desktop-based applications.
- *Can be slow:*

  - As we use software on our personal computer in comparison to that using application software on cloud through cloud computing would be very slow.

  - As lots of users can use cloud at the same time so users may get access slowly as compared to what they can use it in their systems.

- *Stored data might not be secure:*

  - Your confidential data can be leaked or hacked or used by other user's i.e. unauthorized users.

  - All data is stored on cloud and that can be misused by intruders.

- *Stored data can be lost:*

  - If data is lost then there is no local and physical backup of that data but theoretically your files are safe as replicate to many systems.

Chapter 5
Digital Signature Standard

Digital Signature Algorithm is used in Digital Signature Standard based on Elgamal scheme with some ideas from Schnorr scheme. Digital signature standard signatures are faster than RSA Signatures. DSS signatures are smaller than other Signatures. Message send by user to cloud manager is encrypted by using session key already created by Station To Station key agreement.

This Standard has provided many methods for generation of digital signature which is been used for data protection (also known as message) and for the purpose of validation and verification of these digital signatures following three techniques are used:-
(1) Digital Signature Algorithm (DSA)
(2) RSA digital signature algorithm
(3) Elliptic Curve Digital Signature Algorithm (ECDSA)

Rather than written signatures algorithm are specified by this standard for those applications which require a digital signature. In a computer digital signature representation is a string of bits. There are set of parameters and set of rules on basis of these digital signatures is computed and these rules and parameters allow identification of person who signed the message and integrity of data. Digital signatures can be generated on both ends, transmission as well as on stored end.

A private key is been used for signature generation purpose and a public key is been used for signature verification. Each and every signer has a pair of keys, one is public and other is private. As their name suggests public key is publically distributed and known by public while private key is kept secret and it’s private.

For signature generation purpose a hash function is also used so as to obtain a condensed version of message which is to be signed and that condensed version is also known as Message digest. For generation of digital signature message digest is used as input of digital signature algorithm.

5.1 Why DSS?

As we know in any of business transaction a formal document is been signed by the organization head between which any deal or business is going on. After that signatures are matched so as to confirm that signature identifies the signatory and it is unique. Signature matching or we can also call this as signature binding and it is done in many ways, like:-

- Matching is done by using signature cards at bank.
- Current document could be compared with any of past signature document, which were stored.
- Any person Signature can be assured by Notary services.

Now from point of computer as we know that computer has evolved in business. So for business transactions over computer also need a signature and that's where digital signature is been used. These decreases cost of transaction and increases speed of transaction. This will improve financial position and very good for business.

Since 1977 Digital Signature is the technology that is been very useful for Digital documents. This technology is Asymmetric key cryptography also known as public key encryption. Another technology, secure hashing with public key encryption, provides a standard procedure of signing a digital document. Collection of all those procedures is called Digital Signature Standard (DSS).

5.2 Application

A digital signature algorithm allows an entity to authenticate the integrity of signed data and the identity of the signatory. The recipient of a signed message can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time. A digital signature algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. . Digital signature standard signatures are faster than RSA Signatures. DSS signatures are smaller than other Signatures. Message send by user to cloud manager is encrypted by using session key already created by Station To Station key agreement.

Chapter 6
Station To Station Key Exchange Agreement

Station to Station (STS) key exchange agreement is commonly known as Station to Station (STS) protocol. Digital signatures with public key certificates are used to establish session key. It is based on diffie hellman, as in diffie hellman man in middle attack can took place but Station To Station key exchange agreement prevents man in middle attack. As session keys are created for a fixed time stamp it will increase security level.

6.1 Algorithm

a) A random number x that is user private key is already been chosen at the time of registration with a time stamp and will renew it time to time when new g, P, q and B values are received then x is also renewed.

b) New user will calculate $R_1 = g^x \bmod B$ & send this R_1 to cloud manager.

c) After getting R_1, cloud manager will choose a random number y & find out R_2.

d) Now cloud manager will find out key (session key) $K = (R_1)^y \bmod B$

e) After calculating R_2 & the session key, cloud manager concatenates R_1 and R_2 and then signs the result with the private key. Cloud manager now sends R_2, the signature & his own public key certificate to user. Signature is encrypted with session key.

f) Now after getting R_2 user will calculate session key & verify cloud manager signature by the certificate authority.

g) After that user will create a signature by concatenate $R_1|R_2$ and encrypt that signature by K & send user's certificate also & sent an encrypted Timestamp value to cloud manager.

h) Cloud manager will verify Digital signature of user & if it is verified the send the encrypted T-1. That means key K is been set for T-1 time.

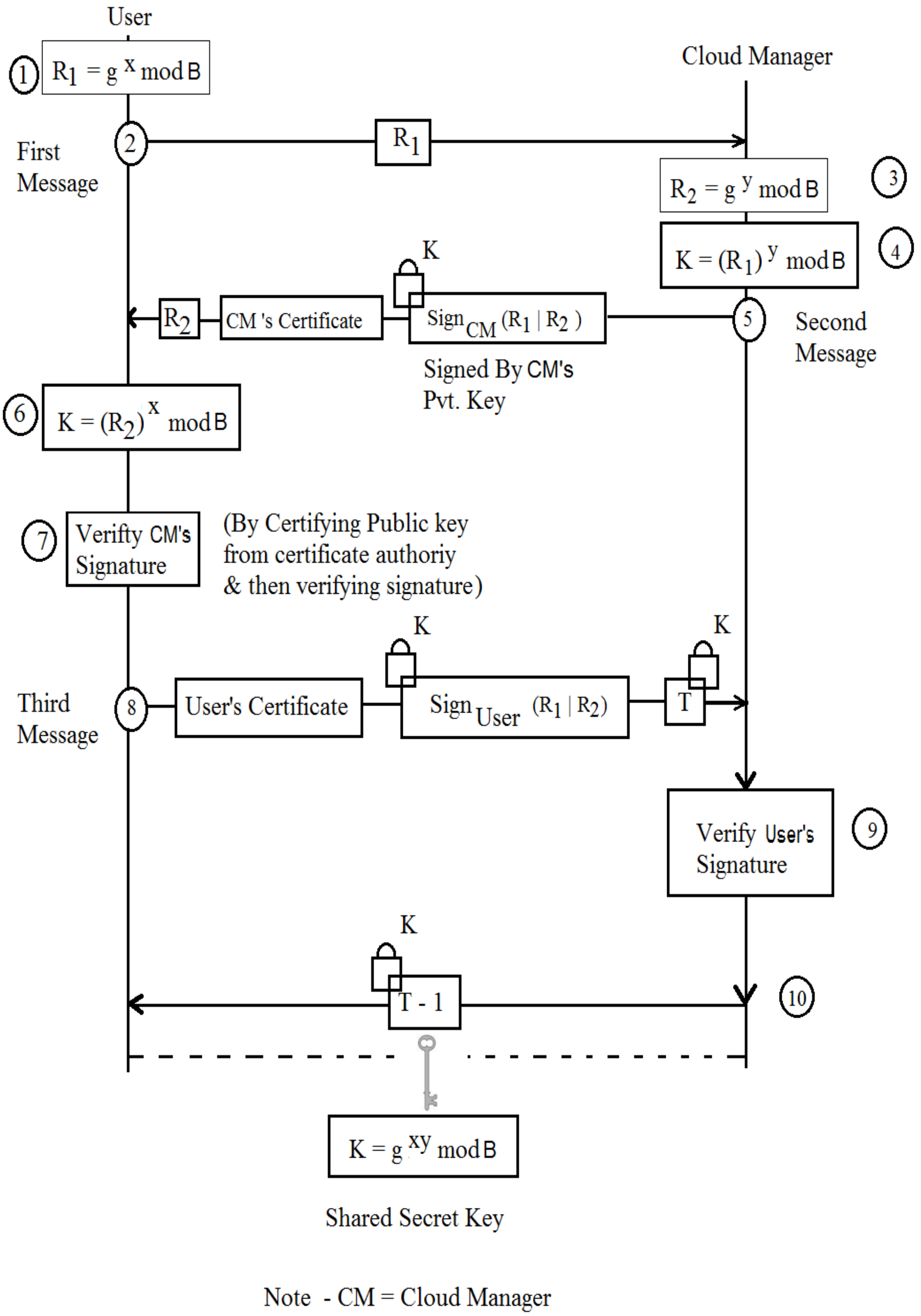

Figure 6.1: Station to Station Key Exchange Agreement

Chapter 7
Cloud Manager

As its name suggest cloud manager manage all those things of cloud server or things related to cloud server.

Cloud manager for cloud computing reduces risk for cloud computing users of their private data being stolen or being misused, and also assists the cloud provider to conform to privacy law.

Cloud Manager Act as a third party to issue session key between user and cloud server, Cloud manager will verify user credentials signed by user and then sent with request message for using any service from cloud.

After providing any of service to a user from the cloud sever cloud manager will remove that session key on which that service was used from session key allocated list managed by cloud manager.

Chapter 8
Related Work

Prashant Rewagad and Yogita Pawar [1]: They have chosen to make use of a combination of authentication technique and key exchange algorithm blended with an encryption algorithm. This combination is referred to as "Three way mechanism" because it ensures all the three protection scheme of authentication, data security and verification, at the same time. In this paper, we have proposed to make use of digital signature and Diffie Hellman key exchange blended with (AES) Advanced Encryption Standard encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of three way mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.

Uma Somani, Kanika Lakhani and Manish Mundra [2]: In Cloud computing, we have problem like security of data, files system, backups, network traffic, host security .They have proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique solves the dual problem of authentication and security. The strength of their work is the framework proposed to address security and privacy issue.

Siani Pearson, Yun Shen and Miranda Mowbray [5]: They have describe a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. They had described different possible architectures for privacy management in cloud computing; give an algebraic description of obfuscation, one of the features of the privacy manager; and describe how the privacy manager might be used to protect private metadata of online photos.

Siani Pearson [6]: Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust, and needs to be considered at every phase of design. In this paper the privacy challenges that software engineers face when targeting the cloud as their production environment to offer services are assessed, and key design principles to address these are suggested.

Mandeep Kaur and Manish Mahajan [8]: The prevalent problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers.

S. Ramgovind, M. M. Eloff and E. Smith [26]: According to them cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure. However the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. The purpose of the paper is to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Gartner's list on cloud security issues, as well the findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.

Wentao Liu [28]: According to him cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.

Chapter 9

Proposed Work

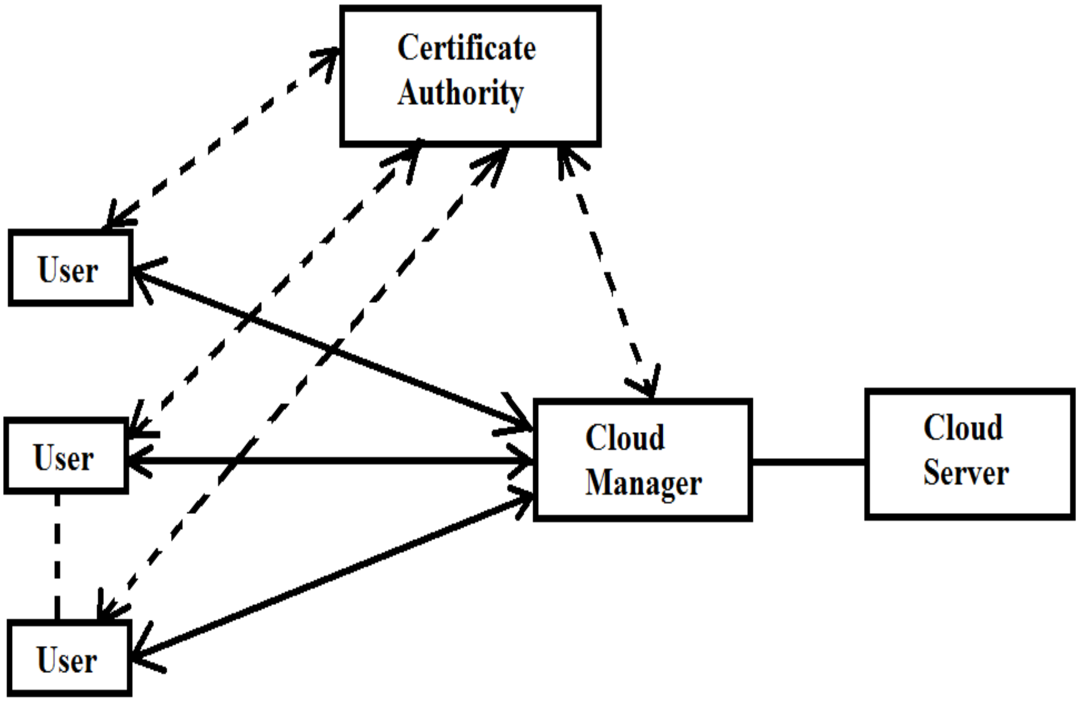

Figure 9.1: Proposed Model Entities layout

We are enhancing security of cloud by using Station to Station key agreement with Digital Signature Standard and Cloud Manager.

This model is working on 3 important parts:-

1. Cloud Manager
2. Station to Station key exchange agreement
3. Digital Signature Standard

Cloud Manager:

As its name suggest cloud manager manage all those things of cloud server or things related to cloud server.

Cloud manager for cloud computing reduces risk for cloud computing users of their private data being stolen or being misused, and also assists the cloud provider to conform to privacy law.

Cloud Manager Act as a third party to issue session key between user and cloud server, cloud manager will verify user credentials signed by user and then sent with request message for using any service from cloud.

After providing any of service to a user from the cloud sever cloud manager will remove that session key on which that service was used from session key allocated list managed by cloud manager.

Services provided by Cloud Manager:

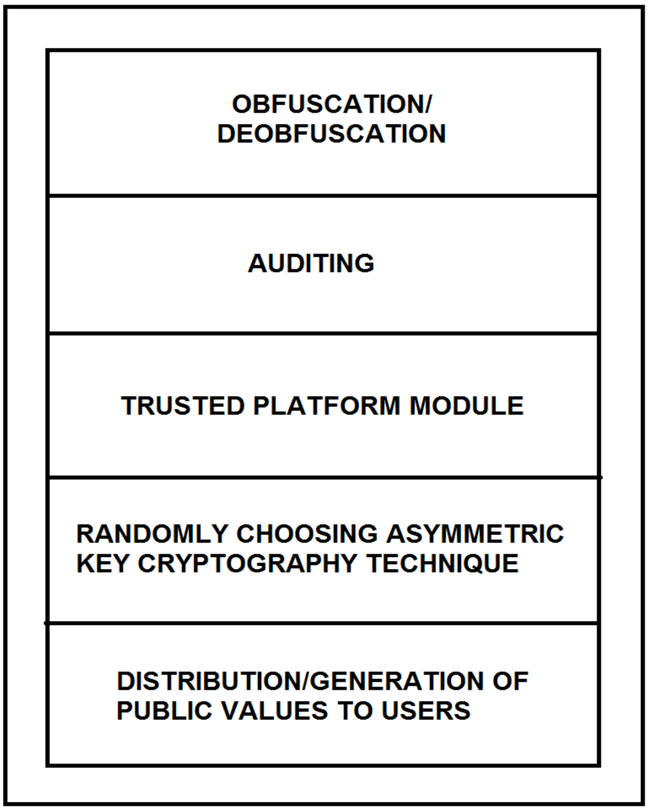
OBFUSCATION/
DEOBFUSCATION
AUDITING
TRUSTED PLATFORM MODULE
RANDOMLY CHOOSING ASYMMETRIC
KEY CRYPTOGRAPHY TECHNIQUE
DISTRIBUTION/GENERATION OF
PUBLIC VALUES TO USERS

Figure 9.2: Services Provided by Cloud Manager

Random Obfuscation: At the time any User will store its file/data on cloud at that time cloud manager will randomly choose one of provided asymmetric Encryption/Decryption method to encrypt provided data by user and store it in data storage of cloud. Randomly chosen encryption method information is stored in one file where all of the information of all files is there and that is encrypted with cloud manager public key.

Every time when a user will request a file from cloud then cloud manager will decrypt that file where all information regarding all files are present and will check from there that which algorithm is been used on user required file so as to de-obfuscate i.e. decrypt that file and provide to user.

After every de-obfuscation, again cloud manager will randomly choose encryption algorithm to obfuscate and store it.

With respect to the privilege of user cloud manager will provide data to him/her i.e. if user is owner then read/write only file is provided and if user is normal user then read only data is provided so that no unwanted changed could be done.

2. *Auditing:* It also act as an auditor by keeping all information regarding what service is provided to users and when. What users did with that service all information is audited.

3. *Trusted Platform Module:* It is a hardware that checks integrity of cloud manager. It decreases risk of unsecured access so increases confidentiality, by providing a tamper resistant hardware based security. Protected data can not be used by other platforms. So Trusted computing is been done and it yields trust in integrity of the privacy management, integrity of involved platforms.

4. *Random Encryption Method:* This service is used for obfuscation and deobfuscation and for that cloud manager have a list of asymmetric encryption

methods which it will randomly choose and save that information in a file which it maintains.

5. *Public Value Generation and Broadcast:* Cloud Manager provide values of g, P, q and B to users at the time of registration and broadcast new g, P, q and B values after timestamp is been reached. So new public key values and private key values are regenerated by users and their new certificates are created by certificate authority (digital certificates are renewed). G, P, q and B are used in Digital Signature Standard as well as in Station to Station key exchange agreement.
   - ($2^{L-1}< P<2^{L}$). L is a multiple of 64.
   - q Is prime divisor of P-1.
   - A random number h is chosen. 0<h<P-1, $g=h^{(P-1)/q}$ modB
   - A value B is also chosen pseudo-randomly or randomly so as to be used in Station to Station Key Exchange Agreement.

A timestamp is set for all these values and when this time expires then these values are regenerated and broadcasted to all users.

Files maintained by Cloud Manager:-

a) *Audit File:* This contains all auditing information.

b) *Session key allocation file:* This file maintains the information about session key provided to users and their timestamps.

c) *Data Files obfuscation information:* This file has information, which encryption method is used for which file for obfuscation.

d) *Public values File:* This file have all values which are public and there timestamp. From this file values are broadcasted to users (Here g, P, q and B are public values, which are broadcasted time to time).

Station To Station Key Exchange Agreement:

Station to Station (STS) key exchange agreement is commonly known as Station to Station (STS) protocol. Digital signatures with public key certificates are used to establish session key. It is based on diffie hellman, as in diffie hellman man in middle attack can took place but Station To Station key exchange agreement prevents man in middle attack. As session keys are created for a fixed time stamp it will increase security level.

Digital Signature Standard:

Digital Signature Algorithm is used in Digital Signature Standard based on Elgamal scheme with some ideas from Schnorr scheme. Digital signature standard signatures are faster than RSA Signatures. DSS signatures are smaller than other Signatures. Message send by user to cloud manager is encrypted by using session key already created by Station To Station key agreement.

Steps for getting a service from cloud:

1. *Registration:*

- User will register to cloud manager by providing required information and user name and password.
- After successful registration g, P, q and B values and hashing technique used for creating digests are provided by cloud manager to user.
- Then a random number x is chosen by user and that would be its private key and from that z = g^xmodB is been generated that is its public key (x and z values are renewed time to time when new values of g, P, q and B are received from Cloud Manager).

2. *Station to Station Key Exchange Agreement:*

Algorithm:

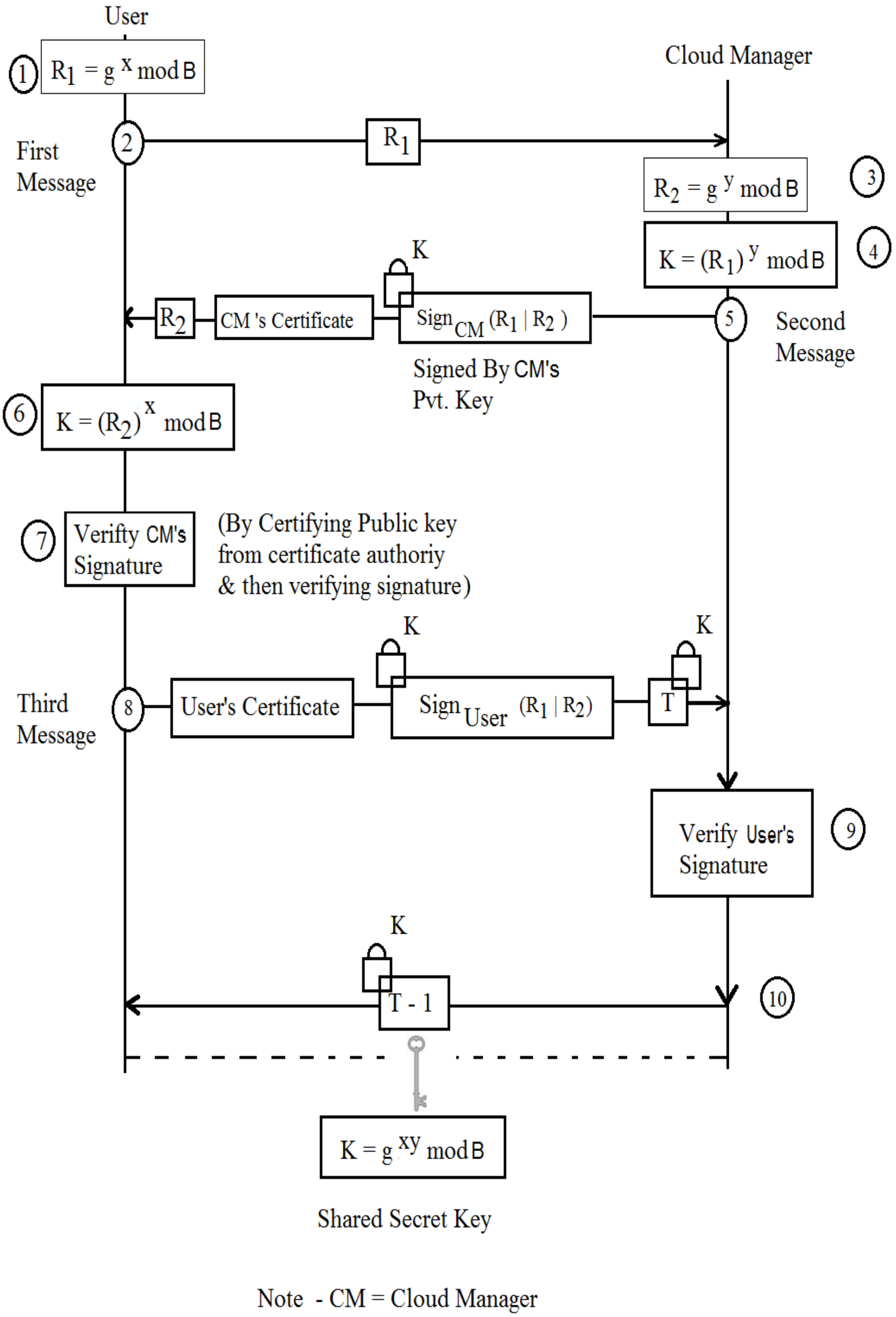

Figure 9.3: Algorithm of Station to Station Key Exchange Agreement

a) A random number x that is user private key is already been chosen at the time of registration with a time stamp and will renew it time to time when new g, P, q and B values are received then x is also renewed.

b) New user will calculate $R_1 = g^x \bmod B$ & send this R_1 to cloud manager.

c) After getting R_1, cloud manager will choose a random number y & find out R_2.

d) Now cloud manager will find out key (session key)
$K = (R_1)^y \bmod B$

e) After calculating R_2 & the session key, cloud manager concatenates R_1 and R_2 and then signs the result with the private key. Cloud manager now sends R_2, the signature & his own public key certificate to user. Signature is encrypted with session key.

f) Now after getting R_2 user will calculate session key & verify cloud manager signature by the certificate authority.

g) After that user will create a signature by concatenate $R_1|R_2$ and encrypt that signature by K & send user's certificate also & sent an encrypted Timestamp value to cloud manager.

h) Cloud manager will verify Digital signature of user & if it is verified the send the encrypted T-1. That means key K is been set for T-1 time.

3. *Digital Signature Standard:*

Algorithm:

Signing:-

a) User chooses a random number n ($1 \leq n \leq q$).

b) User calculates the first signature r = $(g^n \bmod P) \bmod q$.

(Note – value does not depend on M.)

c) User will create digest of Message h(M) by already shared hashing technique with users.

d) Now user will calculate 2nd signature

S = $(((h(M)+xr)n^{-1}) \bmod q)$

e) Now user will send r, s, session key encrypted M & session key encrypted z (public key of user) to cloud manager.

(Note: - Cloud manager won't store value of z.

Verifying:-

a) Cloud manager checks whether r or s is less than or greater than 0 or not because if any of value will be equal to zero then n must be chosen again.

b) Calculates digest using same hash algorithm as used by user because that's already been discussed.

c) Cloud manager calculates V = $\left(\left(g^{h(M)s^{-1}} z^{rs^{-1}} mod\, P\right) modq\right)$.

d) If r is congruent to V then message request is accepted.

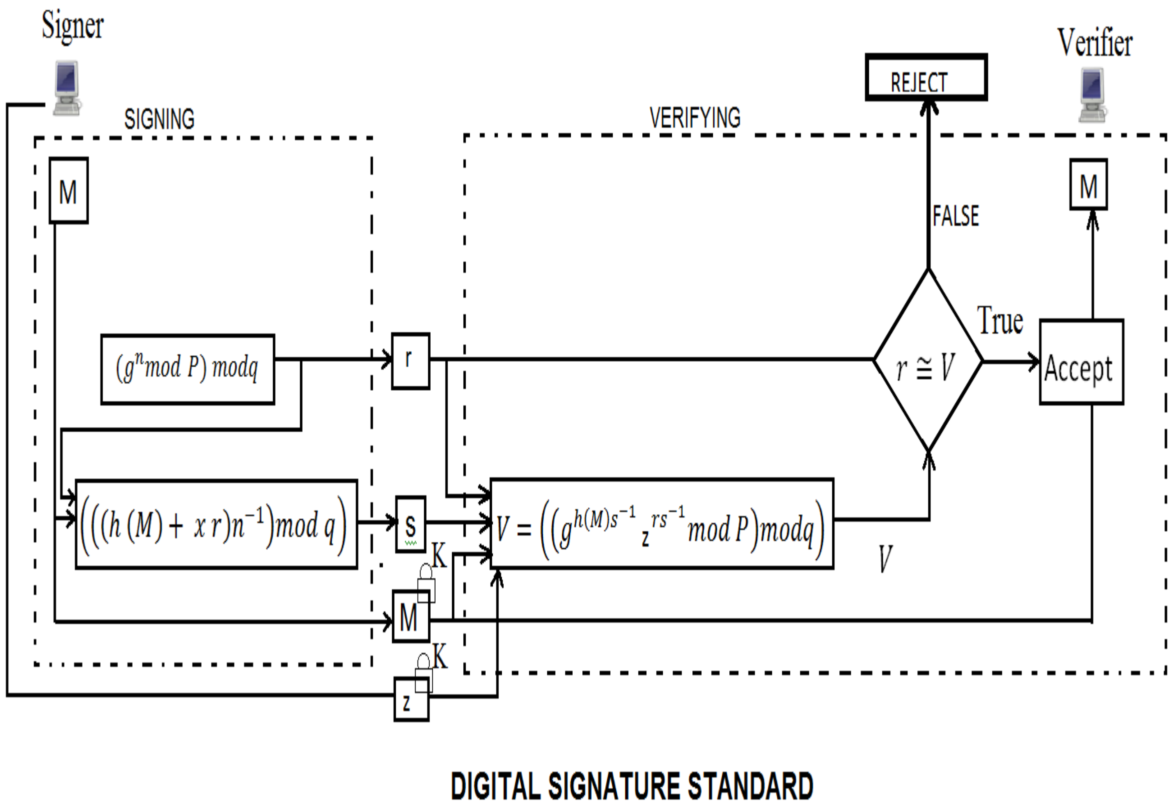
Signer
SIGNING
VERIFYING
REJECT
Verifier
M
FALSE
True
$(g^n \bmod P) \bmod q$
r
$r \cong V$
Accept
M
$((h(M) + xr)n^{-1}) \bmod q$
s
$V = ((g^{h(M)s^{-1}} z^{rs^{-1}} \bmod P) \bmod q)$
K
V
M
K
z
DIGITAL SIGNATURE STANDARD

Figure 9.4: Digital Signature Standard

4. *Providing services from cloud to user:*

- After verification from cloud manager cloud manager will directly provide service to user (except case of data uploading and downloading from data storage of server because in these case cloud manager will be involved for providing service).

- In case of File uploading on cloud:

After getting this request cloud manager will randomly choose one of Asymmetric algorithm for file and store by using its Public/Private key for encryption.

Cloud manager will maintain a file in which it will have information about data & which encryption also been used & it’s been locked by public key of cloud manager.

Every time if a user/owner will request for that file cloud manager will decrypt it & it by again randomly choosing an algorithm of then store it again. Only owner have privileged to overwrite a file.

- In case of downloading a File:

Cloud manager will first de-obfuscate that file first and then provide it to user according to its users.

Chapter 10
Conclusion

There are lots of security vulnerabilities and breaches in cloud computing, to deal with these breaches and vulnerabilities we have proposed a model in which by Station to Station Key Exchange Agreement a one to one medium is created between cloud server and user so as man in middle attack is completely eliminated by this, as session key is generated for fixed time interval, each session key generated for each time use and a file is been maintained that which session key is provided to which user so by all this replay attack is been eliminated and intruders can not use any users session key because for that a file is been maintained. Digital Signature Standard is used for authentication purpose. Cloud Manager will audit all users work on cloud and it will make files as tamper resistant by using tamper resistant module. Cloud Manager do lots of other functioning also like encrypt files by using different encryption algorithm. So Cloud Manager improves privacy and security. Therefore we have used three different parts to enhance security of Cloud Computing.

.

Chapter 11
Future Work

In further enhancement of Cloud Manager, dummy database i.e. Honeypot can also be provided to those whom Cloud Manager will find out that they are trying to use data services on the identity of other users. As by this intruders will think that they actually got that file what they wanted.

Multiple Signatures scheme can be used in place of single signatures if users will want this from Cloud Manager. Multiple signature scheme will make authorization process more secure.

Cloud Manager can further use different hashing techniques for different users as randomly chosen by it at the time of user registration. As this will make intruders work more difficult because they have to take all hashing techniques in account for digital signatures.

Chapter 12

References

[1] Mr. Prashant Rewagad and Ms.Yogita Pawar “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing” 2013 IEEE International Conference on Communication Systems and Network Technologies.

[2] Uma Somani, Kanika Lakhani, Manish Mundra “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[3] Siani Pearson, Yun Shen and Miranda Mowbray “A Privacy Manager for Cloud Computing” HP Labs, Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK.

[4] Volker Fusenig and Ayush Sharma “Security Architecture for Cloud Networking” 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.

[5] Siani Pearson “Taking Account of Privacy when Designing Cloud Computing Services” HP Labs, Bristol, UK.

[6] Deyan Chen and Hong Zhao **“**Data Security and Privacy Protection Issues in Cloud Computing”2012 IEEE International Conference on Computer Science and Electronics Engineering.

[7] Zhang Xin , Lai Song-qing and Liu Nai-wen “Research on Cloud Computing Data Security Model Based on Multidimension” 2012 IEEE International symposium on information Technology in medicine and education.

[8] Jian Wang, Yan Zhou, Shuo Ziang & Jiajin Le “Providing Privacy Preserving in Cloud Computing” 2010 IEEE.

[9] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi “Cloud Security Issues” 2009 IEEE International Conference on Services Computing.

[10] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, May 2011.

[11] Cong Wang, Qian Wang and Kui Ren ”Ensuring Data Storage Security in Cloud computing”, 23 IEEE International Conference on Computer and Information Technology; 2009, pp.1-9.

[12] Wassim Itani. Ayman Kayssi and Ali Chehab “Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures” 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[13] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud, ”IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[14] John Harauz, Lori M. Kaufman, Bruce Potter, “Data Security in the World of Cloud Computing”, IEEE Security and Privacy, July/Aug. 2009, vol. 7, no. 4, pp. 61-64.

[15] Mandeep Kaur and Manish Mahajan “Using Encryption Algorithms to enhance the data security in Cloud Computing” 2013 International Journal of Communication and Computer Technologies Vol 1, issue 3, January 2013.

[16] Shabnam Sharma & Usha Mittal “Comparative analysis of various authentication techniques in Cloud Computing” International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 4, April 2013.

[17] Dave Shackleford “Cloud Security and Compliance: A Primer” SANS Whitepaper-August 2010.

[18] Joshua Browser “The Security Onion Cloud” SANS Whitepaper-2013.

[19] Liang Yan, Chunming Rong, and Gansen Zhao “Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography” Proc. of the 10th Annual Conference for Australian Unix User’s Group, AUG 2004.

[20] M. Sudha and M. Monica “Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography” Advances in Computer Science and its Applications, Vol. 1, No. 1, March 2012.

[21] William Stallings, ”Cryptography And Network Security”, second edition, 2002.

[22] Wentao Liu “Research on cloud computing security problem and strategy”, 2012 IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 21-23 April 2012.

[23] A. Tripathi, A. Mishra “Cloud computing security considerations”, 2011 IEEE International Conference on Signal Processing, Communications and Computing(ICSPCC), 14-16 Sept. 2011.

[24] S. Ramgovind, M. M. Eloff and E. Smith “ The management of security in Cloud computing”, 2010 IEEE Information Security in South Africa(ISSA), 2-4 Aug. 2010.

[25] Paul McDougall, "The Four Trends Driving Enterprise Cloud Computing", http://www.informationweek.com/cloud-computing/blog/archives/2008/06/the-four-trends.html, 10 june 2008, retrieved 26 Feb 2009.

[26] A. Behl and K. Behl , “An analysis of cloud computing security issues”, 2012 IEEE 2012 World Congress on Information and Communication Technologies (WICT), Oct. 30 2012-Nov. 2 2012.

[27] Cloud Security Alliance (CSA) http://www.cloudsecurityalliance.org/.

[28] IDC, "IDC Ranking of issues of Cloud Computing model," http://blogs.idc.com/ie/?p=730/.

[29] Research paper-"Cloud Computing and Security-A Natural Match" http://www.trustedcomputinggroup.org/resources/cloud-computing-and security a natural match.

[30] Research paper-"Security Issues and Solutions in Cloud Computing" http://wolfhalton.info/2010/06/25/security-issues-and-solutions- in-cloud-computing/ISACA (auditor's perspective journal) http://www.isaca.org/ Journal/Past-Issues/2009/Volume-6/Pages/Cloud-Computing-An-Auditor-s-Perspective 1 .aspx .