Using Kerberos with Digital Signature and AES Encryption to Provide Data Security in Cloud Computing

Sreeja Nair
HOD CSE Department
OIST Bhopal

Nupur Gautam
Student
OIST Bhopal

Meenakshi Choudhary
Student
OIST Bhopal

ABSTRACT
The Cloud Computing is the next generation platform that provides dynamic resources pools, virtualization, and high availableness. Today, with the assistance of those computing, we are able to utilize ascendable, distributed computing environments among the boundary of the web, It provides several edges in terms of low value and accessibility of information, conjointly offers associate degree innovative business model for organizations to adopt It's services while not forthright investment. Except for these potential gains achieved from the cloud computing, there are plenty of security problems and challenges related to it and conjointly knowledge privacy protection and knowledge retrieval management is one in all the foremost difficult analysis add cloud computing. To supply security a range of cryptography algorithms and mechanisms are used. Several researchers opt for the simplest they found and use it numerous combinations to supply security to the information in cloud. In this paper, we've got planned to form use of Digital signature and Kerberos with Advanced Encryption Standard cryptography (AES) algorithm program to guard Authentication, Confidentiality, and Integrity of information hold on in cloud.

General Terms
Security, Encryption Algorithms

Keywords
Cloud Computing, Digital Signature, Kerberos, AES Encryption Algorithm.

1. INTRODUCTION
Cloud Computing is the Internet based next generation platform and is employed in computer. It may be defined as utilizing the net to supply technology enabled services to the people and organizations [1] also provide sharing of computing resources to handle applications. It offers reduced cost, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, through which many enterprises wants to include so as to enhance their way of working and allows users to run their applications anywhere and access to the desire services at any time. Except these properties, "Security within the Cloud" is one amongst the foremost important issues. Already many researcher survey cloud security problem with RSA algorithm and digital signature, and also combination with digital signature with Diffie Hellman Key Exchange and AES Encryption algorithm, and RSA algorithm, Digital signature and Kerberos. In this paper, we tend embody new combination Digital signature with Kerberos Version five and AES Encryption algorithm. So we feel with this long filtering we are able to enhance the safety problem within the cloud.

Fig 1: Cloud Computing

1.1 Characteristics of Cloud Computing:
1.1.1 on-Demand Self-service
It allows users to use cloud computing resources and conjointly use of cloud services like computation and storage as needed in additionally to managing and deploying these services.

1.1.2 Virtualization Technology
The main aim of virtualization technologies is to cover the underlying infrastructure. It offers flexibility and conjointly allows a dynamic datacenter wherever lots of pool of resources that are provided by the servers that are controlled as needed, and computation, storage, and network resources changes dynamically.

1.1.3 Broad network access
In Cloud computing, high information measure communication links should be on the market to attach to the cloud services.

1.1.4 Location freelance Resources pooling
Resources which are available in cloud environment may be set anyplace within the geographic locations physically and assigned as virtual elements whenever they're required. Here, client has no management or data over the precise location of the provided resources.

1.1.5 Measured Service

In cloud computing, resources usage may be monitored and beaked mechanically for that individual session, and according by providing transparency for each the supplier and client of the used service.

1.2 Cloud Computing Models

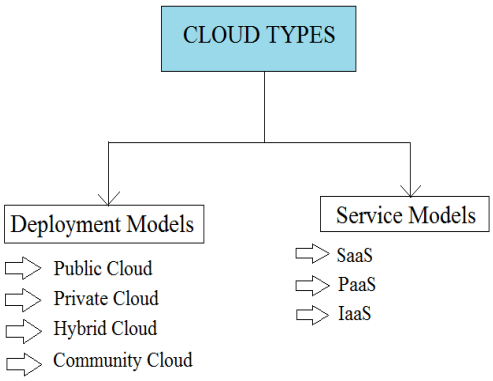


Fig 2: Cloud Computing Models

There are two Categories:

1. Service Models
2. Deployment Models

1.2.1 Service Models

1.2.1.1 Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on an infrastructure.

1.2.1.2 Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

1.2.1.3 Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

1.2. 2 Deployment Models

1.2.2.1 Private Cloud

The cloud infrastructure is operated for a non-public organization. It's going to be managed by the organization or a 3rd party, and should exist on premise or off premise.

1.2.2.2 Public Cloud

The cloud infrastructure is created on the market to the final public or an oversized trade cluster and is owned by a corporation merchandising cloud services.

1.2.2.3 Hybrid Cloud

The cloud infrastructure could be a composition of 2 or additional clouds (private, community, or public) that stay distinctive entities, however there are certain along by standardized or proprietary technology, that permits information and application immovableness (e.g., cloud explosive for load-balancing between clouds).

1.2.2.4 Community Cloud

The Cloud infrastructure is shared by many organizations and supports a selected community that has communal issues (e.g., mission, security needs, policy, and compliance considerations). It's going to be managed by the organizations or a 3rd party, and should exist on premise or off premise.

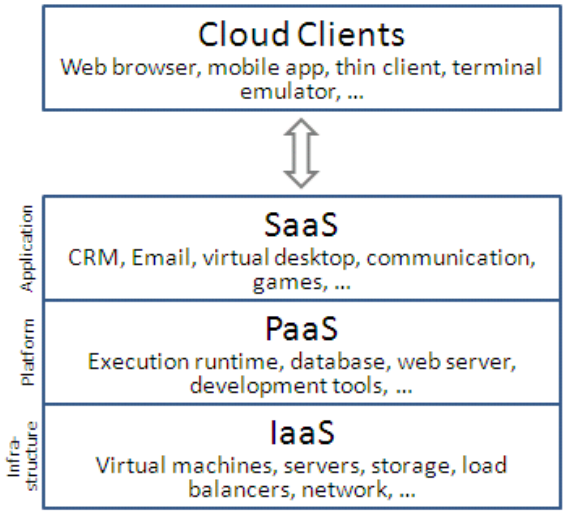


Fig 3: Cloud Computing Models with Examples

2. CLOUD COMPUTING SECURITY ISSUES

Cloud Computing with the virtualization will facilitate corporations accomplish additional by breaking the physical bonds between associate degree IT infrastructure and its users, heightened security threats should be overcome so as to profit absolutely from this new computing paradigm. With the cloud model, you lose management over physical security. In public cloud, you're sharing computing resources with different corporations. In a shared pool outside the enterprise, you don't have any data or management of wherever the resources run. Exposing your information in associate degree atmosphere shared with different corporation may offer the govt. "reasonable cause" to seize your assets as a result of another company has profaned the law. Just because you share the atmosphere within the cloud, might place your information in danger of seizure.

The following list contains many security problems highlighted by Gartner that organizations and key call manufacturers, as a requirement, ought to remove with Cloud Computing Vendors [4]:

2.1 Privileged Access:

Who has specialized/privileged access to data? Who decides regarding the hiring and management of such administrators?

2.2 Regulative Compliance:

Is that the cloud vendor willing to bear external audits and/ or security certifications?

2.3 Data Location:

Will the cloud vendor provide any management over the situation of data?

2.4 Data Segregation:
Is encoding on the market the least bit stages, and were these encoding schemes designed and tested by older professionals?

2.5 Recovery:
What happens to information within the case of a disaster, and will the seller provide complete restoration, and if so, however long will that method take?

2.6 Investigative Support:
Will the seller have the flexibility to research any inappropriate or illegal activity?

2.7 *Long-term viability:*

What happens to information if the cloud vender goes out of business is client information came back and in what format?

2.8 Data Availability:
Will the cloud vendor move all their clients' information onto a distinct atmosphere ought to the prevailing atmosphere become compromised or unavailable?

3. PROBLEM STATEMENT
With Cloud Computing, Organizations will use services and knowledge is hold on at any physical location outside their own management. This facility raised the varied security queries like privacy, confidentiality, integrity etc and demanded sure computing surroundings whereby knowledge confidentiality is maintained. To induce trust within the computing, there is a need of a system that performs authentication, verification and encrypted knowledge transfer, therefore maintain knowledge confidentiality.

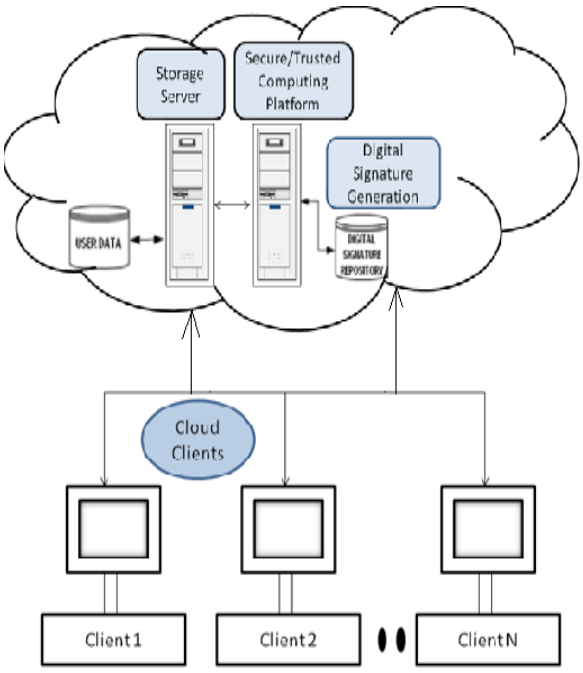
4. RELATED WORKS
4.1 Lakhani et al[6], have downside like security of information, files system, backups, network traffic, host security. They have projected an idea of Digital Signature with RSA formula, to write in code the information whereas transferring it over the network. These systems solve the twin downside of authentication and security. The strength of their work is that the framework projected to deal with security and privacy issues.

4.2 As per Jose, Sanjeev and Suyambulingom[4], They projected to gat RSA public keys and personal keys for public and personal access to beat the matter of information security certificate computer file is employed within management node configuration file to create positive cloud knowledge flow firmly. The management node sends knowledge through Secure Socket Layer once certificate activation. Finally AES formula is employed for secret writing. This distinctive combination makes this resolution best to forestall differing types of attacks. The strength of their work is robust knowledge security against varied attacks. If a user plans to login incorrectly for several times, the system mechanically retardation the service and briefly stop the account service for the actual user.

4.3 As per heidari [7], they projected Union of RSA formula, Digital signature and KERBEROS in cloud security. They used the Kerberos authentication service for problems the price ticket and granting ticket for all users only for building additional security. Digital signature with RSA formula, to encrypt the information whereas we tend to area unit transferring it over the network. A digital signature could be a mathematical theme for demonstrating the genuineness of a digital message or document. At the primary all users connecting to the cloud must build the profile and getting the parole from Kerberos and then they'll get entry to cloud realm for mistreat the cloud and share the data with impact of RSA formula and digital signature. During this article they tend to outline an admin. Admin ought to build the prohibit for all users according to their information processing. At the primary each information processing should be ensure with admin. Second they must apply for taking the price tag. Finally they'll catch the cloud service supplier, but within the cloud realm they have to use the RSA formula and Digital signature for causation the data.

4.4 As per Mr. Rewaged & Pawar [8], They proposed use of Digital signature with Diffie Hellman key Exchange and AES secret writing formula to boost knowledge Security in Cloud Computing. They use combination of authentication technique associate degreed key exchange formula. This mixture is remarked as "Three manner mechanisms" as a result of it ensures all the 3 protection themes of authentication, knowledge security and verification, at an equivalent time. During this paper, they need projected to create use of digital signature and Diffie Hellman key exchange homogenized with (AES) Advanced Secret writing commonplace secret writing formula to guard confidentiality of information hold on in cloud. Notwithstanding the key in transmission is hacked, the power of Diffie Hellman key exchange render it useless, since key in transit is of no use while not user's personal key, that is confined solely to the legitimate user.

5. PROPOSED METHODOLOGY



In these paper we tend to embraced combination of 3 mechanism digital signature with Kerberos five and AES secret writing which give enhance knowledge security in cloud computing.

5.1 Kerberos Authentication Service

Kerberos is one amongst secure technique for authenticating letter of invitation for a service in a network. Kerberos was developed within the Pallas at the Massachusetts Institute of Technology. Users once send the request, they'll take price ticket and granting ticket and eventually which will be accustomed request a specific service from a server.

5.2 Digital Signature

A digital signature or in straightforward manner is written signature could be an authenticated electronic documents. This signature cannot be pretend and it asserts that a named person wrote or otherwise in agreement to the document to that the signature is connected. The recipient of a digitally signed message will verify that the message originated from the person whose signature is connected to the document which the message has not been altered either purposely or accidentally since it had been signed. Also, the signer of a document cannot later deprive it by claiming that the signature was cast. In different words, digital signatures modify the "authentication" and "non-repudiation" of digital messages, reassuring the recipient of a digital message of each, the identity of the sender and also the integrity of the message.

5.3 AES Algorithm

AES algorithm was revealed by bureau in 2001. It is a bilaterally symmetric Block cipher with a block length of 128 bits and support for key lengths of 128,192 and 256 bits. Bureau handpicked Rijindael because the projected AES formula. Dr.Joan Daemen and Dr. Vincent Rijmen are two researchers who developed and submitted Rindael for the AES.

Decryption in AES algorithm involves reversing all the steps taken in secret writing mistreatment inverse functions like InvSubBytes, InvShiftRows, and InvMixColumns.

6. WORKING PROCESS

In Cloud Computing, we've several issues like security of information, file system, backups, network traffic, host security, and alter the information and plenty of additional. Here at the primary we tend to area unit proposing an idea of Kerberos authentication service for problems the price tag for all taking part over the network. Here we tend to use the Kerberos version five which includes extra functionalities compare to previous version of Kerberos. Suppose any user or shopper need to use the cloud services and connecting to cloud, firstly, they have to hook up with the Kerberos and build the profile of information in Kerberos data base for safer. At consecutive step the Authentication Server (AS) of Kerberos do verifies user and created the granting ticket and session key and it sent to the users. Consecutive step users sent the grating ticket and session key to Ticket Granting Server (TGS) for getting the service. Then TGS send price tag and session key for user. In final step the users send the request service to cloud service supplier service to users.

The method of this situation is in 5 steps:

6.1 The shopper logs on the digital computer and sends requests access a price tag-granting ticket on behalf of the user by causation its user's ID to the AS, alongside TGS ID, indicating letter of invitation to use the TGS service.

6.2 The AS responds with a price tag that's encrypted with a key that's derived from user parole. Once this response arrives at the shopper, the shopper prompts the user for his or her parole, generates the key, and try rewriting the incoming message. If the proper parole is provided, the price tag is with success recovered. As a result of solely the proper user ought to apprehend the parole, solely the proper user will recover the price tag. Thus, we've used the parole to get credentials from Kerberos while not having to transmit the parole in plaintext. The price tag itself consists of the ID and network address of the user, and also the ID of the TGS. This corresponds to the primary situation. This is often that this price tag can be employed by the shopper to request multiple cloud service granting tickets, that the granting ticket is to be reusable. However, we tend to don't want associate degree opponent capture the price tag and waits till the user has logged off his or her digital computer. The opponent either gain access to work station or assemble his digital computer with an equivalent network address as that of the victim. The price tag includes a timestamp, indicating the information and time that the price tag was issued, and a life, indicating the length of your time that the price tag is valid. Thus, the purchasers apprehend encompasses a reusable price tag and wish not hassle the user for a parole for every new service request.

6.3 The shopper requests a service-granting price tag on behalf of the user. For this purpose, the shopper transmits a message to the TGS containing the user's ID, the ID of the cloud service, and also the price tag-granting ticket.

6.4 The TGS rewrite the incoming price tag and verifies the success of the decipherment by the presence of its ID. It checks to create positive that the life has not terminated. Then it compares the user ID and network address with the incoming information to manifest the user. If the users are allowed to access to V, the TGS provides a price tag to grant access to the requested cloud service supplier. The service granting supplier price ticket has an equivalent structure because the ticket-granting ticket. Indeed, as a result of the TGS could be a server, we might expect that an equivalent components area unit required manifesting a shopper to an application server. Again, the tickets contain a time stamp and lifelong. If the user needs access to an equivalent cloud service at a later time, the shopper will merely use the antecedently no heritable service-granting price tag and wish not hassle the user for parole. Note that the price tag is encrypted with a secret key (Kv) better-known solely to the TGS and also the server, preventing alteration. Finally, with a specific cloud service- granting price tag, the shopper will gain access to the corresponding service with next step.

6.5 The user request access to cloud service on behalf of the user. For this purpose the shopper transmits a message to the server containing the user's ID and also the cloud service granting price tag, the server authentication by mistreatment the contents of the price tag. Once this method the users will used the cloud service supplier, expect for creating safer we tend to outline the AES formula and digital signature within the cloud realm. All users at the primary should pass the filter of Kerberos and also the second they'll entry to cloud realm, once entry to cloud realm and taking the cloud service, for safer they have to doing follow the AES formula and digital signature.

Assume we've two enterprises A and B. this enterprise passed the Kerberos filtering then associate degree enterprise has a public cloud server with knowledge, applications and plenty of other things. Company B needs a secure knowledge from A Cloud. We tend to area unit here, making an attempt to send a secure knowledge to B by mistreatment Digital Signature with AES secret writing formula.

7. CONCLUSION

In this paper, we have embraced different surveys of the issues in cloud service supplier wherever several researchers have shown an increase in the security problem in cloud taking different combinations and conjointly outlined new combinations of digital signature, Kerberos version five with AES secret writing technique for the safety problems in cloud services. Kerberos version five provides Authentication service with extra functionalities like Realm that indicates realm of user and n number of times that it is employed at the shopper's request. Confidentiality and Integrity is provided by the Digital Signature. Several research workers use RSA formula for secret writing however during this paper we tend to embrace AES formula, since AES formula consumes least secret writing and decipherment time and buffer usage compared to RSA. In this paper we have outlined a technique for enhancing the safety downside with 3 filtering. At the primary every information processing should be ensured with admin. Second they must apply for taking the price tag. Finally they'll catch the cloud service supplier, however within the cloud realm they have to use the AES formula and digital signature for causation of the data.

8. REFERENCES

[1]. Farhan Basher Sheikh and Sajjad Haider "Security Threats in Cloud Computing", 2011 IEEE sixth international conference on net Technology and secured transactions, 11-14 Gregorian calendar month 2011, national capital U.S. of Arab Emirates.

[2]. G.J. Popek and R.P. Goldberg,"Formal

necessities for virtualizable third generation architectures", Communications of ACM, vol.17, no.7, 1974 pp.412-421.

[3]. P.Barham et al," Xen and also the art of virtualization", in proceedings of the nineteenth ACM conference on in Operation Systems principles (SOSP'03), New York, USA, 19-22 October 2003,pp.164-177.

[4]. G. Jai arul Jose, C. Sajeev, Dr. C. Suyambulingom "Implementation of information security in Cloud Computing" International Journal of P2P network trends and Technology Volume1 Issue1-2011.

[5]. Sherif el-Etriby, Eman M. Mohamed and Hatem s. Abdelkader revealed "modern cryptography techniques for Cloud Computing randomness and Performance testing "Within the third international conference on communications and knowledge technology ICCIT 2012.

[6]. Uma Somani, Kanika Lakhani, manish Mundra "Implementing Digital Signature with RSA Cryptography rule to boost the information security of Cloud in Cloud Computing" 2010 IEEE first International Conference on Parallel, distributed and Grid Computing (PDGC-2010).

[7]. Mehdi Hojabri & Island Heidari, department of atomic number 55 and SE Andhra University, Vizag, asian nation E-mail: hozhabri64@gmail.com, monaheid@gamil.com "Union of RSA rule, Digital signature and KERBEROS in Cloud Security".

[8].Mr. prashant Rewagad*1 box, Dept of computing & Engineering prashant_rewagad@rediffmail.com Ms.Yogita Pawar*2 M.E. student, Dept of Computing & Engineering pawaryogita04@gamil.com. "Use of Digital signature with differ hellman key Exchange and AES cryptography rule to boost information Security in Cloud Computing".