International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 05, May-2015

Privacy Preserving Authentication Protocol by Shared Authority in Cloud

Pradnya Rama D S
Student, Dept. of CSE
East West Institute of Technology
Bengaluru, Karnataka

Chandan Raj B R
Assistant Professor, Dept. of CSE
East West Institute of Technology
Bengaluru, Karnataka

***Abstract* – This paper discusses the current problem faced in the cloud computing with regard to preserving the privacy in sharing the data. Cloud computing offers set of services and resources utilizing internet. These services are provided from data centers which are located throughout the world. Contemporary business models for organizations to deploy IT services are offered by cloud computing without any upfront investment. Cloud computing simplifies providing the virtual resources from anywhere in the world to anywhere in the world via internet. With the large-scale adoption of cloud computing, security issues are the main challenges which are need to be solved efficiently and effectively. The proposed system provides a solution for preserving the data in cloud with the aid of encryption protocol. Three modules are presented here namely data owner, Third Party Administrator, and retailer. Advanced Encryption Standard algorithm is implemented in the current work for encrypting the data which has to be stored in the cloud. This data can be retrieved by retailer on providing the valid signature key to decrypt the data.**

Keywords –cloud computing, privacy preservation, data integrity, shared authority

I. INTRODUCTION

Cloud-computing is a computer utility or model, which provides services and resources to any user or organizations using Internet. Cloud computing specifies to both applications which are delivered as services and systems software and hardware in the datacenters that implement these services [1]. The term "cloud computing" is also referred to network-based services which are provided by virtual hardware, but these appears to be maintained by real server hardware. These services run on one or more real machines by software simulation [2]. There is no such standard or agreed-upon definition to define cloud is exists. The US National Institute of Standards and Technology (NIST) define cloud computing as follows [3]:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models".

The cloud model consists of 5 necessary characteristics to enable availability, which are; on-demand self-service, resource pooling, broad network access, measured service, and rapid elasticity. Three service models are Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS). The deployment models are classified into four types such as Private cloud, Public cloud, Community cloud, and Hybrid cloud. The technologies for Cloud Computing include; (1) Powerful, inexpensive server computers (2) Fast wide-area networks and (3) High-performance virtualization for hardware products [3].

The major challenges involved in deploying cloud are; security threats related to data and software [4], cost of data communication [4], charging model [4], Server Level Agreement (SLA) [5], issues related to migrating data [6], and cloud interoperability issue [4].

The proposed system in this work is presented to secure the data using Advanced Encryption Standard (AES) algorithm. The AES, also referred as Rijndael [7], [8] is a standard specification for encrypting the electronic data authorized by the U.S. National Institute of Standards and Technology (NIST) in 2001 [7]. AES is the most widely used encryption standard. AES algorithm can encrypt and decrypt 128-bits of plaintext and ciphertext. This algorithm uses variable length key of size 128, 192, or 256 bits [9].

The essential characteristics, delivery models and deployment models of cloud computing architecture are organized in section II, also with the need and methods of encryption. Section III provides the insight into the proposed system and followed by results and conclusion in section IV and section V.

II. RELATED WORK

A brief review on essential characteristics, delivery models and deployment models of cloud computing architecture are presented in this section.

A. Essential characteristics of cloud computing

On-demand self-service: Whenever consumer requests for an application for arrangement of computing capabilities, such as network storage and server time, these services should be provided automatically without any human interaction with the requested service provider [3].

Broad network access: The services provided by cloud computing should be accessed by every consumer and through standard procedures that enhance use by heterogeneous thin or thick client platforms such as, tablets, mobile phones, laptops, and workstations [3].

Resource pooling: The computing resources are managed by provider to serve multiple consumers using a multi-tenant model, with various virtual and physical resources dynamically assigned and reassigned as per consumer request. The consumers generally don't have knowledge over the mere exact location of the provided resources but are able to determine location at a higher level of abstraction for e.g., state, country, or datacenter. These examples of resources include memory, storage, network bandwidth and processing [3].

Rapid elasticity: The capabilities of cloud computing can be elastically provided and released, automatically or semi-automatically to rapidly outward and inward compatible with demand. The capabilities provided for provisioning to the customer are often appear to be unlimited and can be allotted in any quantity of time [3].

Measured service: Cloud systems regulate and improve resource use by leveraging a metering capability at particular level of abstraction allotment to the type of service e.g., bandwidth, processing, storage, and active user. For providing transparency for both provider and consumer resource utilization can be regulated, reported, and surveyed of the utilized services [3].

B. Delivery models of cloud computing

Software as a Service (SaaS): In this model the consumer have the capability to use the provider's applications running on a cloud infrastructure. These applications can be accessed from different client devices through either program interface or a thin client surface (e.g., web-based email on web browser). The consumer doesn't have the capability to control or manage the underlying cloud infrastructure including operating systems, network, storage, servers, or any individual application capabilities, with the possible exception of constrained user-specific application configuration settings [3], [10].

Platform as a Service (PaaS): The facilities provided to the customer in this model is to setup onto the cloud infrastructure consumer-acquired or created application developed using libraries, programming languages, services, and tools supported by the provider [3]. The consumer in this model has the ability to control over the deployed applications and possibly configuration settings for the application-hosting environment but the consumer does not regulate or monitor the underlying cloud infrastructure including servers, networks, storage, or operating systems [10].

Infrastructure as a Service (IaaS): In this service model the capabilities to the customer provided by provider are to arrange and regulate networks, storage, processing, and any other basic computing resources where consumer can run and deploy arbitrary software, which includes applications and operating systems [3]. The consumer in this model doesn't facilitate or control the underlying infrastructure but has the control over deployed applications, storage, operating systems, and has a limited control of networking components such as host firewalls [11].

C. Deployment models of cloud computing

Private cloud: The private cloud infrastructure is facilitated for exclusive use by a single organization constitutes multiple consumers (e.g., business units). It may be operated, managed, and owned by a third party, organization, or few combinations of them, and it exists on or off premises [3], [11].

Community cloud: Any particular community of consumers can use this deployment model of cloud infrastructure exclusively, which have shared concerns such as, security requirements, mission compliance, and policy considerations. This model can be operated, managed, and owned by one or more organizations in the community, a third party, or some combination of them and this model may exist on or off premises [3], [11].

Public cloud: The cloud infrastructure is facilitated for open use by the general public. This deployment model can be operated, managed, and owned by a academic, business, or government organization, or any few combination of these. This model exists on the premises of the cloud provider [3], [11].

Hybrid cloud: This deployment model of cloud computing infrastructure is a combination of two or more distinct cloud infrastructure (private, community, or public) which remain unique entities, but these infrastructures are constrained together by standardized or proprietary technology that enables data and application portability for e.g., cloud bursting for load balancing between these cloud models [3], [11].

III. CLOUD COMPUTING CHALLENGES

There are many challenges facing by cloud computing consumers and providers, who are still doubtful about its trustworthiness. Based on a survey conducted by International Data Corporation (IDC) in 2008 [12], and 2009 [13]; the leading challenges for deploying and utilizing cloud computing by organizations are as follows:

Security: Security plays crucial role in impeding cloud computing acceptance. For e.g., running our software, putting our data on someone else's hard disk using someone else's CPU troubles us a lot. The primary security issues are data loss, botnet (running remotely on a collection of machines), and phishing which cause serious hazards to organization's software and data. For example consider an hacker who utilize cloud to facilitate botnet as Cloud generally provides more stable infrastructure services at a cheaper price for them to start an attack. These kind of multi-tenancy model and managing computing resources in cloud has developed new security challenges that require innovative techniques to handle with [4].

Costing Model: The consumers of cloud must consider the understanding between communication, computation, and integration. Shifting to the cloud can significantly lower the infrastructure cost, it does increase the cost of data communication, i.e. cost of sharing an organization's data from and to the community cloud and public cloud and the cost per unit of computing resource used is relatively more. The problem of cost is particularly noticeable if the consumer deploys the hybrid cloud model where the organization's data is shared between number of public/private (in-house IT

infrastructure)/community clouds. Apparently, on-demand computing makes it worth only for CPU intensive jobs [4].

Charging Model: The elastic resource pool calculates their cost based on utilization of static computing, which has made the cost analysis a lot more difficult than regular data centers. Moreover, an instantiated virtual machine has developed into the unit of cost analysis instead of the underlying physical server. The cost of establishing multi-tenancy within the contribution can be very significant for SaaS cloud providers. These consist: redevelopment and re-design of the software that was genuinely used for single-tenancy, price of providing latest features that allow for intensive customization, security improvement and performance for concurrent user access, and dealing with complications induced by the above changes. Subsequently, SaaS providers are required to sum up the trade-off amongst the provision of multi-tenancy and the cost-savings allowed by multi-tenancy such as minimized number of on-site software licenses, etc. Accordingly, strategic and feasible charging model for SaaS provider is very important for the sustainability, reliability and profitability of SaaS cloud providers [4].

Service Level Agreement (SLA): Whenever the consumers immigrates their core business model functions onto the authorized cloud they do need to safeguard availability, performance, quality, and performance of these resources even though the consumers doesn't have control over the underlying cloud infrastructure which means it is important for consumers to posses guarantees from providers on service delivery. Mostly, these are supported through Service Level Agreements (SLAs) discussed between the consumers and providers. SLA specifies the suitable granularity, such as the arrangement between complicatedness and expressiveness, so that they can cover most of the consumer expectations and this is approximately simple to be verified, enforced, evaluated, and weighted by the resource pooling mechanism on the cloud. Adding to this, various cloud offerings (IaaS, SaaS, and PaaS) will require defining various SLA meta specifications. This relatively raises the number of implementation problems for the cloud providers. Moreover, advanced SLA mechanisms require to constantly incorporate user feedback and customization features into the SLA evaluation framework [5], [14].

What to migrate?: Based on a survey (Sample size = 244) supervised by IDC in 2008 [13], the seven IT systems/applications being migrated to the cloud are: IT Collaborative Applications (25.4%), Management Applications (26.2%), Applications Development and Deployment (16.8%), Personal Applications (25%), Business Applications (23.4%), Storage Capacity (15.5%) and Server Capacity (15.6%). By looking at the percentage of migration to cloud clears that the organizations worry in moving their data onto the cloud. Organizations are limited in employing in IaaS compared to SaaS, this happens because of the fact that marginal functions are often outsourced to the Cloud, and essence activities are kept in-house [6].

Cloud Interoperability Issue: The offerings established by various clods has its own way on how cloud users/applications/clients collaborate with the cloud, leading to "Hazy Cloud" phenomenon. This inhibits the development of cloud ecosystem by causing vendor locking, which hinders the ability of users to optimize resources at various levels within an organization which has to be chose from alternative vendors/offering simultaneously. More particularly, proprietary cloud APIs makes it hard to coordinate cloud services within an organization's own current traditional systems for e.g., an on-premise data center for highly interactive modeling applications in a pharmaceutical company [4]. The important goal of cloud interoperability is to understand the seamless fluid data over clouds and amongst local applications and cloud. The number of levels that makes interoperability crucial for cloud computing are:

Firstly, an organization often requires holding in-house assets and capabilities correlated with their core competencies to enhance the IT and computing resources while outsourcing insignificant functions and activities for e.g., the human resource system on to the cloud.

Secondly, more often than not, for the need of advancement, an organization may need to contract out a number of minimal functions to cloud services offered by various vendors.

Standardizing the rules of interoperability issue proves to be a good solution to address the existing interoperability problems. In this current era of technology, interoperability issues can be reduced to its minimal effect [4].

IV. PROPOSED SYSTEM

The challenges of cloud computing which are presented in section III, seems to be big threat for any organizations or providers to step into the cloud computing business. In the proposed system, threats related to data authentication, data privacy, and data security are resolved with the aid of well established Advanced Encryption Standard (AES) algorithm and Key Generation algorithm for encrypting and decrypting the data, thus providing data privacy and generating keys for authenticating and securing the data.

Proposed system consists of three modules namely Supplier (Data owner) module, Carrier (Third Party Administrator [TPA]) module, and Retailer (user) module. The architecture of the proposed system working model is shown in Fig. 1. This work has been done in J2EE Eclipse software with the aid of JSP, Java Servelet and HTML programming languages. These modules are established to avoid data privacy, data security and data authentication issues in cloud computing.

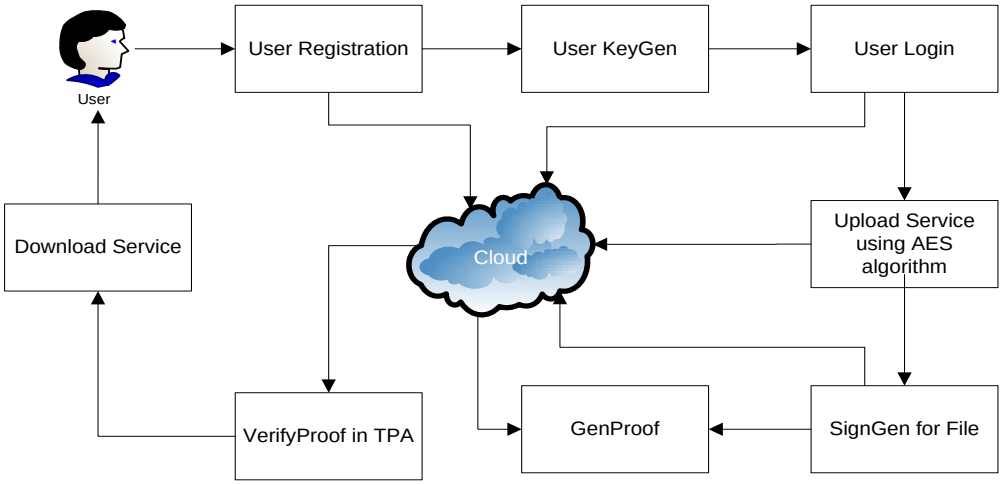

Fig.1. Architecture design of the proposed system.

1. Supplier/Data owner Module:

This module is responsible for encrypting and uploading the encrypted data in cloud. The data could be any file which includes text files, audio files, image files, etc. Supplier has to login with the credentials provided to respective organization to upload the data to the cloud.

2. Retailer/User Module:

User Registration module: This module contains the fields like User Name, Password, Email-id and Contact Number which has to be entered by the user. After entering all fields, user details will be stored in the Cloud. TPA will verify the details which are stored in the cloud and sends acknowledgement to the user. If the details are correct then TPA will send message as "Authenticated" or else "Unauthenticated".

User Key Generation Module: In this module, dynamic key is sent to the client on successful authentication during User Registration module. Dynamic key is a unique key which is generated and sent to user during each login session. It offers much higher security than static passwords.

User Login Module: This module contains the fields like User Name, Password and User Key Value, whose field have to be entered by the user. And before login he/she should be registered as a user, so after registration only he can login and use the secured system in cloud computing.

Key Generation: This module is used to generate key for a file that is file key is sign generation and key for user is key generation. User needs to enter his key and file key to retrieve it.

3. Carrier/TPA Module:

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security when requested on behalf of the user. Users believe on the Cloud Server for cloud data maintenance and storage. They may additionally dynamically interact with the Cloud Server to access and update their stored data for various application purposes. The users may resort to TPA for ascertaining the storage security of their outsourced data, protect their data from TPA.

V. IMPLEMENTATION

Data privacy and data security is preserved using Advanced Encryption Standard (AES) algorithm in the proposed system. AES also referred as Rijndael, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES is the most adopted algorithm for encryption and is fast and flexible. AES is a symmetric encryption algorithm which is also called as single key cryptography. It utilizes a single key for both encrypting ad decrypting the data. In this method, the receiver and the sender has to agree upon a single secret (shared) key. Given a message, which is called plaintext and key, encryption produces unintelligible data, which will be the same length as plaintext. Decryption is the reverse of encryption uses same key as encryption. Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data. For example, a source produces a message in plaintext, $X = [X_1, X_2, X_3... X_M]$ with the message X and the encryption key K as input, the encryption algorithm forms the cipher text $Y = [Y_1, Y_2... Y_N]$. This may be written as $Y = EK(X)$. Cipher text Y is produced by using encryption algorithm, where E indicates the encryption algorithm used and K indicates the key used for encryption. The receiver of this message should apply decryption algorithm with same key used for encryption to get the actual message $X = DK[Y]$. Here D indicates decryption algorithm.

AES algorithm works on 4×4 column-major order matrix of bytes, but few versions of AES have larger block size and have additional columns in the state. Moreover, more AES calculations are done in a special finite field. The key size specifies the number of repetitions required to convert the plain-text into cipher-text for AES cipher. The number of cycles required for repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

There are several processing steps to be done in each round, each containing four similar but different stages, consisting one that depends on the encryption key itself. To obtain the plaintext back from ciphertext, a set of reverse rounds should be applied to transform ciphertext into original plaintext using the same encryption key. The common steps involved in encrypting the data are AddRoundKey, SubBytes, ShiftRows, and MixColumns.

Description of AES algorithm is presented below:

1. KeyExpansions – round keys are derived from the cipher-text using Rijndael's key schedule. This algorithm need separate 128-bit round key block for each round with one more addition.

2. InitialRound – In this round AddRoundKey step is implemented. Each byte of the state is combined with a block of the round key using bitwise xor.

AddRoundKey – This step combines subkey with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule, where each subkey is similar in size as state. Bitwise XOR operation is used to add subkey by combining each byte of the state with the corresponding byte of the subkey.

3. Rounds – SubBytes, ShiftRows, MixColumns and AddRoundKey steps are utilized.

SubBytes – This is a non-linear substitution step where each byte is substituted by 8-bit Rijndael's substitution box according to a lookup table.

ShiftRows – This step performs its operations o the rows of the state; it shifts the bytes cyclically in each row by a specific offset. First row is left unchanged, each byte of the second row is shifted one to the left, and similarly the third and fourth rows are shifted by two and three offsets respectively.

MixColumns – Four bytes of each column of the state are combined using an invertible linear transformation in this step. The MixColumns function considers four bytes as input and outputs four bytes, where each input byte affects all four output bytes. ShiftRows combined with MixColumns provides diffusion in the cipher.

4. ***Final Round –*** Except MixColumns step, SubBytes, ShiftRows, and AddRoundKey steps are performed.

VI. CONCLUSION

Cloud computing establishes immense prospects, but the security threats related to cloud computing ways are directly proportional to its offered benefits. One of the biggest security threats with cloud computing are data sharing. Security issues such as data privacy, data authentication, data security with related to cloud computing can be solved with the help of encrypting the data. AES encryption algorithm is robust, fast and flexible. The symmetric nature of AES algorithm which uses single key to encrypt and decrypt data proves to be fast and uses less computational time. TPA manages and verifies the required necessities efficiently so that the data can preserve its privacy efficiently.

REFERENCES

[1] Michael Armbrust, et.al, "Above the Clouds: A Berkeley View of Cloud Computing", UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[2] P.Vijaya and P.Mallika, "Improved Secure Access Control in Cloud Using Sign Based Ciphertext-Policy Attribute-Based Encryption", International Journal On Engineering Technology and Sciences (IJETS), Volume 1, pp. 178-182, 2014.

[3] Peter Mell and Timothy Grance "The NIST Definition of Cloud Computing", National Institute of Standards and Technology (NIST) Special Publication, 2011.

[4] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing", IEEE International Conference on Cloud Computing, 2010.

[5] Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the Service World." IT Professional, Volume 11, pp. 28-33, 2009.

[6] Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, 2010.

[7] "Announcing the Advanced Encryption Standard (AES)". Federal Information Processing Standards Publication, United States National Institute of Standards and Technology (NIST), 2012.

[8] Daemen, Joan and Rijmen, Vincent, "AES Proposal: Rijndael". National Institute of Standards and Technology (NIST), 2003.

[9] Milind Mathur and Ayush Kesarwani, "Comparison between DES, 3DES, RC2, RC6, Blowfish and AES", Proceedings of National Conference on New Horizons in IT-NCNHIT, 2013.

[10] D. A. Menasce and P. Ngo, "Understanding cloud computing: Experimentation and capacity planning," in Proc. of computer measurement group conf., pp. 1-11, 2009.

[11] IBM Global Services, "Cloud computing: defined and demystified explore public, private and hybrid cloud approaches to help accelerate innovative business solutions", 2009.

[12] IT Cloud Services User Survey, "Top Benefits & Challenges", http://blogs.idc.com/ie/?p=210, 2011.

[13] "New IDC IT Cloud Services Survey: Top Benefits and Challenges", http://blogs.idc.com/ie/?p=730, 2011.

[14] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, and P.Sai Kiran "Research Issues in Cloud Computing", Global Journal of Computer Science and Technology, Volume 11, 2011.