ISSN:0975-9646

A Hybrid Security Service To Achieve Strong Authentication And Cryptography For Cloud Applications

Vivek Dandir, Prof. Mohsin Sheikh

Department of Computer Science and Engineering,
Medi-Caps Institute of Technology and Management
Indore, M.P, India

***Abstract*-- Cloud computing is the recent technology by which various applications and other computing things can be delivered as a service. Mainly it is a formal combination of distributed, grid, cluster, elastic and utility computing. Such computation provides a quality of service based robust usage experience for the user. It serves reduced complexity and service expandability for making standardization. This leads to improved operational efficiencies and offers the client reduced predictable annual costs. Other benefits were realized in areas, such as self service, service catalog, automatic provisioning and deprovisioning, and capacity flexibility. A cloud provides clients with features, such as disaster recovery, security, and metering, which enable clients to reduce costs, increase standardization, and improve business continuity**

In cloud the data center is the location where the users all confidential information is stored by some security schemes provided by the service provider. Along with users normal data there is any more secure and private data which need to be hidden from even service provider and that type of control is not provided by any provider in the market.

Any organization needs securing access to corporate networks, protecting the identities of users, ensuring that a user is who he claims to be and protecting the integrity of business-critical transactions. However, the recent surge in high-profile security threats, as well as evolving business environments requires entirely new considerations for access control. Cloud offerings and mobile platforms represent a shift in how trust and control is established and maintained.

This evolving environment requires a comprehensive set of security services, yet flexible enough to quickly adapt to ever changing requirements without impacting the applications and access control infrastructure in use. Smooth migration is an essential aspect of such flexibility.

With this work, the aim is to make the application level of security provided by any of the servers or provide more effectively and according to the users need. For achieving the confidentiality attribute based encryption is used. Digital signature and multi factor authentication like single sign on one (SSO) are some of their examples. They should be delivered as a service so that multiple small scale companies might also integrate them to serve their users in a better way. Multiple authentication mechanisms, like digital signatures, certificates or 2-factor security and several identity validators can coexist and can be combined to suite the most complex needs.

***Keyword*: Cloud Security, Encryption (KP-ABE), Single Sign on (SSO), Digital Signature.**

I. INTRODUCTION

Cloud must have a planned approach to providing the security control to users along with application access and other important factors. The organization leads towards deploying the server, which offers security functionality. Along with the security factors performance factors should also be kept in a min, because if the security control is heavier than the other applications and their usability might get affected.

Thus a balance must be mad in between the security approach complexity and the kind of resources they are occupying and how they affect the application response. There are some points which keep in concern always while developing cloud security mechanisms.

They are:

- Effective resource management with virtualization support
- Robust service delivery with reliable communications
- Automotive process with reduced fault and performance burdensome and load handling
- Making security just above the value of information
- SOA based security service model

- **Understanding Cloud Service Models**

Here are the different layers, starting at the bottom:

Infrastructure as a Service (IaaS) is a provisioning model in which an organization outsources the equipment used to support operations, including storage, hardware, servers, and networking components. The service provider owns the equipment and is responsible for housing, running, and maintaining it. The client typically pays on a peruse basis.

Platform as a Service (PaaS) is the capability provided to the consumer to deploy onto the cloud infrastructure, consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application hosting environment.

Software as a Service (SaaS) is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- **Cloud Security Challenges**

Technological advancements over the last few decades will lead the social and informational system more secure. It empowers the user's identity belongings and let them more confidential as per the user's needs. Cloud computing is not secure by nature. Security in the Cloud is regularly elusive and less obvious, which definitely makes an incorrect conviction that all is well with the world and anxiety about what is really secured and controlled. The off-premises computing ideal model that accompanies distributed computing has brought about incredible concerns about the security of data, particularly the integrity and confidentiality of data, as cloud service suppliers may have complete control on the computing infrastructure that underpins the services.

Some of those identified areas where the security elaborations can be made are:

(i) Encapsulated information security standards along with service applicability must be applied over the computing servers
(ii) User and organization defined policies should take a control over the traditional security mechanism used for confidentiality and integrity.
(iii) User's belongings and its personal information must be made secure even against the service providers also.
(iv) Security must be of light weight so that additional load cannot be placed on the resources configured.

Since the CSP is the authority that controls the data items stored in the system, the CSP can look into data items stored in cloud storage without the data owner's permission. Thus to make the system more reliable client needs to make some security trusted deals with its data. The actual deployment of cloud computing services is not reliable as they claim because the existing security model doesn't work after migration of services to clouds. This work aims towards making the security more effective by suggesting a novel model which provides security controls over as a service.

Mainly the controls include some of the cryptographic algorithms, single sign on (SSO) and digital signature, all under a single service. It serves as a hybrid mechanism which assures the confidentiality of the user's data and privacy in accessing its configured applications. The cryptographic standards serve multiple algorithms simultaneously.

- **Security Requirements**

The requirements of such mechanism are:

1) **Confidentiality of data:** No one can uncover information about data content from the query and response as well as the cipher texts itself.
2) **Privacy of the data owner**: No one can learn the actual identity of the data owner from the encrypted content.
3) **Integrity and Authenticity of Data**: It provides the correctness of the data which is sent by the user and the originality which is assured by the digital signature to confirm the source identity and its data ownerships.

BACKGROUND

1) Attribute Based Encryption

Attribute-based encryption suggested that one's identity can be viewed as a combination of several attributes expressing the characteristics of the user in the form of access policy by using Boolean expressions such as AND, OR, or NOT. Later studies are broadly categorized into key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE) studies. In KP-ABE, the access policy is associated with keys corresponding to attributes implying that an encryptor is not authorized to grant access to the encrypted content except of descriptive attributes for the data by the encryptor's choice.

On the other hand, CP-ABE is complementary to KP-ABE by enabling encryptor to specify access policy combined with the ciphertext. Both schemes allow secure one-to-many communications such as targeted broadcasts for a specific group and individual user according to their attributes, which are distinct from the traditional cryptographic approaches requiring the explicit identity of the intended receivers.

Although both schemes are steadily improved in different situations, the attribute list in KP-ABE and the access structure in CP-ABE incorporated in ciphertext are exposed in the form of plaintext. This may lead privacy issues such as vulnerability to a guessing attack or information collection of the encrypted content because those attributes are exposed to any party. Some studies suggested modification of ABE schemes by hiding the access policy. These schemes operate on the assumption that the data owner directly delivers the ciphertext to the receiver without an intermediate third party. In other words, when adopting those approaches directly in cloud storage, decryption keys can be exposed to an untrusted third party. Hence, they are not feasible for data retrieval services in the cloud storage systems because the test procedure allows the CSP to learn which attributes the user has.

2) Secure Exchanges using SAML and SSO

SAML is Security Assertion Markup Language. The purpose of the SAML standard is to describe and exchange security information via SAML assertions between online business domains that trust each other. This standard has strict syntax and rules for managing SAML assertions. The

SAML is the core standard used for designing cloud authentication service in this project and the design is based on cloud authentication frameworks described in the following referenced papers. The SSO is single sign on mechanism which takes benefits from the usage of the SAML standard for serving the solution to transfer security information independent of any specific platform, domain and protocol.

Any user or client application, before accessing any resource provided by the application service, is first required to be authenticated. The SSO can be initiated in system and the authentication process contains multiple interactions between different system entities. The end-user first connects to the application service provider through request resource message in order to request access to a protected resource or service. The request message is intercepted by the PEP server.

If the end-user does not have a valid local session for that particular application service, PEP returns an authentication request message, such as SAML Authentication Request and directs the end-user to the SSO service provider. The user connects to the strong authentication server via HTTP Redirect message protocol. Getting the certificate verification result, the authentication server requests the SAML server to issue a SAML ticket.

The SAML Authentication Response ticket is returned to the user through the authentication server according to the HTTP Post message protocol. More specifically, if the user has been successfully authenticated, then PEP creates a local valid session.

3) Digital Signature

The digital signature is a method to authenticate any document. It is a proof to the recipient that the document comes from the correct entity (sender). In the present world most of the documents are electronic due to the cult usage of the computer and its applications like email, e-banking, e-voting, etc. Thus the message, data, documents or any other materials in electronic format has to be signed electronically. This signature that is done electronically is known as Digital Signature. The approach can provide various services like message authentication, message integrity and non repudiation. Non-repudiation can be provided using a trusted party. A digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. The various digital signature schemes are RSA digital signature scheme, ElGamal digital signature scheme, Schnorr digital signature scheme, Digital Signature Standard (DSS) scheme and elliptic curve digital signature scheme.

II. LITERATURE SURVEY

During the last few years various approaches had been developed for improving the current security situations in cloud computing. Aim is towards making the data exchanges and transition more secure against the attackers. Thus, this work mainly deals with security as a service using cryptographic primitives, SAML with single sign on and the digital signature. Some of the articles which relate the work is covered here as surveyed literature.

This paper proposes the first key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant ciphertext size [9]. Towards achieving this goal the paper show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model.

In a key-policy attribute-based encryption scheme, ciphertexts are associated with a set of attributes and private keys correspond to access structures A. Decryption is possible when the attribute set is authorized in the access structure A. It describes a new efficient identity-based revocation mechanism that, when combined with a particular instantiation of general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-size ciphertexts. The downside of these new constructions is that private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes.

The paper [10] had suggested a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms. First is setup which is used as a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK. Second is encryption that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the ciphertext E. Key Generation This is a randomized algorithm that takes as input – an access structure A, the master key MK and the public parameters PK. It outputs a decryption key D. Third is decryption in which the ciphertext E that was encrypted under the set γ of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M. In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. The paper also demonstrates the applicability of suggested construction to sharing of audit-log information and broadcast encryption.

The paper deals with providing security as a service for cloud application using SAML [11]. The implementation of Security Assertion Markup Language (SAML) and its capabilities to provide secure single sign-on (SSO) solutions for externally hosted applications. If the user accesses the external webpage without passing through the internal federated identity manager first, the service

provider will need to issue the SAML request back to the identity provider on behalf of the user. This process of SSO is called service provider initiated. In this case, the user arrives at a webpage specific for the company, but without a SAML assertion.

The service provider redirects the user back to the identity provider's federation webpage with a SAML request, and optionally with a Relay State query string variable that can be used to determine what SAML entity to utilize when sending the assertion back to the service provider. The highest SAML component level is profiles, or the business use cases between the service provider and the identity provider that dictate how the assertion, protocol and bindings will work together to provide SSO. Some of the related web browser profiles for implementing SSO are singe logout profile, artifacts resolution profile, name identifier management profile etc.

In the paper [12], detailed description of SAML is shown along with some modification related to their constrained specifications. It does not include a general security analysis, but provides an attack-by-attack list of countermeasures as security consideration. The paper also presents a security analysis of the SAML Single Sign-on Browser/Artifact profile, which is the first one for such a protocol standard. The analysis of the protocol design reveals several flaws in the specification that can lead to vulnerable implementations. SOAP over HTTP is one of the most important bindings of the SAML Single Sign-on protocol. It utilizes SSL 3.0 or TLS 1.0 with unilateral authentication as communication channel for connections that require confidentiality and integrity. As this binding exceeds the security requirements of the protocol itself, attacks will be more difficult to accomplish. Even a protocol binding with underlying SSL/TLS channels and unilateral authentication can be broken. Most implementations will simply use SSL/TLS channels with unilateral authentication, which complicates or prevents man-in-the-middle and replay attacks. First of all, we strongly recommend that secure channels such as SSL 3.0 or TLS 1.0 with unilateral authentication for message transfer always be used. They outmatch normal transfer of signed and encrypted messages, as they provide authentication, freshness, and replay prevention.

It is important to name protocol type, protocol step, source and destination of a message explicitly in the message. Such measures could for instance prevent attacks where multiple services of a site are involved.

The paper [13] is a white paper given by Salesforce that focuses on Single sign-on process that allows network users to access all authorized network resources without having to log in separately to each resource. Single sign-on allows you to validate usernames and passwords against your corporate user database or other client application rather than having separate user passwords managed by Salesforce.

They offer the following ways to use single sign-on:

- Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization.
- Delegated authentication, single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the permission level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by permissions, not by organization.

Thus, using a stronger type of user authentication, such as integration with a secure identity provider makes your login page private and accessible only behind a corporate firewall. It also differentiates your organization from all other companies that use Salesforce in order to reduce phishing attacks.

The paper [14] continues the above process by further elaborating the explanations about the SSO. The paper suggested a provide formal models of the protocol corresponding to one of the most applied use case scenario (the SP-Initiated SSO with Redirect/POST Bindings) and of a variant of the protocol implemented by Google and currently in use by Google's customers (the SAML-based SSO for Google Applications). The paper had also analyzed these formal models with SATMC, a state-of-the-art model checker for security protocols. SATMC has revealed a severe security aw in the protocol used by Google that allows a dishonest service provider to impersonate a user at another service provider.

The demonstration will reproduce this attack in an actual deployment of the SAML-based SSO for Google Applications. This security aw of the SAML-based SSO for Google Applications was previously unknown.

The above paper covers the two main aspects of this work which are encryption standard KP-ABE and the single sign on (SSO) using SAML.

Now the third phenomenon is a digital signature and is covered here in the paper [15]. Digital signature deals with the security issues of the organizations. It could be achieved by the various mechanisms. This paper mainly works towards Elgamal Digital Signature [EDS] Algorithm which is used in wide applications had proved its efficiency in safeguarding the data.

However, due to different choppers the data is not firmly, reaching the safe side. The previous methods proposed using this EDS Algorithm had given appropriate measures using several methods in protecting the data. But there are some flaws which made EDS Algorithm efficiency poor. The paper also proposes an advanced EDS Algorithm with keys generated through statistical approach which consists of combination of random numbers and prime numbers blend with an Exclusive OR ($\oplus$) operation to enhance the complexity for the key to be generated. EDS Algorithm also ensures security and time complexity of improved

signature. This proposed method can give us an authentication with a Digital Signature for decryption of the data at the receiver side very sanctuary.

The paper [16] further scales the knowledge of digital signature for authenticity of and integrity of an electronics document. It is also used to achieve non-repudiation service, which provides proof for sent or received messages. In this paper we propose a new digital signature scheme using a novel message digest algorithm, 'Algorithm for Secure Hashing-160 (ASH-160)'. This proposed scheme has been implemented in java and the results are analyzed and compared with RSA digital signature scheme using SHA1 and RIPEMD160.

The analysis of experimental results reveals an increase in security strength and slight improvement in the efficiency of RSA with ASH160 than the compared schemes. On the basis of experimental results we can conclude that RSA digital signature scheme using ASH160 consumes less CPU time while encryption process but a little bit more time in decryption process. But in the security point of view the ASH160 is stronger than the SHA1 and RIPEMD160 algorithms.

This work show a path to design new message digests for digital signatures and also strengthen the existing hash algorithms by introducing new mathematical functions which takes less CPU time and withstand against security attacks.

III. PROBLEM DEFINITION

After studying the various factors and approaches of Single Sign on (SSO), digital signature and encryption standard there are some issues identified which still not resolved. These are:

(i) The traditional security control will provide the effective security, but these are loaded heavily with complex operations.
Thus, there must be some approach which reduces the load on the system as well as the user's memory.

(ii) In a cloud environment, all the security options are given by the service provide. Thus, there is not any option where the user plays a role in security for more trust. Thus, by using attribute based encryption, the user attributes will generate the key which could be used in cryptosystems.

(iii) There must be a single approach which provides strong authentication, confidentiality of the user's data and its integrity in single roof.

"**Thus the work mainly focuses on faster response, minimum load, higher security**. "

IV. OBJECTIVES OF WORK

- To develop the security framework for cloud platform which can work across the cross platform
- Reduces the users load from complex security control by using the single sign process using SAML.
- To achieve data isolation with strong authentication along with confidentiality and integrity.
- To provide security in depth with reduced operations
- To work with new encryption standard for cloud Computing having users role in encryption (KP-ABE)
- To focus which security threats can be unsafe to cloud computing and how they can be avoided.
- To analyze the cloud computing, data security features and enhances them for robust applications.

V. PROPOSED SYSTEM

Over the last few years there is a change in technology takes place which shift the user from normal web to interactive webs such as 2.O. This causes a sudden growth in the number of users accessing their applications and other computing resources as a service named under a single roof of Cloud Computing. Thus, for making the system more robust against the attack regarding confidentiality, integrity and authentication, some enhanced mechanism needs to be incorporated with the traditional system. This work proposes a novel hybrid security service model to achieve strong authentication and cryptosystem using single sign on (SSO), key policy attributes based encryption and digital signature.

The components which are integrated will keep the problem resolve and provides effective fine grained access with strong encryption controlled by users attribute elements as a key. The system architecture of the suggested mechanism is given in figure 1.

All it needs is to reduce the security control, heavy loaded operation to some simple control with restricted constrained specifications. The proposed system utilizes the system, cookies and other information for reducing the user credential remembrance loads. Also the other strategies are here incorporated with SAML for assuring the depth security with information value sustainability.

Also, the cloud is a third party location where the users' trust over the system gets reduced if there are an unauthorized access or data losses or theft. The best ways to increase this trust is to give some control in user's hand.

All the above things keep in concern while developing the solution.

Design Architecture

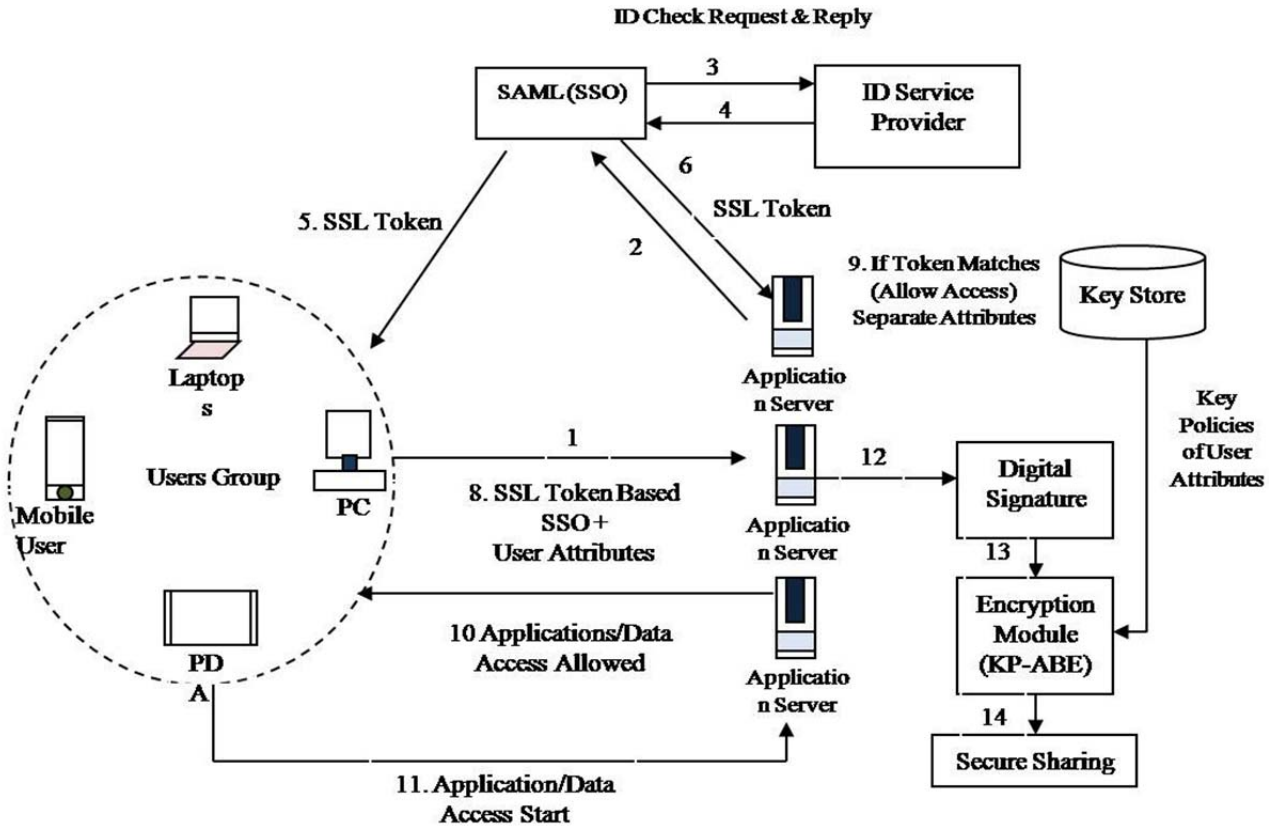

Figure 1: Hybrid Security Service to achieve Strong Authentication and Cryptography

Process Description: The proposed system will provides an effective trusted third party identity authentication using security assertion markup language with strict rules for creating and verifying the single sing on (SSO). The process starts with the users request for accessing its application or data from any of the cloud service provider's application server. By the user's organization or user name, separation is made and a request is send to some identity controller which is SAML. This SAML will verify the identity of the user and checks the users request zone. Now the SAML (SSO) controller will generate a response in the form of security certificate of SSL. This security certificate copy is send to the application server as well as the user's device. Now the users request again sends with this token to the application server and the server verifies both the token. If the token is same then the control is granted to users. This process will satisfy the strong authentication requirements and will provide finer grained access control.

Once the user gets controlled on its application or login is, various sessions and logs are maintained for analyzing the user's behaviors and activity. From this logging information the user's attributes are taken out and stored. This stored information is converted to some key by xoring their values. Application and users' data now digitally signed for user's authenticity which also assures the integrity.

Later on this data for users is encrypted using key policy attribute based encryption. Here the prior separated users attribute is converted to some key which is passed in RSA for encrypting the data and sending to the network. This will works a secure sharing of users file.

The above mechanism is provided as a service having hybrid security mechanism applicable at different locations of data and access. At the last evaluation of the approach analytically seems to provide effective security solution in near future.

VI. EXPECTED BENEFITS

(i) SAML based SSO will provide effective interoperability across the different identity providers. It will also enable once click access and reduces the complex process of access authentication.

(ii) Data isolation and access control can be guaranteed by using access and key policies for various types of user. Policies are used here to define finer grained access control.

(iii) Information value is sustained and security is provided according their value.

(iv) The digital signature will assure the authenticity and integrity of data and user operations.

(v) SAML is a fast, responsive mechanism will reduce the access time.

(vi) It prevents the phishing and fabrication, replay modification attacks.
(vii) Reduces the load and burdensome of password remembrance of multiple accounts.
(viii) KP-ABE will secure the users' data with its own defined controls based on users activity or attributes. Thus the users here were playing a role in his own security.
(ix) The new key combination approach is developed to further increasing security through key policy using attribute based encryption. Multiple attributes of user is combined together to generate a new key in this.

VII. CONCLUSION

Cloud is in the market every in industries as well as individuals. along with the features of the cloud, security another important consideration.

Any organization need, securing access to corporate networks, protecting the identities of users, ensuring that a user is who he claims to be and protecting the integrity of business-critical transactions. However, the recent surge in high-profile security threats, as well as evolving business environments requires entirely new considerations for access control. Cloud offerings and mobile platforms represent a shift in how trust and control is established and maintained.

With this work, the aim is to make the application level of security provided by any of the server or provider more effective and according to the users need. For achieving the confidentiality attribute based encryption is used. Digital signature and multi factor authentication like single sign on one (SSO) are some of their examples. They should be delivered as a service so that multiple small scale companies might also integrate them to serve their user in a better way.

Multiple authentication mechanisms, like digital signatures certificates or 2-factor security and several identity valuators can co-exist and can be combined to suite the most complex needs.

REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak "Decentralized Access Control with Anonymous
Authentication of Data Stored in Clouds" IEEE 2013.
[2] Wentao Liu "Research on Cloud Computing Security Problem and Strategy" IEEE 2012.
[3] Deyan Chen, Hong Zhao " Data Security and Privacy Protection Issues in Cloud Computing" 2012 International Conference on Computer Science and Electronics Engineering
[4] Ming Li , Shucheng Yu, Yao Zheng, *Student,* Kui Ren, Wenjing Lou, " Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attributbased Encryption " IEEE Transactions On Parallel And Distributed Systems 2012
[5] Silvio Micali Leonid Reyzin ,"Improving The Exact Security Of Digital Signature Schemes" 2000
[6] Cloud Security Alliance "Domain 12: Guidance for Identity & Access Management V2.1" April 2010
[7] White Paper on Identity in the Cloud Use the cloud without compromising enterprise security
[8] William C. Cheng_, Cheng-Fu Chou,bLeana Golubchi "Performance of Batch-based Digital Signatures" Appeared in Proceedings of IEEE MASCOTS 2002
[9] Nuttapong Attrapadung, Benot Libert, and Elie de Panaeu " Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts " Belgian National Fund for Scientific Research 2012
[10] Vipul Goyal, Omkant Pandey"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data " ACM 2006
[11] Kelly D. LEWIS, James E. LEWIS "Web Single Sign-On Authentication using SAML" IJCSI International Journal of Computer Science Issues, Vol. 2, 2009
[12] Thomas Grob, "Security Analysis of the SAML Single Sign-on Browser/Artifact Profile " IBM Zurich Research Laboratory.
[13] Single Sign-On Implementation Guide by SalesForce.com
[14] Alessandro Armando, Roberto Carbone , Luca Compagna "Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps " ACM 2008
[15] K Vahini, V Prasad ,U V Chandra Sekhar " Defend Data using ELGAMAL Digital Signature
Data Decryption Algorithm." International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5062-5067
[16] Venkateswara Rao Pallipamu, Thammi Reddy K, Suresh Varma P "Design of RSA Digital Signature Scheme Using ANovel Cryptographic Hash Algorithm" International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 6, June 2014