www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 9 Oct 2015,Page No. 14544-14550

A Strong Token Authentication And Cryptography Based Application And Data Access For Cloud Users.

Ali Asgar Hussain[1], Reetu Gupta[2]

[1]CSE,Sushila Devi Bansal College of Technology Indore ,Rgpv Bhopal,India-alee.asgar@gmail.com

[2]CSE,Sushila Devi Bansal College of Technology Indore ,Rgpv Bhopal,India-reetugupta2000@gmail.com

Abstract— Cloud computing is the latest trend in comuting by which various services, 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.

I. INTRODUCTION

Cloud in a service which perform on real time network and give a computation, unite more than two computing resource in type of bunch in another word cloud additionally called Distributed Computing. Most cloud three sort service give us, Peas and Saas Together with virtualization, clouds could be characterized as computers that are networked anywhere on the planet with the availability of paying the used clouds in a pay-per-use way, implying that simply the resources that are, used will be paid.

Cloud must have an arranged way to deal with giving the security control to users alongside application access and other vital factors. The organization drives towards deploying the server, which offers security usefulness. Alongside the security factors performance factors ought to likewise be kept in a min, on the grounds that if the security control is heavier than alternate applications and their usability may get influenced.

In this way a balance must be distraught in the middle of the security approach many-sided quality and the sort of resources they are involving and how they influence the application response. There are a few focuses which keep in concern dependably while developing cloud security components. They are:

- Effective resource management with virtualization support
- Robust service delivery with reliable communications
- Automotive process with lessened fault and performance burdensome and load handling
- Making security simply over the value of information
- SOA based security service architecture.

- **Cloud Security Challenges**

Cloud computing benefits involve major changes for organizations. Majorly to gain the trust to deploy crucial data and complex business applications to a third party's infrastructure. Certainly it makes security a major issue as organizations need to look at cloud services and providers. Main principles for Securing the Cloud computing are Secure Identity, Information, Infrastructure as shown in fig below..

Public cloud computing needs to adopt a strong security model that maintains scalable and multi-tenant supports with the need for trust and assurance. As enterprise organizations deploy their computing systems with their identities, business information and infrastructure to the cloud, some level of controls, they must be willing to give up to the providers.

Cloud users normally have no control over the Cloud resources used and there is an innate danger of data exposure to third parties on the Cloud or the Cloud supplier itself.Some policies are:

- Whether there exists an Information security policy, which is endorsed by the management, published and conveyed as fitting to all workers.
- Whether it expresses the management responsibility and set out the organizational methodology to overseeing data security.

- Whether the Security policy has a manager, who is in charge of its maintenance and survey as indicated by a characterized audit process. Whether the procedure guarantees that a survey happens because of any progressions influencing the premise of the first evaluation,*Example*: noteworthy security episodes, new vulnerabilities or progressions to organizational or technical infrastructure.

Some of those recognized zones where the security elaborations can be made are:

(i) Encapsulated information security standards alongside service appropriateness must be connected over the computing servers

(ii) User and organization characterized policies ought to take a control over the conventional security instrument utilized for confidentiality and integrity.

(iii) User's possessions and its personal information must be made secure even against the service providers moreover.

(iv) Security must be of light weight so that extra load can't be put on the resources configured.

Since the CSP is the authority that controls the data things put away in the system, the CSP can investigate data things put away in distributed storage without the data proprietor's consent. In this way to make the system more reliable client needs to make some security trusted deals with its data. The genuine deployment of distributed computing services is not reliable as they claim in light of the fact that the current security model doesn't work after migration of services to clouds.

This work points towards cloud security suggesting so as to make the security more effective a novel model which gives security controls over as a service. Essentially the controls incorporate a portion of the cryptographic algorithms, single sign on (SSO) and digital signature, all under a single service. It serves as a hybrid mechanism which guarantees the confidentiality of the user's data and privacy in accessing its configured applications. The cryptographic standards serve multiple algorithms simultaneously.

II. BAGROUND

Cloud seciruty have several stratagies already exixting, below we are trying to show some of the approches used by CSPs

1) Attribute Based Encryption

Attribute-based encryption proposed that one's identity can be seen as a mix of a few attributes communicating the characteristics of the user as access policy by utilizing Boolean expressions, for example, AND, OR, or NOT. Later studies are extensively classified into key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE) studies. In KP-ABE, the access policy is connected with keys relating to attributes inferring that an encryptor is not approved to give access to the scrambled content aside from of graphic attributes for the data by the encryptor's decision.

Then again, CP-ABE is complementary to KP-ABE by empowering encryptor to indicate access policy joined with the ciphertext. Both plans permit secure one-to-many communications, for example, targeted broadcasts for a specific gathering and individual user as indicated by their attributes, which are unmistakable from the customary cryptographic approaches obliging the explicit identity of the planned receivers.

2) Secure Exchanges using SAML and SSO

SAML is Security Assertion Markup Language. The reason for the SAML standard is to depict and exchange security information through SAML attestations between online business domains that trust one another. This standard has strict syntax and rules for overseeing SAML attestations. The SAML is the core standard utilized for designing cloud authentication service in this project and the design is based on cloud authentication frameworks depicted in the accompanying referenced papers. The SSO is single sign on mechanism which takes profits by the use of the SAML standard for serving the answer for exchange security information independent of any specific platform, space and protocol.

Any user or client application, before accessing any resource gave by the application service, is initially needed to be authenticated. The SSO can be started in system and the authentication process contains multiple interactions between distinctive system entities. The end-user first associate with the application service provider through request resource message keeping in mind the end goal to request access to a protected resource or service. The request message is intercepted by the PEP server.

In the event that the end-user does not have a substantial local session for that specific application service, PEP gives back an authentication request message, for example, SAML Authentication Request and directs the end-user to the SSO service provider. The user join with the strong authentication server through 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 come back to the user through the authentication server as per the HTTP Post message protocol. All the more specifically, if the user has been effectively authenticated, then PEP makes a local legitimate 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 the majority of the documents are electronic due to the religion usage of the computer and its applications like email, e-banking, e-voting, etc. Along these lines the message, data, documents or some other materials in electronic format must be signed electronically. This signature that is done electronically is known as Digital Signature. The methodology can provide different services like message authentication, message integrity and non repudiation. Non-repudiation can be provided utilizing a trusted party. A digital signature does not provide privacy. On the off chance that 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 legitimate 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 imperative to detect forgery or tampering. The different 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.

III. LITERATURE SURVEY

In the most recent few years different approaches had been developed for enhancing the current security circumstances in cloud computing. Point is towards making the data exchanges and transition more secure against the attackers.Subsequently, this work basically deals with security as a service utilizing 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 taking into account non-monotonic access structures (i.e., that may contain negated attributes) and with constant ciphertext size [9]. Towards achieving this objective the paper demonstrate 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 specific instantiation of general monotonic construction, gives rise to the first genuinely 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. Then again, 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). A (Key-Policy) Attribute Based Encryption scheme comprises of four algorithms. To start with is setup which is used as a randomized calculation that takes no input other than the implicit security parameter. It yields the general population parameters PK and a master key MK. Second is encryption that takes as input a message m, a set of attributes γ, and people in general parameters PK. It yields the ciphertext E.

The paper deals with giving security as a service to cloud application utilizing SAML [11]. The implementation of Security Assertion Markup Language (SAML) and its capabilities to provide secure single sign-on (SSO) answers for externally hosted applications. On the off chance that the user accesses the external webpage without going through the internal federated identity manager to start with, the service provider should 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, yet without a SAML assertion.

The service provider redirects the user back to the identity provider's federation webpage with a SAML request, and alternatively 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 cooperate to provide SSO. Some of the related web browser profiles for implementing SSO are singe logout profile, artifacts resolution profile, name identifier management profile

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 rather 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 obscure.

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.

Presently 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 at

IV. 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.

V. 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

VI. PROPOSED SYSTEM

Design Architecture:

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.

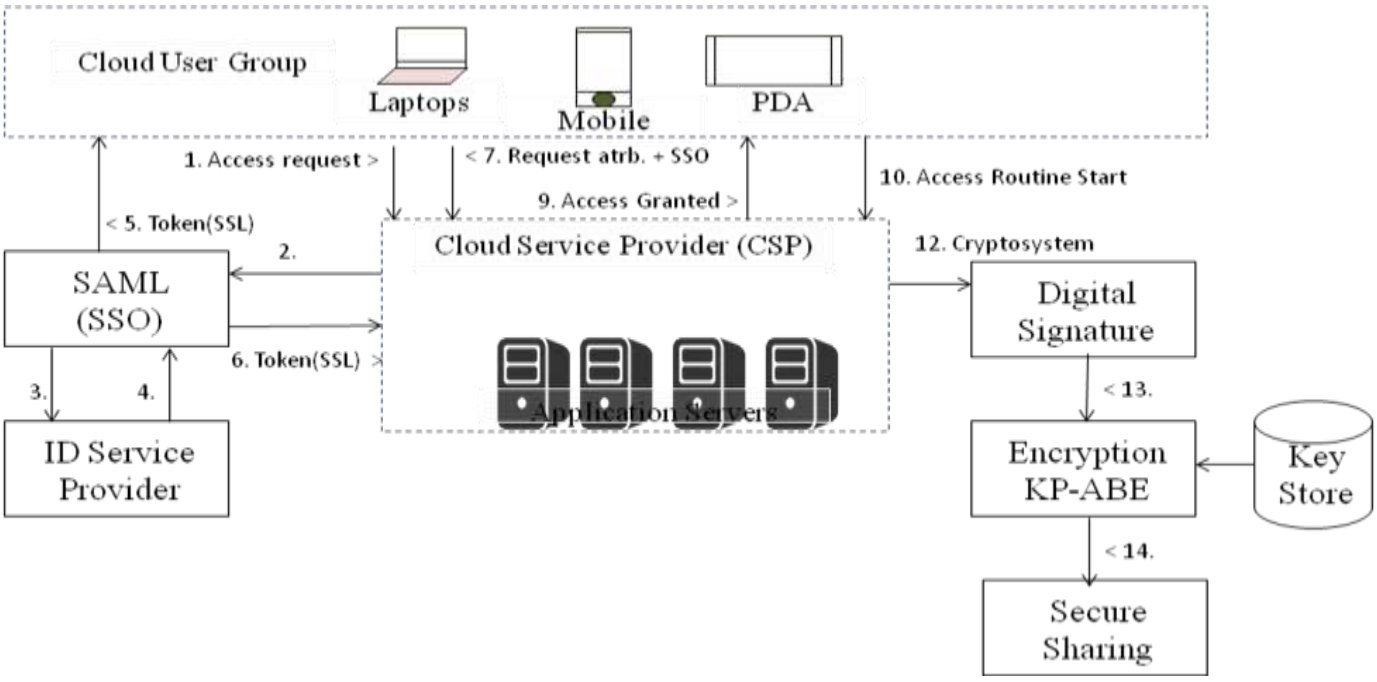
All it needs is to reduce the security control, heavy loaded operation to some simple control with restricted constrained specifications. The proposed system utilizes the system, cookies and other information for reducing the user credential remembrance loads. Also the other strategies are here incorporated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

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 user's identity and checks the users request zone.

DOI: 10.18535/ijecs/v4i10.02



Presently 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. Presently the users request again sends with this token to the application server and the server verifies both the token. In the event that 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.

VII. 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.

VIII. CONCLUSION

Cloud is in the market every in industries as well as individuals. along with the cloud's features, 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