Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics

B.Prasanalakshmi
Assistant Professor
Department of CSE
Thirumalai Engineering College
Kanchipuram.

A.Kannammal
Associate Professor
Department of CA
Coimbatore Institute of Technology
Coimbatore

ABSTRACT

Cloud computing is introducing many huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always the focus of numerous potential cloud customers, and a big barrier for its widespread applications.Companies have increasingly turned to application service providers (ASPs) or Software as a Service (SaaS) vendors to offer specialized web-based services that will cut costs and provide specific and focused applications to users. The complexity of designing, installing, configuring, deploying, and supporting the system with internal resources can be eliminated with this type of methodology, providing great benefit to organizations. However, these models can present an authentication problem for corporations with a large number of external service providers. This paper describes the implementation of Security Assertion Markup Language (SAML) and its capabilities to provide secure single sign-on (SSO) solutions for externally hosted applications, including security measures for federated identity management systems using multifactor authentication ,which also includes Biometric identification.

General Terms

Computer networks and security.

Keywords

SAML, SSO, Multifactor, Cloud security, Biometrics, Federated identity management.

1. INTRODUCTION

Cloud computing is a style of computing in which dynamically *scalable* and often *virtualized* resources are provided *as a service* over the *Internet*. According to NIST," Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].Cloud computing provides on demand services for network infrastructure, platforms, and applications based on an off premise, pay-as-you-go operational model.

The concept generally incorporates a combination of the following elements, which includes the various services as[2]

• *Infrastructure-as-a-Service* (IaaS), eg. Amazon's EC2

• *Platform-as-a-Service* (PaaS), eg. Google applications and Force.com

• *Software-as-a-Service* (SaaS), eg. Salesforce.com

• Other recent technologies that rely on the Internet to satisfy users' computing needs

1.1 Deployment models

Deployment models characterizes the management of computational resources, as well as to differentiate the classes of consumers. The deployment models are broadly classified as[3]:

- A public cloud , in which the infrastructure and computational resources that it comprises are made available to the general public over the Internet. It is owned and operated by a cloud provider delivering cloud services to consumers and, by definition, is external to the consumers' organizations.
- A private cloud, in which the computing environment is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it. A private cloud has the potential to give the organization greater control over the infrastructure, computational resources, and on cloud consumers than a public cloud can do.
- A community cloud falls between public and private clouds with respect to the target set of consumers. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.
- Hybrid clouds are more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.

1.2 SAML and SSO

SAML is a set of specifications that encompasses the XML-format for security tokens containing assertions to pass information about a user , protocols and profiles to implement authentication and authorization scenarios. Key actors of SAML 2.0 are Identity Providers (IdP), Service Providers (SP), Discovery Services, Metadata services etc. As more and more mission-critical applications migrate beyond

the firewall and with the implication in the raise of usage of SaaS, Web Services and cloud-based applications ,their access and identity enforcement processes aren't suitable for Web 2.0. To minimize the impact on users, many organizations are trying to extend their legacy single sign-on (SSO) to the cloud, which also is found less effective beyond the firewall. In order to overcome such a proliferation of non-interoperable proprietary technologies, standard bodies have proposed to combine underlying SSO and identity federation standards.

The SAML (Security Assertion Markup Language) has emerged as the go-to SSO protocol for B2B applications.[Kelly D. LEWIS, James E. LEWIS, Web Single Sign-On Authentication using SAML, IJCSI- International Journal of Computer Science Issues, Vol. 2, pp.41-48,2009.] SAML is deployed in SSO connections, large enterprises, government agencies and service providers as their standard protocol for communicating identities across the Internet. SAML is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).

1.3 Identity and Access Management

Preventing unauthorized access to information resources in the cloud is a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove to be difficult. Employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, leads to complication that can become unworkable over time. Identity federation, popularized with the introduction of service oriented architectures, is one solution. Identity federation allows the organization and cloud provider to trust and share digital identities and attributes across both domains, and to provide a means for single sign-on. For federation to succeed, identity and access management transactions must be interpreted carefully and unambiguously and protected against attacks. Identity federation can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard or the OpenID standard.

- **Authentication.** Authentication is the process of establishing confidence in user identities. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved . A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information between cooperating domains.

For example, a SAML transaction can convey assertions that a user has been authenticated by an identity provider and also include information about the user's privileges. Upon receipt of the transaction, the service provider then uses the information to grant the user an appropriate level of access, once the identity and credentials supplied for the user are successfully verified. SAML request and response messages are typically mapped over SOAP, which relies on the eXtensible Markup Language (XML) for its format. SOAP messages are digitally signed. In a public cloud, for instance, once a user has established a public key certificate with the service, the private key can be used to sign SOAP requests. SOAP message security validation is complicated and must be carried out carefully to prevent attacks. XML wrapping attacks have been successfully demonstrated against a public IaaS cloud. XML wrapping involves manipulation of SOAP messages. A new element is introduced into the SOAP Security header; the original message body is then moved under the wrapper and replaced by a duplicate body containing an operation defined by the attacker . The original body can still be referenced and its signature verified, but the operation in the replacement body is executed instead.

- **Access Control.** SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud consumer privileges and maintain control over access to resources is also needed. As part of identity management, standards like the eXtensible Access Control Markup Language (XACML) can be used by a cloud provider to control access to cloud resources, in lieu of some proprietary means. The XACML standard defines an XML-based language for stating policy and forming access control decisions. XACML focuses on the mechanism for arriving at authorization decisions, which complements SAML's focus on the means for transferring authentication and authorization decisions between cooperating entities. XACML is capable of controlling the proprietary service interfaces of most providers, and some cloud providers already have it in place. The basic XACML usage model assumes that when a resource access is attempted, a Policy Enforcement Point (PEP), responsible for protecting access to resources, sends a request containing a description of the attempted access to a Policy Decision Point (PDP) for evaluation against available policies and attributes. The PDP evaluates this request and returns an authorization decision for the PEP to enforce. XACML does not define protocols or transport mechanisms or specify how user credentials are validated. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, including unauthorized disclosure, replay, deletion and modification attacks, unless sufficient safeguards are in place to protect transactions .

1.4 Challenges and solutions

Cloud computing services are still in a developmental stage best practices on cloud computing are evolving, and security is still a major concern. one of the challenges is how to integrate all cloud computing resources with enterprise resources in order to deliver a unified service to employees and customers anywhere and anytime while still maintaining a secure environment. With the developing technology there exists some challenges like Business challenge, SSO challenge, Security challenge and Remote access challenge.

The solution to these challenges comprises the following three components.

- Identity federation
- Remote access
- Security

1.4.1 Identity Federation

Identity federation has two meanings:

• The virtual reunion or assembled identity of a person's user information , which is stored across multiple, distinct *identity management* systems. Typically, the user's name, being a common token, joins the data.

• A user's *authentication* process which is integrated across multiple IT systems or even organizations.

For example, a traveler could be a flight passenger as well as a hotel guest. If the airline and the hotel use a federated identity management system, this means that they have a contracted mutual trust in each other's user authentication. Initially, the traveler can self-identify as a customer for booking the flight and then this identity can be transferred to hotel reservations.

The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, without requiring redundant user administration. The goal requires that all participating systems use the same protocol to be interoperable. To integrate cloud service into an enterprise's remote access portal with SSO, an identity federation open standard such as SAML is recommended by NIST.

The SAML protocol decouples both the SAML identity provider and the SAML service provider. This enables the enterprise to have a centralized identity provider that can support many other service providers in a distributed fashion. The SAML identity provider focuses on identity management, access policy management, and security token generation, while SAML service providers receive the remote security token, retrieve credential data, and reinforce user access policies locally. With the SAML protocol, the enterprise can provide service to other enterprises. Identity federation supports cross domain single sign-on (CD SSO) and interchanges access control information with a wide range of partners, reflecting business trust relationships. The SAML protocol is interoperable. Because cloud service providers implement different identity federation protocols or different versions of the same protocol, the enterprise cloud can leverage Security Token Service (STS) to interoperate between these different SSO practices.

1.4.2 Remote Access

Remote access is another part of the total solution. Remote access allows employees to work across geographies in real time, thereby reducing travel costs and energy consumption. In some enterprise environments, remote access is required to provide portals, collaboration, and messaging in one place, securely bridging the end user to the enterprise. In other enterprise environments, the remote access solution enables users to access the subscribed services offered by third-party companies.

Remote access includes application portals aggregating Web applications and other emerging technologies such as Virtual Desktop Infrastructure (VDI), and it supports HTTP-based and non-HTTP based applications such as Telnet, SSH, and Remote Desktop Protocol (RDP). Because remote access delivers open, high performance, secure access to customers, suppliers, and partners, it can support different consumer technologies and help to ensure a good end user experience. Besides supporting a Web browser running on workstations and personal computers, remote access supports smart PDAs, airport kiosks, and other frequently used access devices.

1.4.3 Security

Security is the most important part of the total solution and requires end-to-end security practices. From an identity and access perspective, the enterprise can provide an identity authentication service for its employees regardless of where the service resides, either internally or in the cloud computing environment. The company owns and manages the employee's identity repository and does not share identities with any other entity. The company provides a central point in managing an employee's identity, including password preset/reset/changes.

The company enhances identity and security protection by protecting an employee's confidential and credential information, because the identity federation approach allows the enterprise to manage its employee's access control policy—determining where SSO occurs, asserting trust appropriately, and sharing acceptable attributes between the identity provider and the service provider. From an end user's perspective, remote access can reinforce security by using advanced authentication mechanisms such as strong authentication or multifactor authentication to prevent identity theft over the Internet, or to leverage the Host Checker to verify allowed hardware, thereby ensuring a safe environment. In summary, cloud computing as it pertains to end users is about enabling remote access among existing data centers and the combination of any cloud environment (either private cloud or public cloud). With SAML, the remote access solution improves the user's experience in securely accessing content between enterprise and hybrid cloud environments. SAML simplifies Identity Access Management and also provides interoperable IAM functionality in hybrid cloud environments.

2. SAML FOR SSO BASED MULTI-FACTOR AUTHENTICATION

Security Assertion Markup Language (SAML) provides a secure, XML based solution for exchanging user security information between an identity provider (our organization) and a service provider (ASPs or SaaSs). The SAML standard defines rules and syntax for the data exchange, yet is flexible and can allow for custom data to be transmitted to the external service provider. There are three roles involved in a SAML transaction – an asserting party, a relying party, and a subject. The asserting party (identity provider) is the system in authority that provides the user information. The relying party (service provider) is the system that trusts the asserting party's information, and uses the data to provide an application to the user. The user and their identity involved in the transaction are known as the subject.

The components that make up the SAML standard are assertions, protocols, bindings and profiles. Each layer of the standard can be customized, allowing specific business cases to be addressed per company. The transaction from the asserting party to the relying party is called a SAML assertion. The relying party assumes that all data contained in the assertion from the asserting party is valid. The structure of the SAML assertion is defined by the XML schema and contains header information, the subject and statements about the subject in the form of attributes and conditions. The assertion can also contain authorization statements defining what the user is permitted to do inside the web application. The SAML standard defines request and response protocols used to communicate the assertions between the service provider (relying party) and the identity provider (asserting party).

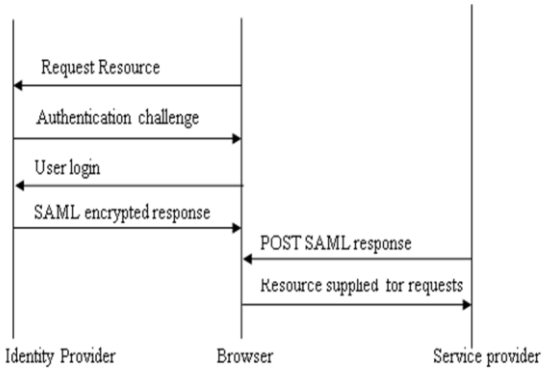

Figure 1 Identity Provider Initiated SAML Assertion Flowchart

Two profiles will be briefly discussed in more detail, the artifact resolution profile and web browser SSO profile. The artifact resolution profile can be used if the business case requires highly sensitive data to pass between the identity provider and service provider, or if the two partners want to utilize an existing secure connection between the two companies. This profile allows for a small value, called an artifact to be passed between the browser and the service provider by one of the HTTP bindings. After the service provider receives the artifact, it transmits the artifact and the request/response messages out of band from the browser back to the identity provider. Most likely the messages are transmitted over a SSL VPN connection between the two companies. This provides security for the message, plus eliminates the need for the assertions to be signed or encrypted which could potentially reduce overhead. When the identify provider receives the artifact, it looks up the value in its database and processes the request. After all out of band messages are transmitted between the identity provider and service provider, the service provider presents the information directly to the browser.

The web browser SSO profile may be initiated by the identify provider or the service provider. If initiated by the identity provider, the assertion is either signed, encrypted, or both. In the web browser SSO profile, all of the assertion information is sent at once to the service provider using any of the HTTP bindings and protocols. The service provider decrypts if necessary and checks for message integrity against the signature. Next, it parses the SAML XML statements and gathers any attributes that were passed, and then performs SSO using the Assertion Consumer Service. The diagram in Figure 1 shows the identity provider initiated SAML assertion. 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. After receiving the request from the service provider, the identity provider processes the SAML request as if it came internally. This use case is important since it allows users to be able to bookmark external sites directly, but still provides SAML SSO capabilities with browser redirects. Figure 2 demonstrates this service provider initiated use case.

The most popular business use case for SAML federation is the web browser SSO profile, used in conjunction with the HTTP POST binding and authentication request protocol. The implementation and framework section will discuss this specific use case and the security needed to protect data integrity.

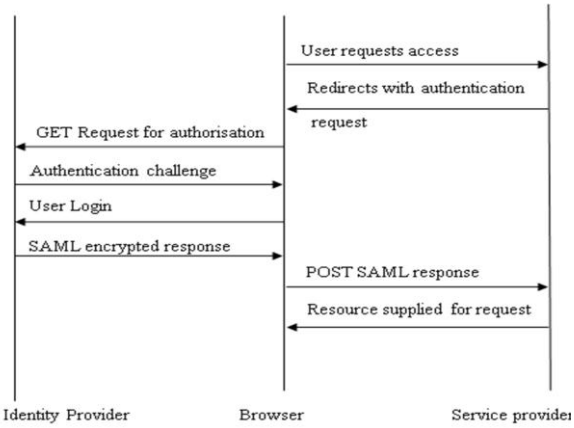

Figure 2 Service Provider Initiated SAML Assertion Flowchart

3. SECURE CREDENTIAL FEDERATION FOR A HYBRID CLOUD ENVIRONMENT

The efficiency of enterprise data center is maximised by deploying enterprise applications into private cloud. When the private cloud reaches maximum capacity, the additional instance of the enterprise applications deployed in public cloud are federated to withstand the increasing load. Such federations are preferred by enterprises during the peak usage period, in order to scale up the existing capacity of the private cloud as shown in figure 3. Federation of the private cloud with the public cloud is also done to reduce the costs, since enterprises pay only for the capacity they need. This federation faces the risk of exposing their user credentials. In order to avoid the theft of identities, enterprise users must be authenticated within the enterprise perimeter and their private cloud identities are mapped to different identities provisioned to the public cloud instances. Thus, during usage peaks, when the private cloud reaches capacity, application instances must be started in a public cloud. The enterprise needs a solution to authenticate and authorize the user to access the public cloud instance while protecting the enterprise identity. Security Gateway [4] is a service gateway that can enforce security policies across security domains, provide authentication and authorization to a local credential directory, Log authentication failures for auditing and proxy messages between two endpoints. A Security Gateway is placed on the enterprise perimeter to proxy public cloud instances hosted in the Service provider. When a user attempts to connect to a public cloud instance, the Security Gateway authenticates the user's credentials against the enterprise identity store, and on successful authentication, maps the enterprise identity to a public cloud identity, never exposing the protected identity or credentials outside the enterprise perimeter. Then, Security Gateway starts the cloud instance and signs the user in with his mapped public cloud identity.

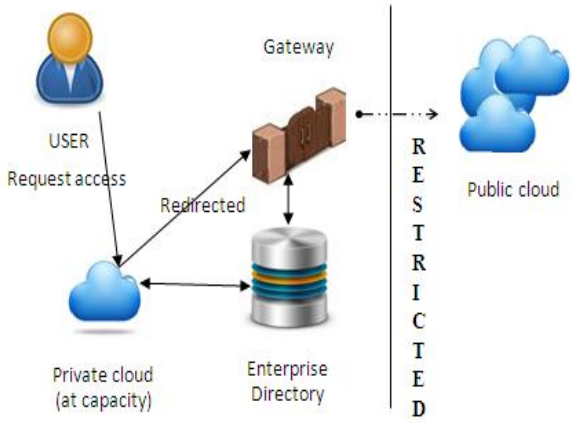

Figure 3 . Hybrid cloud Environment

3.1 Configuring Cloud Federation

To create the hybrid cloud environment, enterprise data center operators and application architects must select a platform and create an application image to deploy on the platform. The data center operators then deploy Security Gateway in the enterprise DMZ(Demilitarized zone) and set it up as a proxy for the public cloud instances. The proxy service determines whether to start and connect to application instances in the private cloud or in the public cloud. For the public cloud instances, the proxy service also orchestrates the authentication and authorization process before starting an instance in the public cloud. This eliminates the cost of an unnecessary instance on the CPU that an authentication or authorization failure would cause.

Administrators would follow these steps to configure Security Gateway for the authentication and authorization process:

1. *Configure Security Gateway to connect to the enterprise identity directory.*

The settings depend on whether the directory is an LDAP or Active Directory server. Essentially, the settings needed are the server address and port, a trusted user account (like an administrator), and the part of the directory where the user entries are based.

2. *Configure an identity service in Security gateway*

This is done to connect to the application instance on the public cloud. This consists of configuring the information needed to build the SAML assertion sent to the public cloud instance to sign in the user with his public cloud identity.

3. *Configure any authorization policies that apply to the cloud application*:

a. Configure the built-in policy decision point with the applicable XACML policies based on user ID, group ID, or role within the enterprise.

b. In the identity service, enable an additional policy enforcement step that extracts the necessary subject and resource information needed by the decision point.

4. *Activate the identity service*.

3.2 A Detailed Look at the Federation Process

During application deployment, the application architects and data center operators must fix up a size for the enterprise private cloud. Then the data center operators deploy Security Gateway at the enterprise perimeter and configure it to act as a proxy to the public cloud running on the platform of the service provider. With Security gateway linked to the enterprise directory and the identity service configured and running, the application is ready for users to sign on. When a user is unable to sign on to the private cloud application, since the cloud has reached capacity, Security gateway begins the authentication and authorization process for the public cloud instance. If the user has already signed on to the enterprise through an enterprise SSO solution, the Security Gateway identity service knows the user has been authenticated and skips asking the user for his credentials. In other cases, the identity service presents the user a sign-on page, where the user's credentials must be presented. After receiving the credentials, Security Gateways verifies these credentials against the enterprise directory.

If an authentication failure occurs, Security gateways log an authentication failure event to the audit log for later investigation by the security administrators. Because the failures occur within the enterprise authentication domain, the log contains authentication failure events for both the private and public cloud instances. Therefore, authentication failures for the private and public clouds are integrated. When a user is both authenticated and authorized, Security Gateway finishes the public cloud access by starting the public cloud application instance and logging in the user. The user's enterprise identity is mapped to the user's public cloud identity, and the user begins his work with the application.

3.3 Multi-factor Authentication for Ensuring Client Credentials Are Valid

Enterprises are expanding their use of public clouds to host applications. In some cases, the public cloud is used to scale up capacity for peak usage periods. Increasingly, however, enterprise applications are completely hosted in the public cloud. This trend is gaining momentum because application deployment to public clouds creates significant cost savings by allowing enterprises to pay for only the capacity they need when they need it. However, moving to public clouds creates new security issues, namely protecting enterprise data from unauthorized access. Enterprise users must be authenticated and authorized to use the cloud-based application. In order to protect enterprise identities and enable a strong authentication method, an enterprise-based gateway integrated with a Multi-factor authentication solution is needed. Multi-factor authentication is gaining popularity as a way to increase the security of user authentication as shown in figure 4.

In this use case, Security Gateway is placed at the enterprise perimeter to transparently proxy application client sign-on and service requests to application instances on the public cloud. During sign-on, Security Gateway acts as an identity provider (IdP) and initiates the sign-on authentication process. As the client presents his credentials, it also presents a nonce that is signed with the private key as the second factor of the strong authentication process. The credentials are authenticated against the enterprise credential directory (IdM) and the nonce signature verified, and the multimodal biometric data stored in the space specified token is verified with the BioBex server and on successful authentication, Security gateway presents an SAML token to the cloud application. The enterprise identities and credentials are not exposed beyond the enterprise perimeter, and the enterprise benefits from the stronger authentication of its users. To support compliance needs, the audit log feature of Security Gateway captures the authentication and authorization events into an audit log. Administrators can filter the log for such events to distinguish the kinds of rogue access attempts being made on the public cloud application.

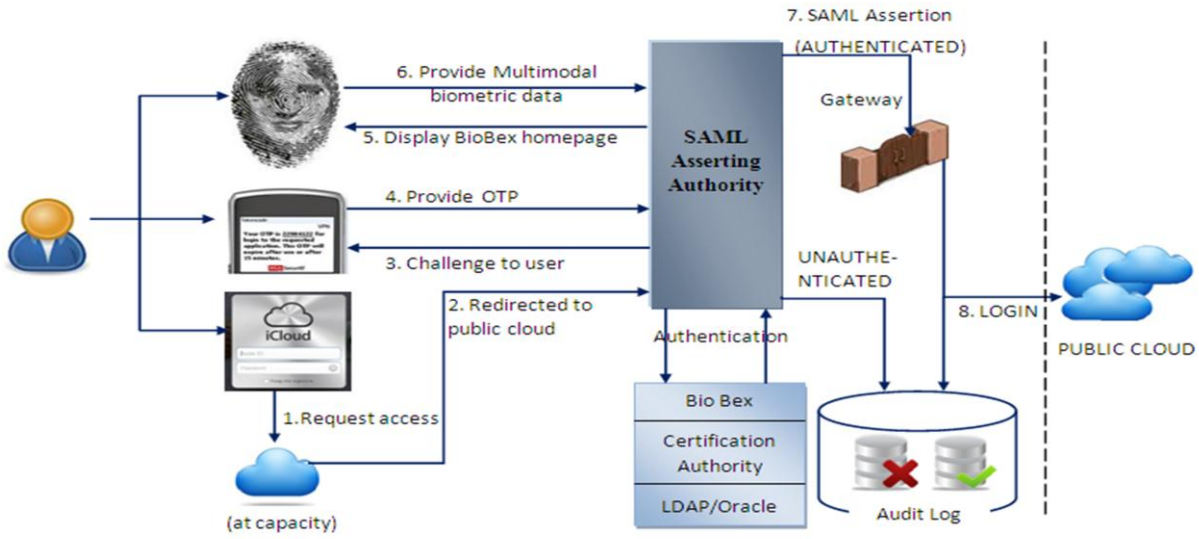

Figure 4 : The proposed Multifactor authentication system

In this use case, Security Gateway is placed at the enterprise perimeter to transparently proxy application client sign-on and service requests to application instances on the public cloud. During sign-on, Security Gateway acts as an identity provider (IdP) and initiates the sign-on authentication process. As the client presents his credentials, it also presents a nonce that is signed with the private key as the second factor of the strong authentication process. The credentials are authenticated against the enterprise credential directory (IdM) and the nonce signature verified, and the multimodal biometric data stored in the space specified token is verified with the BioBex server and on successful authentication, Security gateway presents an SAML token to the cloud application. The enterprise identities and credentials are not exposed beyond the enterprise perimeter, and the enterprise benefits from the stronger authentication of its users. To support compliance needs, the audit log feature of Security Gateway captures the authentication and authorization events into an audit log. Administrators can filter the log for such events to distinguish the kinds of rogue access attempts being made on the public cloud application.

3.3.1 Configuring Multi-factor Authentication

When the enterprise deploys an application to a public cloud platform, the enterprise security architect enables sign-on to the cloud application through Security gateway deployed in the enterprise DMZ. The security architect configures the Security Gateway identity service to collect the user's credentials and connect to the enterprise identity directory to authenticate those credentials. In addition, the security architect configures the identity service to enable
signing using the private-public pairing on his client system. This second factor ensures that the user is signing on from a trusted device and thereby strengthens the protection against rogue access to the cloud application. And, administrators would follow these steps to configure the enterprise for the Multi-factor authentication method described previously:

1. Configure Security Gateway to connect to the enterprise identity directory.

The settings depend on whether the directory is an LDAP or Active Directory server. Essentially, the settings needed are the server address and port, a trusted user account (like an administrator), and the part of the directory where the user entries are based.

2. Configure an identity service in Security gateway to connect to the cloud application:

a. Enable signing using the TPM during user authentication. The administrator needs to collect the TPM public keys from user systems to put in the key store.

b. Configure the information needed to build the SAML assertion given to the cloud application to sign on a user.

c. Configure the user provisioning process.

3. Configure any authorization policies that apply to the cloud application:

a. Configure the built-in policy decision point with the applicable XACML policies based on user ID, group ID, or role within the enterprise.

b. In the identity service, enable an additional policy enforcement step that extracts the necessary subject and resource information needed by the decision point.

4. Activate the identity service.

When the identity service is activated, Security Gateway performs the bulk provisioning process, if configured, and users can sign on to the cloud application.

3.3.2 A Detailed Look at the Authentication Process

Once the security architect completes the Multi-factor authentication configuration and activates the identity service, Security gateway becomes the enterprise proxy to the publicly deployed cloud application. Users work with the cloud application on trusted systems deployed within the enterprise. When the user accesses the cloud application and begins to sign on, Security Gateway transparently intercepts the user access to the cloud to begin the Multi-factor authentication process . Security Gateway initiates the sign on by challenging the user to present his credentials. The user is presented with a sign-on page asking for his user ID and password .When the user supplies his ID and password, a

script in the sign-on page triggers the client system to sign a nonce using RSA on the private-public key pair. This signing attests that the user is signing on from a trusted system. After Security Gateway has gathered the credentials and signed nonce, it authenticates the user and the trusted system in the enterprise directory. Security Gateway queries the directory, which can be either LDAP or Active Directory, for the user identity information. On a successful look up, the user's credentials are checked, and the nonce signature is verified with the stored public keys. At this point, if the user is not authenticated as a trusted user or if he is a trusted user but not on a trusted system, the authentication fails. The user is not signed on to the cloud application, and the enterprise is protected from a rogue access to the application and its data. Security gateway logs the details of the failed authentication in the auditing log, creating an audit trail for security administrators to investigate later. On a successful user and system authentication, the Biobex server displays its input page to gather multimodal biometric information as stored in the space specified token[5] and on final authentication, Security Gateway then determines all authorization policies that apply to the user when accessing the cloud application. The user's ID, group, and role within the enterprise are considered when evaluating the applicable policies. This policy evaluation results in a decision to permit or deny access to the application and its data. In this way, Security Gateway acts a policy enforcement point (PEP) and policy decision point (PDP). Now that the user has been authenticated and the authorization decision permits access, the user is signed on to the cloud application. The authentication and authorization process has been conducted securely within the enterprise, out of view of any eavesdroppers between the enterprise perimeter and the public cloud. For further security, Security Gateway maps the user's identity to a public identity, thereby protecting the security of the user's enterprise identity and password. After sign on, Security Gateway continues to act as proxy for the cloud application. This allows for continued auditing, event monitoring and logging, and potentially additional authorization decisions for access to modules and functions of the cloud application. The proposed system is as depicted in figure 4.

4. CONCLUSION

In this paper, multimodal biometrics has been involved as another means of authentication. The multimodal biometric system provided here is itself a secure system involving three biometric traits, the face, fingerprint and the palm vein. The key generated from palm vein is used to encrypt the fingerpirnt image which is then embedded into the face biometric as presented in the previous works. This security system may also be extended with other biometric traits.

5. REFERENCES

[1] Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft).NIST. 2011. http://www.productionscale.com/home/2011/8/7/the-nist-definition-of-cloud-computingdraft.html#axz z1X0xKZRuf.

[2] S. Subashini , V.Kavitha ,A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications ,Vol. 34,pp. 1–11,2011.

[3] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In: ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009. p. 50–5.

[4] http://www.intel.com/content/dam/doc/reference-architecture/cloud-computing-cloud-gateway-security-intel-soa-expressway-architecture.pdf

[5] B. Prasanalakshmi, A. Kannammal, B. Gomathi, K. Deepa, R. Sridevi, Biometric Cryptosystem Involving Two Traits And Palm Vein As Key, Procedia Engineering, Vol. 30, PP. 303-310, 2012.