Improving Privacy and Trust in Federated Identity Using SAML with Hash Based Encryption Algorithm

Jissy Ann George  
College of Administrative and Financial Services  
AMA International University  
Kingdom of Bahrain  
jissy.george@amaiu.edu.bh

S. Veni  
Department of Computer Science  
Karpagam University  
Coimbatore, Tamil Nadu  
venikarthik04@gmail.com

Safeullah Soomroo  
College of Computer Studies  
AMA International University  
Kingdom of Bahrain  
s.soomro@amaiu.edu.bh

Abstract - Cloud computing is an upcoming technology that has been designed for commercial needs. One of the major issues in cloud computing is the difficulty to manage federated identities and the trust between the user and the service providers. This paper focuses on how security can be provided between the user and the service provider and how the user information can be authenticated. For the purpose of providing privacy and authentication, Security Assertion Markup Language (SAML) based Single Sign-On is used. Security is provided by using Hash based Encryption algorithm (HBE). HBE algorithm works with the help of Key Exchange Protocol which contains poly hash function. In the algorithm, Identity providers maintain user directory and authenticates user information; service provider provides the service to users. The user has to register their details with the identity provider prior to this. During this stage, Hash based Encryption algorithm is used to provide secure communication between the identity provider and the user. In this paper we suggest that higher security can be given to user login by using an additional cryptographic technique, i.e. Hash based Encryption algorithm with the help of the Key Exchange Protocol.

Index Terms - Cloud security, identity provider, Security Assertion Markup Language, Single sign-on, Hash Based Encryption.

I. INTRODUCTION

Cloud computing provides different kinds of services to users with different charges based on the particular usage of services. In cloud, the services are cost effective and those services [1] are easy to use. But the main issues are access control, security, maintaining and managing the user identities. When providing service to the user, their identities are needed to manage high security, and for this purpose, identity as a service (IDaaS) is used. IDaaS is very important in all services including software, platform, and infrastructure service in both public and private clouds. Therefore, identity management system is very important because in the enterprise environment, the application data may be interrupted by a third party. At the same time, issues such as consistency in authentication, authorization and auditing are handled by identity management using the identity layer which was in IDaaS.

IDaaS manages all user information using different identity management models like isolated, central, centric and federated. Providing security to user identities and managing trust between the user and the service provider are the main issues. In the proposed system, the identities are managed by using Security Assertion Markup Language with Single Sign-On [2] and encryption algorithm. SAML is an extensible markup language which is used for user communication to the service provider with the help of particular authentication [3]. The single sign-on method provides adequate security for user entities in the identity management, hash based encryption algorithm is used. At first the user has to register the details in identity provider and they must encrypt the user details with a particular length of key which is used to manage the user information for further processing. During the sign-on processing, complete assertion and authentication process helps to increase privacy of service related identities. In HBE, the user has a different number of keys which is used to validate the password with encryption and decryption keys. The user identifier, a 128-bit keyword is used to provide complete security and authentication to access service from the cloud. The key has to be changed using a different internet key exchanging protocol because it only provides additional security to user information and integrity check. Key exchange protocol has used particular hash functions to authenticate message code while transferring secret keys in the cloud. The key protocol first encrypts the user information using a secret key and then it is transmitted to further security based service access. Encryption algorithm provides the best security because both the service provider and the user have different encryption and decryption keys while sharing the password through the internet. So while an identity provider hides the user attributes from being accessed by a third party. In addition, it is easy to identify the third parties who are trying to access the user information using the encryption and decryption keys with different protocols. Additionally, this
proposed system covers the lack of service access, process and data management using the encryption algorithm. The following section describes the identity management related works, and security related proposed system.

II. RELATED WORK

Cloud computing is one of the main resources for developing a new business with a minimum cost and flexible platforms. It has provided different kinds of services but the main challenges are privacy, security, authentication, authorization and access control. Therefore, user information management, trust between the user and the cloud service providers have to be managed using different kinds of security and encryption algorithms. Federated identity management is the main feature to manage the user information using different security concepts like OpenID, OAuth, SAML with Single Sign on method. Eghbal Ghazizadeh et al., [4] proposed using trusted computing, federated identity management and OpenID Web SSO to solve identity theft in the cloud. They mention that identity issues are managed by using OpenID but some of the attacks lead to low security in identity management. They further mention that OpenID requires further steps to control the identity theft. Cloud computing is one of the main technologies for providing different kinds of services to the service requestor. The service provider needs to maintain security to manage user information and identity management.

Hongwei Li et al. [5] proposed different identity based cryptography techniques to be used to manage security. Hierarchical based cloud computing architecture is built and then security is managed by using identity based encryption, identity based signature with an authentication protocol like Secure Socket Layer (SSL) to manage user side information. Finally, the security in cloud computing is established using different cryptography techniques. Cloud computing is a developing scenario for new generation which provides different kinds of resources to service requestors.

Nida et al., [6] focused on the importance of Identity and Access Management (IAM). IAM is identity and resource management within the organization and it is the building block for the information security program and the most widely interacted security areas by the user. Identity and access management is, therefore, one of the most important concepts which helps to manage remote access user credential. In cloud computing, security is the main issue but security changes from one cloud identity model to another. Unique identification and authentication are important when providing services to the cloud service requestor.

Bernd Zwattendorfer et al., [7] identified different numbers of cloud identity management models that are available like isolated, user centric, central, federated and federated broker model. The user information has to be managed, based on the identity model. They proposed that federated broker based identity model should provide the best security and authentication to the user information. Identity based management system provides some security issues while dealing with the federated identity model.

Liang Yan et al., [8] showed the need to combine WS-Security approach federated identity management and HIBC and how it can reduce security problems in the hybrid cloud. This method is advantageous compared to other security algorithms and it reduces the SOAP header size. They have also shown that identity based problems can be restricted by using Hybrid Identity Based Cryptography (HIBC).

Roshni Bhandari et al., [9] discussed different identity management techniques for providing authentication, authorization, non-reputation, data confidentiality. In this paper author discusses about the various identity management frameworks such as SAML, OpenID, OAuth, PRIME, OneLogin and identifies related usage areas.

Jan Vossaert et al., [10] explained that user centric based identities are managed by using different trusted models. The user centric based model overcomes the federated identity model problem. It also has the extra functionality to provide security and trust between the service provider and the user. In the proposed system, the author demonstrated flexibility and more secure properties.

Md. Sadek Ferdous [11] implemented an approach which does not require change in SAML. It focuses on trust issue which is managed by dynamic federation. SAML based identity federation is created by users. They provided a means of creating dynamic federations automatically. Antonio Celesti [12] showed how trusted inter-domain communication is established using CLEVER based cloud. Authentication and trust between different CLEVER domain is achieved by SAML based SSO profile. It obtains authentication, trust between users and the cloud provider using SAML and CLEVER based cloud.

III. SAML AND HBE FOR IDENTITY MANAGEMENT

In cloud computing identity management is the main issue, because a large number of users requests the enterprise for various services. At the time identities are managed by using different federated identity protocol like OpenID, OAuth, SAML [13]. In the existing systems, the services are accepted by using the user name and the password but the user credential is hacked by using different phishing attacks. So, it is difficult to maintain user credential using the Single Sign-On (SSO) method and the main drawback of the existing system is the trust between the user and service provider. Another problem is the identity provider and the service provider may misuse the user information during authentication and authorization. Therefore, in federated based identity model, it is very difficult to manage the user information when several users request the service.
Federated based management system also focuses only on the Personal Identification Information (PII) during that time and is thus difficult to provide security to user credential.

Proposed System: In federated identity model, it is difficult to manage multiple user credential details for authentication and authorization data between parties in spite of managing user identities from different security and authentication issues. In the proposed system, the user identities are managed by using the User-Centric identity management model with Security Assertion Markup Language based Single Sign-On algorithm for providing authentication between the user and the identity provider because the centric model works based on Personal Trusted Device (PTD) with the help of Personal Transaction Protocol (PTP). In the identity model, the user information and the credential details are stored in the identity provider so that the user information is stored in the Personal Authentication Device (PAD) [14]. PAD is the context of the computer security which provides the particular key like PIN number to the user, so the user can access the different number of services using a single PIN. In addition, SAML provides secure login with Personal Authentication Device so that the user can store in unlimited details in the service provider with a single sign-on login. This procedure enables authentication and security to identities. Another problem is trust between the user and service provider. This drawback can be overcome by using encryption algorithm, Hash based Encryption (HBE). The user password is encrypted and decrypted using this encryption algorithm with key exchange protocol with poly hash function. The service provider and the user use different 128 bit key for encryption and decryption, so no one can access the user identities. Finally, encryption and decryption process increases the trust between the user and the service provider.

Security assertion and markup language: Security Assertion and Markup Language is one of the Extensible Markup languages. This is used to provide authentication between the user and the identity provider with the help of different protocols like HTTP, SOAP, and XML. SAML has three different components, namely assertion, binding, protocols, which give security to the user credentials [15]. These components are used between the Identity provider (IP) and the Service provider (SP) which indicates how it works together with the single sign-on. The single sign-on method is initiated by the identity provider or the service provider. If the service is initiated by IP, assertion is signed, encrypted or both. The browser or the user requests the resource from IP using their user name and password; then the IP redirects the authentication request to the browser. The browser then gets the authentication for the username and the password using a particular encryption algorithm and posts the request to the service provider. After that, SP gives resources to users. Figure 1 shows Single Sign-On authentication via SAML [16].

Hash based encryption algorithm: In cloud computing, communication is done with the help of media data so the data can be prevented from phishing and malicious attacks. For protecting the data, cryptography techniques are used. In the proposed system, Hash Based Encryption cryptography technique is used because it overcomes several problems like security and attacks. In HBE, fixed 128 bit of plaintext is used for encryption with different key lengths of 128 bit, 192 bit, 256 bits. In cloud, the services are accessed from different unknown service providers so the user identities need to be saved for further processing. Authentication and authorization is maintained by using Key Exchange Protocol (KEP). Poly message authentication code is combined with protocol which increases the security while transferring the user password with the known public key and secure private keys. Following steps describe the procedure of HBE algorithm.

Step by Step Procedure of HBE Algorithm
- HBE processes the entire data block and in parallel each round perform substitution and permutation.
- Input has 128bit and input related key is expanded into forty-four 32bit words.
- It has four different stages to provide the security one for permutation and the other three for substitution.

1. Substitute Bytes
   Different block ciphers used for special substitution called ‘S-box’ which is used to perform byte by byte substitution.
2. Shift Rows
   A simple shifting is performed row by row, but the row 0 is never changed.
3. Mix columns
   Substitution of the alerts of each byte in a column as a function of all the bytes in a column
4. AddRoundKey
   Simple X-OR operation should be performed between the current block and the expanded key.

For both encryption and decryption cipher text started with the AddRoundKey and followed by nine rounds with each performing those four stages.
The proposed system SAML with HBE encryption algorithm and key exchange protocol provides a high level security for the user identity management. Figure 2 explains the basic work flow between the user, the Identity Provider and the Service Provider using Security Assertion Markup Language with Hash based Encryption algorithm.

At first, the user requests the identity provider to access the particular service from the cloud using his own user name and password. Here the identity management is managed using the user centric identity model so that users need not memorize all the details. He or she just remembers that electronic PIN number. After that, the Identity Provider accepts the user request and authenticates the user information and returns the acceptance message to the user with help of SSO login via SAML [17]. Here the security and user information is managed by a third party, but in the cloud trust between user, identity provider and service provider is one of the main issues. For overcoming this issue, encryption algorithm with fixed input 128 bit block text and variable key length encryption algorithm is used to authenticate the user information.

It is proposed to use the hash based encryption algorithm, because the key length is changed every time and the key expansion plays an important role in security and authentication system. HBE algorithm work is also based on nine rounds and followed by the tenth round. For every round it has four different stages like substitution bytes, shift rows, mix column, key expansion. For every round the key length has to be increased (e.g. 128 bit has 10 rounds, 192 bit has 12 rounds, and 256 bit has 14 rounds). The secret key has to be exchanged between the user and the service provider with poly hash function. Thus encryption and decryption between the identity provider and the service provider helps to avoid the misuse of user information.

IV. RESULTS AND DISCUSSION

In this proposed work, implementation is done using Java platform. SAML is used for implementing both service provider and identity provider communication with Single Sign-On (SSO). To address the security issue, cryptographic technique Key Exchange Protocol (KEP) – Hash based Encryption Algorithm is used to ensure secure communication. Table 1 shows the average time taken to run HBE algorithm with different key lengths.

| Key Size (MB) | Megabyte processed | Time taken (ms) | MB/second |
|-------------|-------------------|----------------|-----------|
| 128         | 256               | 2.976          | 44.386    |
| 192         | 256               | 3.196          | 41.010    |
| 256         | 256               | 3.817          | 33.145    |

So, it has been shown that HBE algorithm provides better security in cloud because it takes several billion years to crack the 128 bit key using a brute force attack. Table 2 displays the time to taken to crack key versus and key size.

| Key Size (bit) | Time to crack (ms) |
|--------------|--------------------|
| 128          | 256                |
| 192          | 256                |
| 256          | 256                |

From Table 2, it is easy to know that phishing and brute force attacks cannot hack the user information because it takes more time and it is also difficult to find the secret key from the cloud. SAML with HBE algorithm has a minimum computation time, which is clearly explained using Table 3 and Figure 3.

| Key Size (bit) | Execution time (ms) |
|--------------|---------------------|
| 128          | 3.567               |
| 192          | 4.985               |
| 256          | 6.126               |

Figure 3 shows the time taken for computing Encryption with and without hash function. During the key schedule, it allocates different number of rounds and those round related secret keys work with key exchange protocol. Hash based key encryption combined with SAML results in less encryption time. The algorithm works with poly function,
which increases the security between user identities. So, HBE algorithm has been proved to provide the best security and also build the trust between the user and the service provider with a minimum execution time.

**CONCLUSION**

In this paper, cloud security and trust between user and the Service Provider have been provided by using Security Assertion Markup Language with Single Sign-On. Even though it provides authentication to user login, by using an additional cryptographic technique, i.e. Hash based Encryption algorithm, high security with the help of the Key Exchange Protocol can be obtained. That the identities and user credential details are managed by user centric identity management model has been thus proved through implementation in this paper. Thus, different enterprises request for and receive their services through cloud using SAML user web browser with a high security, and a fast acceptance.

**ACKNOWLEDGMENT**

Part of this work was done for my Thesis work Titled, "Improved User-Centric Identity Management Solution Using Cryptographic Techniques for Cloud Security”.

**REFERENCES**

[1] Antonio, C., T. Francesco, V. Massimo and P. Antonio, “Federation establishment between CLEVER clouds through a SAML SSO authentication profile”. International Journal on Advances of Internet Technology, volume 4, pp. 14-27, 2011.

[2] Bernd, Z., Z. Thomas and S. Klaus, “An overview of cloud identity management-models”, Proceedings of the 10th International Conference on Web Information Systems and Technologies (WEBIST), pp: 82-92, 2013.

[3] Eghbal, G., A.M. Jamalul-Lail, Z. Mazdak and P.Abolghasem, “A survey on security issues of federated identity in the cloud computing” Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science, 2012.

[4] Elisa, B., P. Federica, F. Rodolfo and S. Ning, “Privacy-preserving digital identity management for cloud computing”, Proceedings of the IEEE Computer Society Technical Committee on Data Engineering, 2009.

[5] Hongwei, L., D. Yuanshun and Y. Haomiao, “Identity-Based Authentication for Cloud Computing”, Springer-Verlag, Berlin, Heidelberg, pp: 157-166, 2009.

[6] Hongwei, L., D. Yuanshun and Y. Bo, “Identity-Based Cryptography for Cloud Security”. Retrieved from: https://eprint.iacr.org/2011/169.pdf, 2011.

[7] Jan, V., L. Jorn, D.D. Bart and N. Vincent, “Usercentric identity management using trusted modules”, Math. Computation Model, 57(7-8): 1592-1605, 2013.

[8] Liang, Y., R. Chunming and Z. Gansen, “Strengthen cloud computing security with federal identity management using hierarchical identity based cryptography”. Proceedings of the 1st International Conference, CloudCom, Beijing, China, 2009.

[9] Manoj, V.T., D. Anand and K. Chandrasekaran, Single sign-on in cloud federation using cloudsim, International Journai of Computer Network and Information Security, Volume 6, pp: 50-58, 2015.

[10] Nida, P., D. Harsh and H. Shahnawaz, “A survey on identity and access management in cloud computing” International Journal of Engineering Research & Technology (IJERT), vol. 3, Issue 4, 2014.

[11] Prasanalakshmi, B. and A. Kannammal, “Secure credential federation for hybrid cloud environment with SAML enabled multifactor authentication using biometrics”, International Journal of Computer Applications, Vol. 53– No.18, pp. 0975 – 8887, September 2012

[12] Roshni, B., B. Upendra and P. Dhiren, “Identity management frameworks for cloud”, International Journal of Computer Applications, Vol. 83(12), pp:25-31, December 2013.

[13] Sadek Ferdous, M. and P. Ron, “Dynamic identity federation using Security Assertion Markup Language (SAML)”, Proceedings of the 3rd IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, pp: 131-146, 2013.

[14] Safiriyu, E., A. Olatunde, O. Ayodeji, O. Adeniran, O. Clement and K. Lawrence, “A user identity management protocol for cloud computing paradigm”, Int. J. Communications, Network and System Sciences, Vol. 4, pp: 152-163, 2011.