Centralized Profile Translation Using Enhance Security

Priyanka Badwaik

***Abstract*— now days the value of web services are going to increase due to emerging trends in e-commerce. There are number of service providers like eBay, Amazon, LinkedIn where user needs to create their own profile under service provider domain. The profile is stored locally within proprietary personalization architecture at the service provider cloud under his control. Such system contains disadvantages like replicating the same information of user profile among multiple service providers decreases consistency of user profile and increase storage overhead. Consistency increases by centralizing the information, but there is again issue of privacy and security. For that user must keep trust on the service providers that their system is safe from hacking. In this paper we are trying to increase privacy, security, consistency and integrity of user profile data. Here, consistency and integrity achieved by centralizing the profile data and keep it under user control. Privacy and Security achieved by using Homomorphic Authenticable Ring Signature (HARS) scheme to authenticate correct user for accessing credential data of user. This concept is especially interesting for future mobile applications..**

***Index Terms*— Web service, e-commerce, personalization, user profile.**

I. INTRODUCTION

The growth of the Web services today is simply phenomenal. It continues to grow rapidly and new technologies, applications are being developed to support end users modern life. The Internet has enabled and accelerated new forms of human interactions through instant messaging, Internet forums and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Benefits of ecommerce are overwhelmingly varied and the intensity of internet usability has meant that information sharing is greatly achievable. Profile act as a cornerstone for web services. There are many cloud computing service providers like eBay, Amazon, Google, Microsoft etc. where user need to create their own profile by submitting their personal information. This profile is stored locally within proprietary personalization architecture at the service provider under his control. User must keep trust on the service providers that their system is safe from hacking. Replicating the same information of user profile across multiple service providers decreases consistency of user. profile. In Centralizing Profile Architecture Using Enhance Security (HARS), we focus on the point of profile storage location, user profile personalized architecture and security provide to the profile are consider [1][6][7] . Cloud computing improves due to centralization of data, it increased security but concerns can persist about loss of control over certain sensitive data or information, and the lack of security for stored data. Security is better than personal systems, because providers are able to devote resources to solving security issues that many customers cannot afford. There are many techniques available for providing security to cloud data which are explained in this paper below.

Personalization architecture increases the value of web services and has many benefits for user as well as service provider.

The benefits for users are:

- A better user experience in a different range of situations.
- Profile data will only need to be defined once. Users will not have to re-enter their information each time they acquire new services and devices.

The benefits for service providers are:

- Satisfied customers' needs that will cause to better user loyalty.
- Require less service development time.
- Larger user segments reached more easily and quickly.

II. PERSONALIZATION

In general personalization is a process of tailoring pages to individual user's characteristics and preferences. It collects behaviour of individual users and helps it for future recommendation system. There are three categories of personalization:

- Profile based personalization.
- Behaviour based personalization
- Collaboration based personalization.

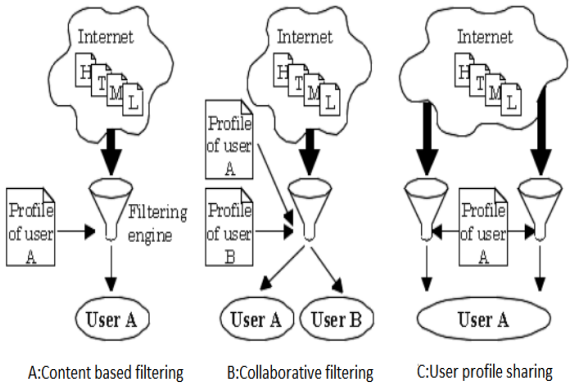

Fig 1. Personalization Architecture

The technology used in personalization includes collaborating filtering, user profiling and data analysis. In collaborating filtering, filter is applied for selecting relevant data which can be used in specific e-commerce experience of a customer. User profiling uses data collected from different sites and create personalized web page which can be used to predict future interaction by data analysis tools. The heart of personalization architecture is user profile.[6][9]

III. Creating User Profile

User Profile is nothing but a formal summary or analysis of user information which representing distinctive feature or characteristics about user. This information is accessed by key value pair. Profiles contain Meta information (i.e. data about data) to augment information. Such Meta information could be used to assess the user information [1].

The information collected either by implicitly or explicitly. Implicit collection of information contains many techniques like through Browser Cache, Proxy Servers, Browser Agents, Desktop Agents, Web Logs, and Search Logs. Many personalization architecture use browser agent base technique because agent place within user desktop computer. It also gives fewer burdens on the user, and it automatically updates as the user interacts with the system. Profile constructed manually by user or expert or it will construct automatically. Some approaches use genetic algorithms or neural networks to learn the profiles [2].

IV. Storing And Managing User Profile

There are three common ways for storing and managing user information in personalized system. Server based architecture where user profile both stored and managed at server. This system is also called as centralized system. The need of centralized system is to identify the user for correct information. There is no need of user profiles to transit through the network but there is issue of security and privacy.

In cookie based architecture, user profile stores on the client side and manages them on server side. The main advantage of such architecture is the distributed nature of the storage, which frees the service provider from supplying software and disk space for the database, but the transmission of the user profile between its storage location and the management location increases the response delay. Last is client based architecture where user profile manages and stores on the client side, such a system is also called as client-server architecture. For managing the information of user profile there is user profile management agent. Agent is responsible for managing and storing the user profiles as well as providing personalization support to Web applications [7] also we can create middleware for secure management [8].

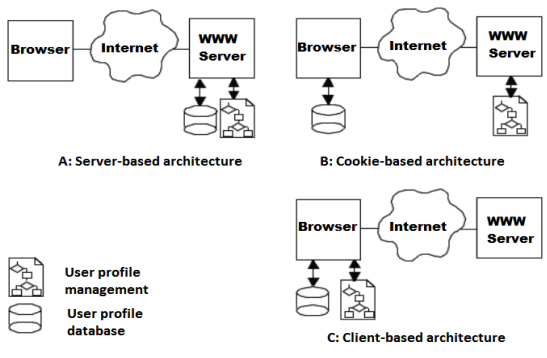

Fig 2.Storing And Managing Profile

V. Literature survey

Existing system has simple Login account which does not deal with central database. User profile stored at different service providers under their control. In such case if user want to update any profile, changes are not made in all account.

In the paper "Client –Side Profile Storage: a means to put the user in control" author gives the solution for security issue. They propose a distributed client side profile architecture to personalization. They consider that data should be stored locally within user domain, permitting personalized actions even if the device is not connected to a network. This client side user profile breaks into number of parts. These parts of the profile is distributed, replicated and kept consistent on user devices. Thus the user can access any profile data from any device in a trusted way. Device should manage all the profile information but such system contains some disadvantages that, if someone want to change any data of a profile then they have to make sure that changes should be occurred across all the replicated parts which contain those data[7].

In the paper "Architecture for profile translation" authors combine both technique i.e. centralizing and client base architecture for increasing the consistency and illuminating the security issue. Technically they separate user information into user profile and profile structure (view). User profile keep within user domain and profile structure keep centrally i.e. towards service provider. This system required different profile structures for different, independent profiles. The transparent linkage between structure and information created which will be free of context and semantics [1].

Open ID concept allows to use an existing account to sign in to multiple websites, without needing to create new passwords. With Open ID, user password is only given to identity provider, and provider then confirms the identity to the websites that user visit. The drawback of this system is redirection.

OAuth (Open Authentication) is authentication method like Open ID, but Open ID is a way to use a single set of user credentials to access multiple sites, OAuth is a way to allow one site to access and use information related to the user's account on another site. With Open ID, the process starts with the application asking the user for their identity (i.e. Open ID URI), whereas in the case of OAuth, the application

directly requests a limited access OAuth Token (valet key) to access the APIs (enter the house) on user's behalf. If the user can grant that access, the application can retrieve the unique identifier for establishing the profile (identity) using the APIs..Disadvantage of such system is that user can't save additional information about itself on the server.

For providing security over cloud data there are number of cryptographic algorithms which are classified into two categories: symmetric and asymmetric algorithms. Symmetric algorithm uses a single key i.e. secret key for both encryption and decryption process whereas asymmetric algorithm uses two keys i.e. Public key which is available publically and other is the private key, which is kept secret used to decrypt the data. Breaking the private key is rarely possible. Examples of symmetric algorithm are Data encryption standard (DES), International data encryption algorithm (IDEA), advanced encryption standard (AES). On the other hand asymmetric key algorithm include RSA algorithm. Asymmetric algorithms are mostly used in real world whereas symmetric algorithms are ideally suited for security applications like remote authentication for restricted websites which do not require full-fledged asymmetric set up.

The use of passwords for authentication process is popular among the users but the transmission of messages containing password create a path for hackers. Advanced authentication techniques include single-usage-password where the system may generate challenge token expecting the user to respond with an encrypted message using his secret key which converts the password to some derived value enabling. For using the cryptographic techniques care should be taken for storing encryption and decryption keys.

In many applications, it is desirable to work with signatures that are short and where many messages from different signers are verified very quickly. RSA signatures also help for verifying signers, but are generally thousands of bits in length. Recent developments in pairing based cryptography produced a number of short signatures which provide equivalent security in a fraction of the space but verifying these signatures is computationally intensive due to the expensive pairing operation. In an attempt to simultaneously achieve short and fast signatures here introduce new ring and aggregate signature schemes.

VI. NEED OF ENHANCING THE SECURITY IN CLOUD

There is number of user shared their data with other users but when user share data for other users then that time owner of data does not know about who access data so there is chances of accessing authorized data by unauthorized person. In this system also user profile data is shared among different service providers, some service provider login through another service provider ID (e.g. LinkedIn login through Face book or Gmail) without taking permission from owner, such system arise questions on security and privacy and increase chances of accessing credential data from unauthorized users.

VII. FUTURE ENHANCEMENT

For enhancing security level of shared data in cloud numbers of techniques are available like use dynamic hashing technique and ammonization technique in encryption algorithm to protect shared data from attackers. Recently many works focus on providing three advanced features for remote data integrity checking protocols i.e data dynamic, verifying data publicly and providing privacy against various verifiers.

VIII. ALGORITHM FOR ENHANCE SECURITY OF DATA ON CLOUD

A. Homomorphic Authenticable Ring Signature (HARS)

This algorithm is extended form of ring signature. It helps to verify privacy as well as support to block less verification.

B. Attribute Based Signature (ABS)

In this algorithm, users send a complaint to server with a message. This complaint helps to know the user have authenticated access or not, without knowing user identity. Other users or the cloud verify the user and the validity of the message stored. By combining ABS (Attribute Based Signature) ABE(Attribute Based Encryption) to get authenticated access control without knowing the identity of the user to the cloud. This system create symmetric key to provide privacy preserving authenticated access control in cloud .

C. Markle's Signature Algorithm

This algorithm gives an alternative of signature scheme. It is based on a secure hash function and a secure one-time signature. It is used for modification of data when user wants and for doing dynamic operation on data like when any user want to modified other user data at that time firstly verify that user and send massage to authenticate user if user is valid then data will be modified by user otherwise not. This algorithm work on append mode.

D. Provable Data Possession (PDP)

This algorithm allows to user that contain stored data at an entrusted server to verify that the server actual data without downloading. This system require proofs of possession of server by sampling set of random blocks from the server for that purpose user need to maintains a specific amount of large data to verify the proof. Thus, this model for remote data checking requires large data sets in widely-distributed storage systems .

E. Third party Authentication (TPA)

This model allows private as well as public audit ability and increase the security of data that store on cloud. To secure that data third party used encryption algorithm like RC5 to store data and create one secret key which send to user to decrypt data. But some time there is untested things are

generated that's why there is many possibility to loss of data.

F. International Decryption Encryption Algorithm (Idea)

This algorithm is used to store data in encrypted format on cloud without any central authority interference. To enhance security on cloud IDEA combine with Bit Serial architecture algorithm which is used to create data pattern when encrypt the data.

Below system use Homomorphic Authenticable Ring Signature (HARS) algorithm for providing security to the profile data which is stored on cloud and shared among different service providers because it support Public Auditing, Data Privacy and Identity Privacy.

IX. RING SIGNATURES

The concept of ring signatures was first proposed by Rivest in 2001. With ring signatures, a verifier understand that a signature is computed using one of group members' of Service providers private keys, but the verifier is not able to find which one. Considering , a ring signature and a group of d users, a verifier cannot distinguish the signer's identity with a probability more than 1/d. This property helps to preserve the identity of the signer from a verifier. The ring signature scheme introduced by Boneh (BGLS) is constructed on bilinear maps. Here, we will extend this ring signature scheme to construct our public authentication mechanism.

X. HOMOMORPHIC AUTHENTICATORS

Homomorphic authenticators are basic tools to construct public auditing mechanisms Here, only a user with a private key can generate valid signatures. In this paper we use this technique for generating homomaorphic ring signature. A homomorphic authenticable signature scheme should satisfy the following properties:

Blockless verifiability: Block less verifiability allows a verifier to audit the correctness of data stored in the cloud server with a special block (here we consider attribute because profile consist of different attribute), which is a linear combination of all the block in data. If the integrity of the combined block is correct, then the verifier believes that the integrity of the entire data is correct. In this way, the verifier does not need to download all the data to check the integrity.

Non-malleability: It indicates that an adversary cannot generate valid signatures on arbitrary block by linearly combining existing signatures.

XI. NEW RING SIGNATURE SCHEME

Homomorphic authenticable ring signature (HARS) scheme, which is extended from a classic ring signature scheme. The ring signatures generated by HARS are not only able to preserve identity privacy but also support the system from hacking by unauthorized users. In this system Ring signature is generated by using private keys of different service provider and this task is perform by TPA. Building the privacy-preserving public authentication mechanism for shared data in the cloud based on this new ring signature scheme is explain in following section.[2]

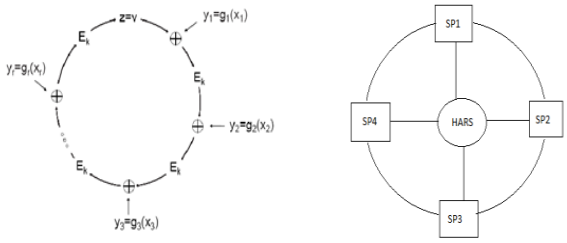

Fig 1. Ring Signature

XII. CONSTRUCTION OF HARS

HARS includes three algorithms: KeyGen, RingSign and ProofGen, ProofVerify.

1) ***KeyGen:*** The KeyGen algorithm is run m times to obtain a set ((pk1, sk1)... (pkm, skm)) Of keypairs .Here, TPA generates Private and Public keys for each user profile.

2) ***RingSign*** (***σ):*** In Ring Sign a server generate a signature which will be applicable on credential data for providing advance security. Signature is generated by aggregating private key of each service provider onto which user initialized

3) ProofGen: This work is done by server. It generates proof for correct authentication.

4) ***ProofVerify:*** ProofVerify is a verifier (here TPA) which verify whether the proof generated by server is correct or not. In proposed system this work is done by TPA.

XIII. SYSTEM MODEL AND ARCHITECTURE

In system architecture user, cloud storage server, TPA and service provider plays important role. First user have to create a centralized profile by filling detail personal information like name, address, mobile number, bank detail, educational detail etc and set one Id and password for accessing this profile. The profile is stored into server so the server contains number of different user's profile. Now user is ready to join any services by giving name and type of services to which he want to connect. When user connects with any of the service, one unique random number is generated for that users service.TPA plays a role of key generation. It generate key for each user profile. When communication is done in between user and cloud storage

server, the data is encrypted with ring signature and perform homomorphic authentication while travelling through network. This ring signature is generated by server and it share this sign with all service provider to which user connect. When user want to edit some profile data or send data it perform homomorphic operation on encrypted data and send it. It is very difficult to read this data by unauthorized users because they does not know the encrypted key and if they get the key then also homomorphic operation provide another level of security.

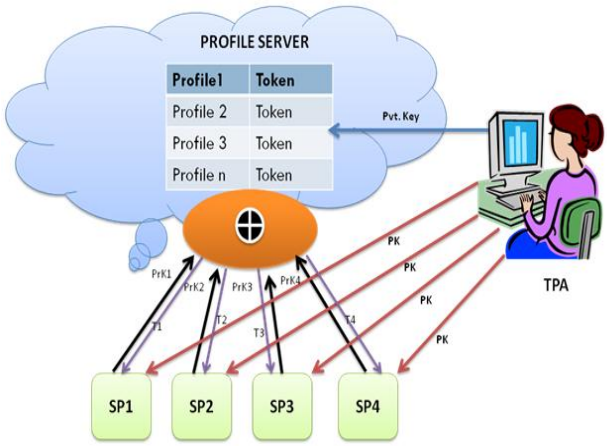

Fig 3. System Architecture

XIV. ANALYSIS AND RESULT

In fig 4(a) & 4(b) the generation time of a group signature on a block is determined by the number of users in the group and the number of elements in each block. when k is fixed i.e 100 and 200, the generation time of a ring signature is linearly increasing with the size of the group. And when G is fixed i.e 10 and 20 the generation time of a ring signature is linearly increasing with the size of elements per block. In all the graph we compare HARS algorithm with AES algorithm and found that HARS is more efficient than AES.

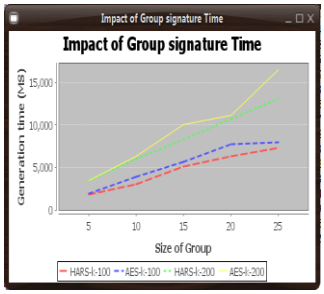

Fig.4 (a)

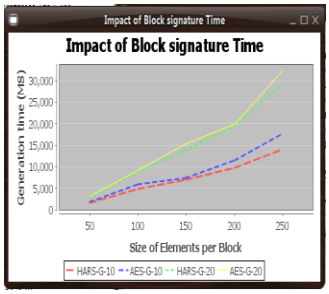

Fig.4 (b)

Fig 5(a) & 5(b) shows impact of group communication time and block communication time. If blocks are fixed i.e. 300 and 460 and size of group is increase then communication time linearly increase. In second graph as we increase size of element per block then also communication time increase. In both the cases i.e. impact of group communication time and block communication time HARS take less communication time compare to AES algorithm.

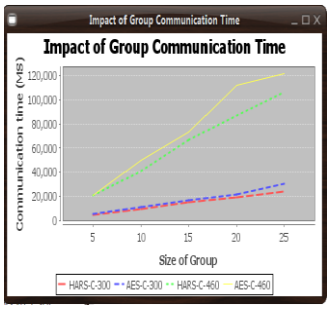

Fig.5 (a)

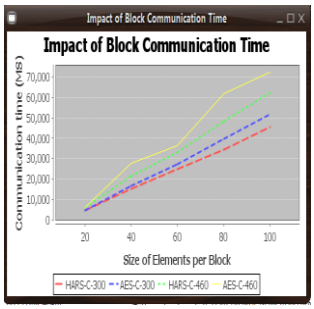

Fig.5 (b)

Based on our proceeding analyses, the auditing performance of this system under different detection probabilities is illustrated in below graph 6(a) and 6(b). The auditing time is linearly increasing with the size of the group and size of block. Suppose when C is 300, if there are two users sharing data in the cloud, the auditing time require is only about 10000 ms; when the number of group member increases to 20, then it takes about 25000 ms to finish the same auditing task.

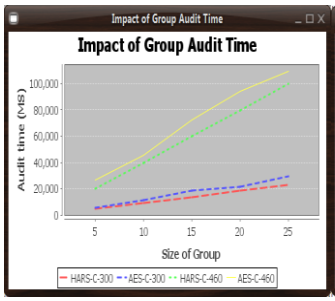

Fig.6 (a)

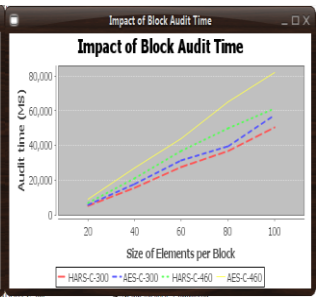

Fig.6 (b)

XV. CONCLUSION

For using any web service user first need to create their own profile by submitting personal data. Traditionally there are many systems where user profile stored at different service providers under their control. This causes many issues like security, inconsistency of user data, wastage of memory due to storing similar data across many sites etc. These issues can be eliminated by centralizing profile architecture. Personalization plays important role in centralized profile. The main aspect of this architecture is to make the unique profile to access users multiple accounts. The system is design in order to make a centralized database to reduce the complexity of database. It will helps user to work conveniently with different account by using single profile. And the user will more secured due to the HARS security system. Here HARS use for authentication purpose. It will recognize correct user by generating proof and verifying it.

REFERENCES

[1] Bjoern Wuest, Olaf Drogehorn and Klaus David,"Architecture for Profile Translation" IST summit 2012.
[2] Boyang Wang, , Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud"IEEE TRANSACTIONS

ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.

[3] Susan Gauch, Micro Speretta, Aravind Chandramouli, and Alessandro Micarelli,"User Profiles for Personalized Information Access".

[4] Laurent Frelechoux and Tomonari Kamba "An architecture to support personalized Web applications- A User Profile Management Proxy" .

[5] Ziegler M., Muelle W., Schaefer R. , Loeser C.,"Secure Profile Management in Smart Home Networks", IEEE Database and Expert Systems Applications, ISSN :1529-4188, ISBN:0-7695-2424-9, Aug. 2005.

[6] Tatiana Kovacikova, Françoise Petersen, Mike Pluke, Valentine Alonso Alvarez, Giovanni Bartolomeo, Antonella Frisiello, Erik Zetterström, Scott Cadzow, "Personalization and user profile standardization",ETSI STF 34, European Telecommunications Standards Institute Sophia Antipolis France.

[7] H. Hirsh, C. Basu and B. D. Davison, "Learning to personalize", In Communications of the ACM, Vol.43.8, p. 102-106.

[8] S. Riche, G. Brebner, M. Gittler, "Client-Side Profile Storage: a means to put the user in control", Public Technical Report, Hewlett Packard Laboratories Grenoble, November 2012.

[9] Poonam N. Railkar, Parikshit N. Mahalle, "Proposed secure context aware profile translation" IJITS, Vol. 1; No. 2: ISSN: 2277-9825.

[10] www.wikipedia.com

[11] R. Vanathi, L. Dhanam, K.R. Senthilnathan, M.S. Vinu, "Secured and Reliable Data Transmission Using Lychrel Numbers RGB Colors and One Time Password" IJCSMC, Vol. 2, Issue. 10, October 2013.

[12] Salem Aljareh ,Anastasios Kavoukis," Efficient Time Synchronized One Time Password Scheme to Provide Secure Wake-up Authentication On Wireless Sensor Networks "International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 3, No.1, January 2013.

Priyanka Badwaik, is graduate in Computer Technology from KDK college of engineering, Nagpur and pursuing her master from AISSMS Collage of Engineering under SSPU, Pune. Author has published a paper, "Centralized Profile Translation Architecture Using Enhance Security "
in International Journal Of Computer Science And Information Technology, vol 5,Issue 6 2014.

