An Efficient Model for Securing Identity Access in Scalable System

Sunil Singh
IIIT- Allahabad

Manish Kumar
IIIT- Allahabad

Shantanu Das, PhD.
IIIT- Allahabad

ABSTRACT

This paper proposes an identity management system model which will ensure secure storage and retrieval of the IDs information in the scalable identity database. The proposed model uses the distributed database technology for information storage and retrieval to make the system more reliable. The IDs information storage is secured by using cryptography mechanism of data conversion in the identity database. Authenticated link by internet service providers is used for secure communication of the user information between the authenticated service agencies/ user service providers and the Identity server. For retrieval of the user sensitive information, this paper proposes an access method based on request and authorization of the service provider.

Keywords

Digital Identity, Identity Server, Data Privacy, Authenticating Service Agency, Service Provider.

1. INTRODUCTION

A user needs to provide relevant identification information like username/password, card number etc. to authenticate them to obtain the services offered by the service providers. Each organization provides digital identity, according to its suitability, to authenticate the person and provide services they offer. So a user may possess multiple identities provided by various organizations. Therefore, need a unique ID concept to replace multiple IDs of a person to a single ID, globally accepted by the entire service provider. Integrating identity in such a large scale is a complex task, and it arose various security and privacy issues in ID storage and access.

The unique identifier and descriptive attributes of a person constitute the unique identity of that person. Because of the rising need of unique identity allocation for its population in various countries for giving basic amenities; this is the need of the hour to implement some concrete security measures for protecting such important identity database. The security is necessary because the information it contains. Identity database contains extremely crucial details like finger print, iris scan and in future various other data like DNA. The main difference between this data with conventional data is later being changeable and former fixed for life, once it compromised it revealed forever and lifelong burden for the victim. Apart from this, there is another epic threat for the nation state security because these databases contain crucial details of almost whole population once it compromised the security of the whole state compromised.

The digital identity life cycle [8] may be defined as

1. **Identity aggregation and synchronization**: To manage the identity for the scalable system is a highly dynamic task because of frequent changes in different parameters like domicile, email address, phone number etc. Keeping track of all these changes and consistency within the central database is called identity aggregation and synchronization.
2. **Maintaining Identity Information:** The primary information, which was collected during the first phase about any person, undergoes modification during its lifecycle is known as maintaining the identity with latest changes.
3. **De-provisioning the identity:** When an identity reaches the ends of its life cycle, the corresponding account must be either removed or disabled. Hence De-provisioning in timely and accurate manner provides the security as well as fulfillment of legal liability against various laws corresponding to that geographical area.

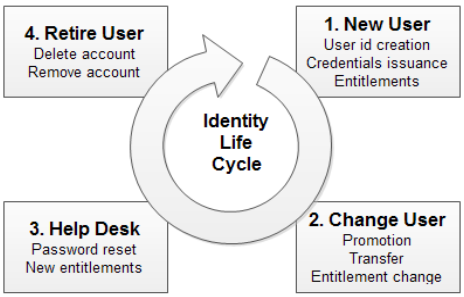

Fig 1: Identity Life Cycle

Above discussion shows that the unique identity management is highly dynamic exercise and provides security to such a valuable resource is a big challenge because of details present at a single place. There are various techniques used for storing and dissemination of such information but very few utilize the concept of hardware based encryption. Hardware based encryption is pretty much faster than its counterpart and hence useful for identity management in scalable system where the biggest challenge is providing the information in efficient and timely manner but in a secure way.

Unique identity infrastructure can be useful in various social welfare services and effective monitoring of these services. While the main focus of such id infrastructure is welfare of the general public, it can also be used by various other enterprises and service providers like telecom, banking etc. for better services. Identity authentication can be used by service providers for the following three basic uses types.

1. Ensuring presence and proof of delivery.
2. Used as a common identifier to link related databases.

3. Verification for Know-Your-Customer (KYC) credentials.

Section 3 discusses related work, summarizing common Identity management concepts and storage mechanism. Section 4 introduces the problems in Existing IDM system and Section 5 consist of two subsections, first is proposed system architecture and second is issues addressed by the proposed model. Section 6 describes detail working procedure of the proposed model and section 7 concludes the paper with future work.

2. Related work

Identity management is intuitive concept and therefore it is extremely difficult task to determine its exact origin in history. The most fundamental issue is the definition of identity and what constitutes an identity [1]. Advent of a new concept such as digital identity intended for better management of various resourced is of considerable importance for population as whole but at the same time cumbersome process for manage such a vast data resource. This transition from conventional identity towards digital identity and their respective trade-off like association of different features of digital infrastructure such as protocols to biometric is given by Alvaro J. Gutierrez [9]. Apart from the above source a truly comprehensive text tries to give life cycle of identity in apprehensible form and provide a base for precise possible improvements in different phases [8].

A technique proposed by Vajihollahi Mona [1] tries to explain identity management by giving widely accepted management models using different concept like predicate calculus. But due to the very dynamic environment, continuous changes in components of identity like iris scan, fingerprint, face recognition [5, 13] etc. necessitate to adapt these changes. Besides such changing conditions, another important issue of tackling very large number of such requests for identity creation and authentication try to achieve in the existing model [2] has better scope for improvement. Storage of such a large database is also a serious matter of concern because of efficient resource management and rapid information retrieval [7].

Designing scalable system for supporting extremely large number of requests caring about security issues is stated by Alan R. Downing [6]. Privacy is another important feature for such important data because of its static nature like finger-print and iris scan etc. The paper published by Surajit Chaudhuri [4] deals with privacy issues [10] in an efficient manner. Apart from this another way of information storage is proposed by Ashutosh Saxena [3, 11], which helps in comply with privacy issues in trans-border affairs.

3. Issues in existing IDMS

The various issues related to the security of the information stored in the existing ID management system are as follows-

- **Inconsistency:** the ID integration is not fully secure as it depends on the information provided by the ID user which may be some times false. Sometimes for gaining more benefits, a person may obtain more than one identity by providing false document. This makes the ID management system inconsistent.
- **Intrusion:** Digital identity is used over the public network for verification of a person and obtaining the services. The information shared over the public network can be misused by intercepting the communication or deploying worm and viruses to the victim's machine. Intrusion can lead to the privacy violation and also serious security issues.
- **Unreliability:** The ID management systems currently in use are unreliable. Because, they use the unreliable service over the public network for ID integration and verification. The information send over these unsecure networks may be intercepted and can be misused.
- **Insecurity:** the current ID management Infrastructure rely on the browser security, cookies, http authentication etc. which are vulnerable to various types of attacks. This makes the current infrastructure insecure for providing a reliable digital ID management System.
- **Duplicate Information:** A user may register themselves from more than one of the authenticating service agencies in order to get more benefit from the duplicate ID. This will result in duplication of the information in the IDMS database.
- **Availability:** Most of the current ID management systems are based on centralized database, in which the ID are stored and verified from a single database server. This lead to a single point failure and the availability of ID verification process is not guaranteed round the clock.

4. Proposed IDMS Model

The ID management systems currently in use are based on the centralized database technologies for ID storage and verification. These types of systems are not efficient because they are prone to single point of failure and the whole ID integration and verification process fails. The IDMS, stores critical information of the user and in case of physical security breach; the entire user's ID information in the database are compromised. This may lead to severe concerns about national security in case of the IDMS like UID.

4.1 IDMS Architecture

In this model, the distributed database technology is used to ensure that the ID verification is uninterrupted and 24x7. The distributed technology will ensure the availability of the IDMS server for verification; unlike in the Centralized database server where a single point of failure results in the collapse of the entire IDMS system. The distributed system architecture of the IDMS will make the verification process faster, in comparison to centralized IDMS server, as more IDs can be verified by using multiple IDMS server.

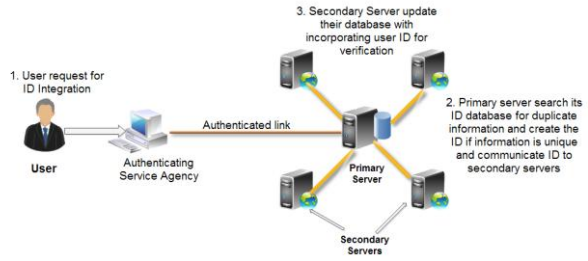

Fig 2(a): Identity Integration

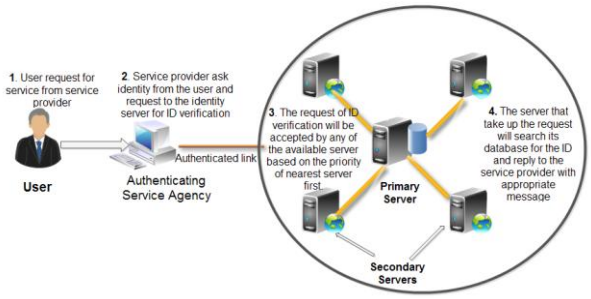

Fig 2(b): Identity verification

Components of the network Architecture

User: User is the entity that request for the services offered by the ASA's by presenting their ID's. The ASA's in turn provide services to person after the ID verification by the IDMS server's based on the information provided by the user.

Identity Server: The user's IDs are initially stored in the primary IDMS server during the ID creation/Updation, and communicated to the secondary servers via authenticated link. The information in the primary server is synchronized with the other servers in a periodic interval. The entire servers would update their database periodically so that the ID's verification can be done by using any server. By using multiple IDMS servers, it ensures that the service delivery is continuous. Even if one server is down the verification can be done through other server.

Authenticating Service Agencies: These are the trusted node of the IDMS system for identity integration and user service authorization. The integration or updation of the ID information is done through ASAs. It would be the responsibility of the ASA's to verify the document provided by the user during ID creation and updation.

User Service Provider: The entities that provide the user service like banking, gas connection, medical etc. to the user; are called user service provider. The user request for services from the service provider, which in turn request the identity server for user ID verification or user's information needed to provide the requested service. If the user request is genuine, the service is provided to user else denied.

Authenticated link: Special links by the internet service providers dedicated to IDMS are used to authenticate the components of the system.

4.1.1 Secure ID storage System

In the present scenario, various types of IDs are used to access different type of services. To integrate all the services of the nation to a single unique ID create the challenge to enhance greater security and privacy in the IDMS. As the IDs contains the sensitive information like biometric identity, that is unique of a person and for the life time and cannot be changed in the due course, requires a greater concern during storage and retrieval of the information in the IDMS. Because, the information is very critical and once compromised can be used in various ways, to obtain the services illegally and can even cause a threat to national integrity and security.

Therefore, the security to the IDMS should be ascertained by providing the security measures from point of information collection, to storage and up till the information retrieval by the service provider.

In proposed model, devices specially developed by the trusted computing group are used for storing the sensitive information in the IDMS. These devices are developed by the TCG as a part of promoting the use of the security enable devices that store and deliver the information in a secure manner when required.

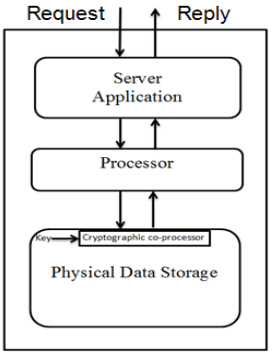

Fig 3: Storage Structure

Component of the Storage System

Server Application: The storage system contains the server side application program to serve the request for the identity verification by the user. The application server provides services like security, load balancing and management for distributed databases.

Processing Unit: It is the computational unit of the system. At the time of ID integration, it processes the query received from the server application and store the information in the database. At the time of retrieval of the ID's information, it performs the required computation.

Storage Device: Devices developed by the TCG is used to store the information of the ID's in a secure manner. The trusted computing is a notion for trustworthiness of a node in the network. The device uses the concept of encryption and decryption for securing the information while storing. The storage medium contains a cryptographic co-processor, a key and an algorithm to store the encrypted information. When the request for data storage is made, the co-processor encrypts the data with the key available and then stores the information. At the time of the information retrieval, the co-processor decrypts the data by the key and then passes the information to the processing unit for further computation.

4.1.2 ID verification system

Information in the IDMS needs to be protected from unauthorized access and also the privacy of the ID's should be maintained. This increases the concern to provide security during information access by the various service providing agencies.

Traditionally IDMS uses a centralized repository system to store all the information of the ID's. This creates the problem of single point failure. As all the services are connected to one ID, therefore, the verification should be 24x7.

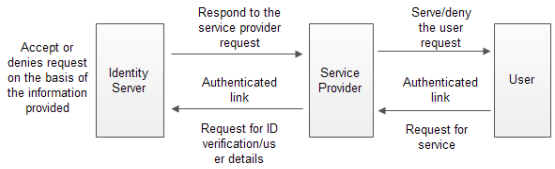

Fig 4. ID verification process

In proposed system, the database would be distributed instead of traditional centralized database for IDMS. The distributed database model will ensure that the identity verification is continuous. To reduce the computation load on the server, proxy server can be used. All the necessary computation on the server side may be done by the proxy server so that the resources on the server side may be fully utilized. The IDMS server will be accessible by the Authenticating Security Agency (ASA) after the authentication. The authentication between IDMS server and ASA is done by using public key cryptography. The ASA will provide the expected services to the user after ID verification by the IDMS server.

4.2 Security and Privacy issues addressed by proposed model

The following are the issues addressed by the proposed model which make it more secure and reliable than the existing IDMS

- **Reliability:** The proposed model uses the authenticated links for ID integration and verification provided by the internet service providers. Hence the services are reliable.
- **Security:** The proposed model provides greater security by storing the information in encrypted form, which cannot be decrypted by using normal hardware configuration. Thus in cases of physical security breach the information of the user are secure.
- **Privacy:** The proposed model ensures the privacy of the user by making the information available only to the authenticating service agencies accessible only through the authenticated link.
- **Availability:** The proposed model uses the distributed technology to store and retrieve the information, this ensure that the ID integration and verification process are available round the clock. Mere failures of one or two server do not hinder the service's availability to the users.
- **Link authentication:** The model uses the authenticated and secure link of the internet service providers to ensure that the communication between the IDMS component are secure and cannot be intercepted. Encryption of the information over the link is done to ensure the security and privacy of the communication.
- **Access Control:** The information's of the user's in IDMS are accessible only via the authenticated nodes (ASA), hence the information of ID can only be accessed by the authenticated user by furnishing their information to the ASAs.
- **Unique ID:** The proposed model will remove the duplicate ID issue by providing a unique ID to each user by incorporating biometric identity to the digital identity.

5. WORKING

The proposed model uses the features of the distributed system technology to provide reliability to the IDMS and make the ID's information available when required. The model contains one primary and multiple secondary servers. ID integration in the system is done through the primary IDMS server, and the ID information is communicated to the secondary servers that may be used later for user's ID verification.

For obtaining the Unique ID in this system, a user has to request the ASAs authorized by the IDMS with the relevant document for identity verification. The ASAs transfer the request of ID integration to the primary server. The server matches the information with the existing IDs for duplication. If information is unique, then the ID of the user is created on the server. The newly created ID information is communicated to the secondary server via authenticated link. The user gets the ID via ASA from the primary server. The user can update their information subsequently via the same process.

When the user request for the services provided by the user service provider like gas connection, fund transfer, insurance etc. then the service provider chooses any one of the available IDMS servers (primary/secondary) and sends the user information for verification. The server search its database for the verification of the user ID based on the information provided by the service provider. The server replies to ASA whether user ID is authenticated or information furnished by the user are false.

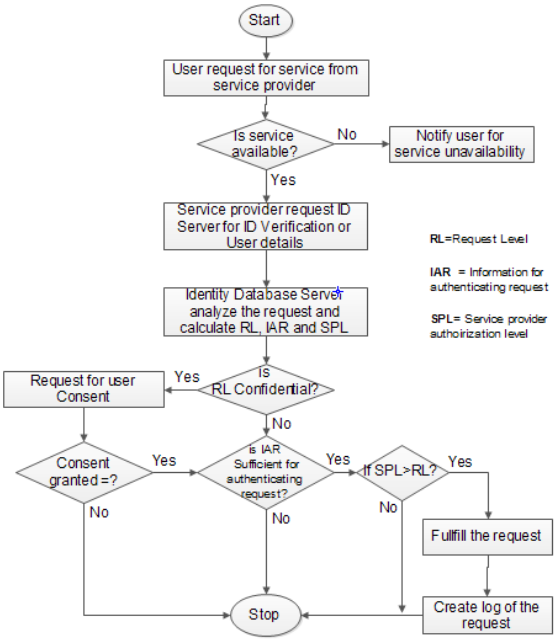

Fig 5. Information Access flow diagram

Sequential process for ID verification and user information access

Step 1: The user request for service from the service provider.

Step 2: On the basis of the availability of the service the service provider may accept or deny the user

request. If the requested service is not available then user, is notified with an appropriate message.

Step 3: If the service is available, the user is asked to provide identity. The service provider request for the ID verification/user information from the Identity Database.

Step 4: The Identity Database analyze the request from the user service provider and identify the authorization level of the requesting service provider, the type of the information requested and the information provided for request authentication.

Step 5: If the information requested need the user consent, a message is send to the user asking for his consent to provide information to the service provider. If the user give positive acknowledge, then further processing is done otherwise the service provider is denied of the user information stating that user do not want to disclose the information.

Step 6: For checking the authenticity of the request from the service provider the additional information provided by the service provider is checked. If the information is adequate, then the request is processed else denied with an appropriate message.

Step 7: In the next step, if the level of the information requested is less than or equal to the authorization level of the service provider, the user information requested is given to the service provider and a log of the request of the service provider is stored.

Step 8: Else if the authorization level of the service provider is less than the level of the information requested then also the service request is denied.

6. Conclusion and future work

The proposed model provides the digital identity services in scalable system. The model utilizes the cryptographic technique for secure storage of the ID information and uses the distributed database concept to provide greater reliability and security than the existing system. The sensitive information of the user can be accessed securely through the proposed access method. The availability and the security features are better than the other system. Also, the model proposed is very easy to implement. The presented idea can be efficiently applied to other systems that provide the digital ID management.

In future, this model can be used to accomplish refined access methods to protect the user privacy and make it more efficient. There is also possibility to authenticate the service providers based on the remote attestation method.

7. REFERENCES

[1] Uwe Glasser, Vajihollahi Mona. Identity Management Architecture. IEEE, June 17-20, 2008, Taipei, Taiwan 1-4244-2415-3/2008.

[2] Meng-Ju Hsieh, Chao-Rui Chang, Li-Yung Ho, Jan-Jan Wu, and Pangfeng Liu. SQLMR: A Scalable Database Management System for Cloud Computing. International Conference on Parallel Processing, 2011.

[3] Vishal Gupta and Ashutosh Saxena. Personalized Data Set. IJDMS Vol.2, No.4, November 2010.

[4] Surajit Chaudhuri, Raghav Kaushik and Ravi Ramamurthy. Database Access Control & Privacy: Is There A Common Ground? 5th Biennial Conference on Innovative Data Systems Re-search (CIDR ’11) January 9-12, 2011.

[5] M Johnson I Agbinya, Nazia Mastali, Rumana Islam and Jackson Phiri. Design and Implementation of Multimodal Digital Identity Management System Using Finger print Matching and Face Recognition. 6th International Conference on Broadband Communications & Biomedical Applications, November 21 - 24, 2011.

[6] Alan R. Downing, Ira B. Greenberg and Teresa F. Lunt. Issues in distributed database security. IEEE, TH0287-3/90/0000/0196 Q 1990.

[7] Chiung-Shien Wu, Gin-Kou Ma, and Mei-Chian Liu. A scalable storage supporting multistream real-time data retrieval. Springer-Verlag, Multimedia Systems 7, pp.458–466, 1999.

[8] David Mowers and Michel Baladi, “Microsoft Solutions for Security and Compliance,” Microsoft Corporation, Sci. Rep. 85, 2006.

http://technet.microsoft.com/en-us/library/cc162924.

[9] Alvaro J. Gutierrez, Professor Joan Feigenbaum. Towards Better Digital Identity Management. Sensitive Information in a Wired World CPSC 457b - Spring 2006.

[10] The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. http://www.oecd.org/dataoecd/55/48/43091476.pdf.

[11] The Next-Generation Secure Computing Base (NGSCB).

http://en.wikipedia.org/wiki/Next-Generation_Secure_Computing_Base.

[12] The trusted computing base (TCB). http://en.wikipedia.org/wiki/Trusted_computing_base.

[13] Unique Identification Authority of India. (2012). Aadhaar Enabled Service Delivery [White paper]. http://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf