USER’S PRIVACY IN CLOUD WITH IRIS AUTHENTICATION

***P.S.Abdul Lateef Haroon, **Dr. Fathima Jabeen**

**Assistant Professor, Dept. of ECE, BITM, Bellary-583104*

***HOD, Dept. of ECE, KSSEM, Bangalore-560062*

ABSTRACT

Cloud computing allows use of resources which are being daily accessed by millions of users which poses risk on the privacy of the users. In our paper we use Iris as a part of PII (Personal Identifiable Information) to authenticated the user itself to the service provider as Iris recognition is computationally effective as well as reliable in terms of recognition rules. After user is being authenticated service provider cannot be trusted to share other sensitive information in PII like social security numbers etc to perform various transactions , to prevent sensitive information to be exposed we propose use of IDM .The approach is based on the use of unary function over encrypted data and multi-party computing for negotiating a use of a cloud service. It uses active bundle.—which is a middleware agent that includes PII data, privacy policies, a virtual machine that enforces the policies, and has a set of protection mechanisms to protect itself. An active bundle interacts on behalf of a user to authenticate to cloud services using user’s privacy policies.

Keywords— Cloud Computing, Privacy, Iris, Active Bundle, Iduser management system, Multiuser computing

I. INTRODUCTION

In today’s computational era, cloud is gaining popularity and expanding day by day. Cloud computing allows the use of Internet-based services to support business processes. Millions of users utilize the services provided by the cloud on daily basis .It offers a concentration of resources, so due to such high networking traffic it imposes risks on the privacy of the users. A cloud *service provider* (*SP*) is a third party that maintains information about, or on behalf of, another user. Trusting a third party requires taking the risk that the trusted third party will not exploit the sensitive information provided by the users and privacy of the user will not be breached. A single breach can cause significant loss. In cloud computing, users may have multiple accounts associated with a single or more than one service provider (SP). Sharing sensitive iduser information that is, PII (Personally Identifiable information) can lead to mapping of the idusers to the user. Privacy in cloud computing can be stated as what information a user reveals about himself to the cloud Service Provider and the ability to control who can access that information. Numerous existing privacy laws impose the standards for disclosure of personally identifiable information (PII) that must be satisfied even by cloud SPs. PII is commonly known as id user information. In cloud computing, there is little information available to point out where data are stored, how secure they are, who has access to them, or if they are transferred to another host (if that host can be trusted). A cloud cannot be used for storing and processing data and applications if it is unsecure. The major problem regarding privacy in cloud is how to secure PII from being used by unauthorized users and how to prevent attacks against privacy (such as userid theft) even when a cloud SP cannot be trusted, and how to maintain control over the disclosure of private information. Iduser management (IDM) is one of the core components for user privacy in cloud. Solutions which are available today use trusted third party (TTP) in identifying users to SPs. In this paper, we propose an approach which uses iris templates to authenticate the identity of an user and to impart the privacy we propose IDM system without considering trusted third party. Iris templates are considered for authenticating the user to the SP as use of iris is highly sophisticated mechanism for identifying a user but the existing algorithm for matching the iris templates in database consumes lot of time and resources of cloud. So we introduce an efficient algorithm for matching iris templates using booth's algorithm. The approach is based on the use of unary function over encrypted data and multi- party computing for negotiating a use of a cloud service. It uses active bundle, which is a middleware agent that includes PII(iris and sensitive data), privacy rules, a virtual machine that enforces the policies, and has a set of protection mechanisms to protect itself. An active bundle interacts on behalf of a user to authenticate to cloud services using user's privacy policies.

II. IRIS RECOGNITION

All According to John Daugman [1], following are four steps for creating an iris template:-

1). Segmentation
2). Normalization
3). Enhancement
4). Feature Extraction

1) Isolating the actual iris region in digital eye image.
2) Performing Linear and Circular Transformation on extracted iris image to obtain edge map, horizontal and vertical map.
3) With the use of daugman's integro differential operator circular iris, pupil regions and arcs of upper and lower eyelids are located.
4) The image obtained is normalized and is passed through gaber filter tp obtain encoded iris template.

The existing approach available to match iris templates is:- Comparison of bit patterns generated is done to check if the two irises belong to the same person. Calculation of Hamming distance (HD) is done for this comparison. The Hamming distance is a fractional measure of the number of bits disagreeing between two binary patterns. Two similar irises will fail this test since distance between them will be small. The test of matching is implemented by the simple Boolean Exclusive-OR operator (XOR) applied to the 2048 bit phase vectors that encode any two iris patterns. Letting A and B be two iris representations to be compared, this quantity can be calculated as with subscript 'j' indexing bit position and denoting the exclusive-OR operator.

Goodness of Match Factor:-

$$\frac{1}{2048}\sum_{j=1}^{j=2048} A_j \oplus B_j$$

The result of this computation is then used as the goodness of match, with smaller values indicating better matches. John Daugman, the pioneer in iris recognition conducted his tests on very large number of iris patterns (up to 3 million iris images) and concluded that the maximum hamming distance that exists between two irises belonging to same person is 0.32.The decision of whether these two images belong to same person depends upon following result.

If HD < = 0.32 decides that it is same person. If HD > 0.32 decides that it is different person.(Or left and right eyes of the same person).

III. PROPOSED WORK

We propose an efficient algorithm to match iris templates generated from above described steps. An iris is divided into 8 sub-parts and each subpart is given a tag. A template is created in which each tag represents the sub-band of a particular iris region. This algorithm uses Booth's algorithm for generating tags for iris code.

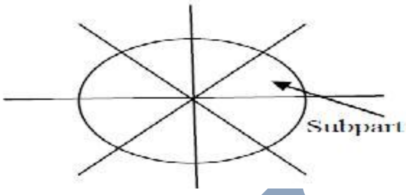
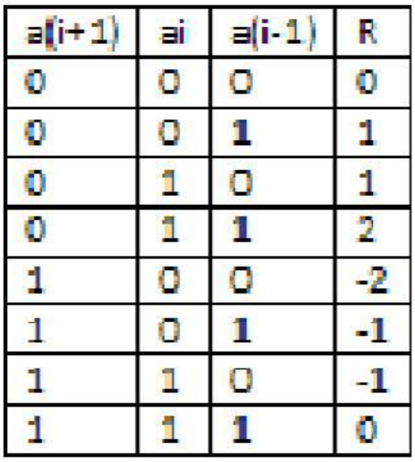


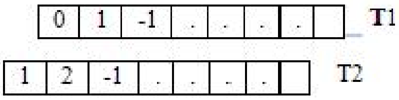
Fig 1: Dividing Iris into 8 equal parts.

Algorithm and model:
1) Take image submitted by user as input and extract the iris image using circular transformation.
2) Convert it into an iris code using John Daugman's [1] method.
3) Let M be an iris code and it is represented as a set of binary bits (1, 0) M= {M0, M1, M2….Mn}
4) Divide this whole iris into 8 sub bands.
5) Let M = | M / 8 |.
M= {{m0, m1...mn} 1, {m0...mn} 2,.... {m0, m1, mn} 8} And M' = { {m0,m1,…mn}i } for 1 <= i < = 8
Where,{m0,m1…mn}1…..{ m0,m1…mn }8 are the 8 Sub-bands of iris. Each sub- band is formed by number of bits.
6) Select any 3 bits from each sub-band forms a template
T = {T1, T2, T3…T8} Where Ti = {mi, mj, mk}.
And i , j ,k are not equal and 0 <= i,j,k <= n
Ti is obtained by passing all three bits through Booth's algorithm.



a(i+1)	ai	a(i-1)	R
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	2
1	0	0	-2
1	0	1	-1
1	1	0	-1
1	1	1	0

T1 is a string generated (template) of the authenticated image and T2 be a string (template) generated of the selected image.



0	1	-1	.	.	.	.		T1

1	2	-1	.	.	.	.		T2

Working of proposed algorithm:
1) Each template is arranged in a form of a circular linked list which constantly rotating head.
2) The image submitted by user is compared with the image templates stored in the cloud database.
3) Iris templates in Cloud database is searched in following way:

Comparison:

I] Iris template created by above process will be of 8 bit long.
II] At each position out of eight, five values are possible i.e. it can be 0,1,2,-1,-2.
III] So we can store total of 5^8 (390625) templates in cloud database.
IV] In searching process, first bit of user iris template is checked and it will be one of the five possible bits i.e. either 0,1,-1,2,-2.
V] So if first bit is 0 then 312500 other iris templates which has first bit other than zero will be redundant and search will continue for remaining iris templates.
VI] As next bit is encountered, 62500 more iris template will become redundant.
VI] In similar way, as comparison progresses, more and more iris templates will become redundant.
VII] Due to which the time required to search image stored in database reduces exponentially.

4) Above proposed algorithm helps to reduce time in searching process in vast cloud environment.

IV. WORKING OF SYSTEM

In the Earlier section we proposed an efficient algorithm to match iris templates

USE OF ACTIVE BUNDLE IN IDM

Let us take a look now at the active bundle scheme, and its use for IDM. An active bundle includes sensitive data, metadata, and a virtual machine. Sensitive data contains content to be protected from privacy violations, data leaks, unauthorized dissemination, etc..—e.g., it contains PII. Metadata describes the active bundle and its privacy policies. Virtual machine (VM) manages and controls the program code enclosed in a bundle. Its main functions include:

(a) Enforcing bundle access control policies through apoptosis, evaporation, or decoy actions;

(b) Enforcing bundle dissemination policies; and

(c) validating bundle integrity.

The components of an active bundle for IDM are:

1) Identity data: Data used for authentication, getting service, using service (e.g., SSN, DOB). These data are encrypted and packed inside the active bundle.

2) Disclosure policy: A set of rules for choosing which identity data to disclose. E.g., if identity data I are used for service S, then I should be used each time S is accessed (minimizing disclosure of PII).

3) Disclosure history: Used for logging and auditing purposes. It is also used for selecting identity data to be disclosed based on previous disclosures.

4) Virtual Machine: It contains the code/algorithm for protecting PII, on untrusted hosts.

An active bundle is sent from a source host to a destination host. When arriving at a "foreign." host, an active bundle ascertains the host's trust level through a TTP. Using its disclosure policy, it decides whether the host may be eligible to access all or part of bundle's data, thus becoming a "guardian" for the data, and which portion of sensitive data can be revealed to it. The remaining data (not to be revealed) might be evaporated as specified in the access control policies, protecting the data. We consider a number of different metrics for adaptive control of the degree of evaporation, including trust-based metrics. An active bundle may realize that its security is about to be compromised.

System work takes place in following steps:

We have presented a use-case view of our proposed work of the system .In the system presented, we have assumed a bank is there in the cloud SP and user has to share the sensitive information with the bank only to perform the transaction. Two keys would be used Pk(Public Key), MSK(Multiparty key) for encryption of the PII. Pk, will be present with SP also to get the iris image whereas MSK will be present with the user and with which be shared.

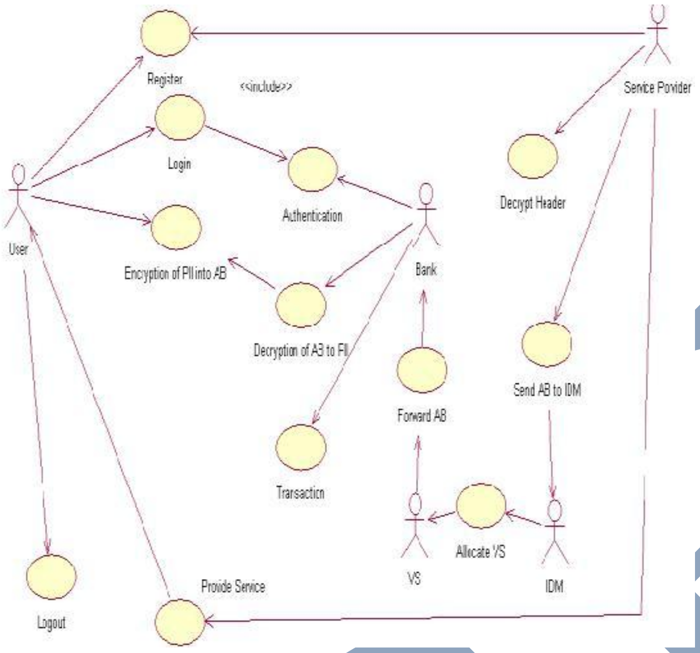


Fig 2: Active Bundle in IDM

1) User:

a). The user can register itself to service provider, by authenticating his iris to guarantee the service provider that he is the owner himself.
b). The user has to encrypt the sensitive data that has to be shown to the bank only not the service provider. The Active Bundle (AB) acts as a mobile agent and guardian of PII. Two keys would be generated Pk(Public Key) , MSK(Multiparty key) for encryption of the PII. PII would be present in Active Bundle in encrypted form. Iris image would be encrypted using Pk, whereas the information that has to be shown to bank only would be encrypted using Pk , MSK.
c). The user can seek the cloud service from the service provider.

2) Service Provider:

a). SP decrypts the header in the Active Bundle and checks the validity of the user by checking the user's iris and the matching algorithm that we proposed earlier would be used. The SP has only Pk, so it can only decrypt the a part of PII that is iris image.
b). It send the AB to the IDM.
c). It can provide services to the user.

3) IDM

a). IDM allocates a virtual server.
b). IDM encrypts the AB with new public key and sends it to bank. The AB was again encrypted with a new public key because it during the way to bank it might be attacked by some attacker.

4) Bank

a). Bank decrypts the AB using MSK and accesses the sensitive information like card no's to make the transaction and checks the validity of the information.

V. CONCLUSION

With the increasing scope of cloud computing, privacy of user has become a critical concern for any user. There is a need for an efficient and effective privacy-preserving system. The system should:
(1) Be independent of any trusted third party
(2) Be able to unambiguously identify users that can be trusted
(3) Be able to protect users' Personally Identifiable Information (PII). The goal is to prove effectiveness of the proposed privacy and identity management system, as well as its potential for becoming a standard for privacy and identity management in cloud computing.

REFERENCES

[1] John Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.

[2] Rohit Ranchal, Bharat Bhargava , Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang , Mark Linderman Protection of Identity Information in Cloud Computing without Trusted Third Party 2010 29th IEEE International Symposium on Reliable Distributed Systems

[3] Pelin Angin, Bharat Bhargava, Rohit Ranchal, Noopur Singh, Lotfi Ben Othmane, Leszek LilienAn Entity-centric Approach for Privacy and Identity Management in Cloud Computing

[4] D.Kesavaraja*1, D.Sasireka 2, D.Jeyabharathi3 Cloud Software as a Service with Iris Authentication Volume 1, No. 2, September 2010 Journal of Global Research in Computer Science

[5] Siani Pearson Taking Account of Privacy when Designing Cloud Computing Services

[6] Guidelines on Security and Privacy in Public Cloud Computing Wayne Jansen, Timothy Grance

[7] Data Security Model for Cloud Computing Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing