International Journal of Computer and Communication Technology

Volume 3 | Issue 3 Article 7

July 2012

THREE TIER DATA STORAGE SECURITYIN CLOUD USING FACE FUZZY VAULT

VRUSHALI JOSHI
AISSMSIOIT, Pune, Maharashtra, India, joshi.vrush@gmail.com

PAYAL SANGHVAI
AISSMSIOIT, Pune, Maharashtra, India, payal.sanghavi@gmail.com

YOGITA BHARGUDE
AISSMSIOIT, Pune, Maharashtra, India, yogitabhargude@gmail.com

THREE TIER DATA STORAGE SECURITYIN CLOUD USING FACE FUZZY VAULT

VRUSHALI JOSHI, PAYAL SANGHVAI & YOGITA BHARGUDE

AISSMSIOIT, Pune, Maharashtra, India
E-mail : joshi.vrush@gmail.com, payal.sanghavi@gmail.com

Abstract - The well-known buzzword, say Cloud Computing, attracts the attention from both academy and industry across the world, because of its potential in achieving the long-held dream, say Utility Computing and opens a new era for new spawned companies to provide services above this new concept[6],[8]. At the same time hackers have also turned their faces to cloud to breach the security. The best software solution provides utilization of cloud computing and take full advantage of it with best security solutions and assurance. To achieve this goal proposed system provides the following solution, which uses three tier security in cloud environment. Set of biometric features are first extracted from user's face image, The extracted features are then quantized and mapped to binary representation for feature point matching. The produced features and the secret key (which will restrict unauthorized access) are bound using Face fuzzy vault scheme .During authentication key will be correctly retrieved if face vault matches. Also to prevent data from cloud service provider, data is encrypted while saving it on the cloud using Confidentiality, Integrity, Availability (CIA) values which will categorize data in three rings. While providing data if user is authorized then the concerned password gets extracted from the fuzzy vault and the extracted password will help to decide which user belongs to which data ring.

Keywords - *Cloud Computing, Face fuzzy vault, CIA, Data ring, Three tier security.*

I. INTRODUCTION

Today a growing number of companies have to process huge amounts of data in a cost-efficient manner. Classic representatives for these companies are operators of Internet search engines, like Google, Yahoo, or Microsoft. The vast amount of data they have to deal with every day has made traditional database solutions prohibitively expensive. Thus the cloud is best suitable for above requirements.

One of the cloud services Data as a Service (DaaS) is capable in order to simplify the development of distributed applications. On top of such architectures, many of these companies have also built customized data processing frameworks. Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [7].Cloud provides key features such as on-demand self-service, broad network access, virtualization, Resource pooling and data sharing. Different Service Models available which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), Data as a Service (DaaS). The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. Deployment Models are: Private cloud: Enterprise owned or leased, Community cloud shared infrastructure for specific community, Public cloud: Sold to the public, mega-scale infrastructure, Hybrid cloud: Composition of two or more clouds. Now a day cloud computing make everything flexible and easier but there is another aspect that is the security issue. According to the survey, some companies states that due to cloud computing it becomes easier for bad guys to focus their effort and breach hundred and thousands of record. There is no security rating system in place for cloud computing, so business users can't rely on third party security mechanism. Risk factor with cloud computing are high because level of security provided by cloud provider are not same. CRYPTOGRAPHIC techniques [1] are being widely used for ensuring the secrecy and authenticity of information .The security relies on the cryptographic keys and maintaining the secrecy of keys is one of the main challenges in practical cryptosystems. However, passwords can be easily lost, stolen, forgotten, or guessed using social engineering and dictionary attacks. Limitations of password-based authentication can be alleviated by using stronger authentication schemes, such as biometrics. Biometric systems [3],[4],[5]establish the identity of a person based on his or her anatomical or behavioral traits, such as face, fingerprint, iris, voice, etc.

A critical issue in biometric systems is to protect the template of a user which is typically stored in a database or a smart card. The Face fuzzy vault construct is a biometric system that secures both the secret key and the biometric template by binding them in single template to provide unique identification.

According to literature survey, we found that To provide security in private cloud environment following framework is suggested [9].As shown in figure1 when user sends request along with username to access the data to cloud provider, the cloud

provider first checks in which ring requested data belong. If authentication is required, it first checks the username in its own directory for existence, if the username does not exist it ask the user to register itself. If the username matches, it redirects the request to company for authentication, then the user sends password for authentication, and after authentication it redirects the request to cloud provider to access resource.

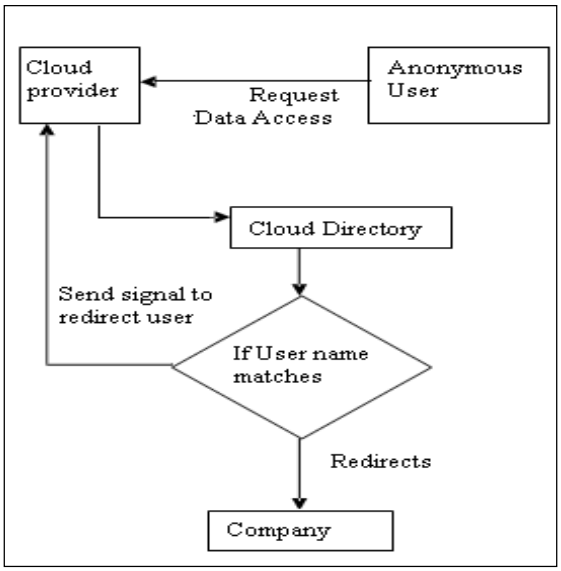

Fig. 1 : Security with redirection

Above framework introduces redirection for security which will increase time, space and maintenance cost. Proposed system will provide secure framework without redirection which is shown in figure 2.Juels and Sudan [2] proposed a cryptographic construction called a fuzzy vault that operates in the key binding mode and, in principle, can compensate for intra class variations in the biometric data. They have presented a fully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae. In the SonglongYuana 's [10]online authentication model, at the registration stage, fuzzy vault encoding is implemented using both key and transformed template. And then the fuzzy vault is encrypted using digital signature. Face extraction can be implemented [11], [13] with PCA algorithm, but face may get injured due to any mishaps and then the user may lose his/her identity. Considering all available techniques and related issues, proposed system will provide one of the solutions to handle different challenges that we found in survey. To solve security issue proposed system will provide THREE TIER SECURITY which is as follow.

TIER 1: Focuses on the problem of data leakage the data classification is done by company before storing the data. This classification is done on the basis of CIA (Confidentiality, Integrity, Availability).The value of C is based on level of secrecy at each junction of data processing and prevents unauthorized disclosure, value of I based on how much assurance of accuracy is provided, reliability of information and unauthorized modification is required, and value of A is based on how frequently it is accessible. With the help of proposed formula, the priority rating is calculated, accordingly data having the higher rating is considered to be critical and Three Tier security is recommend which will provide higher security.

TIER 2: Clients are also categorized to avoid unauthorized access. Classified data is distributed in three rings. Clients are categorized according to these rings, same priority clients belong to same ring. To provide unique access each ring will contain a secrete key.

TIER 3: Face fuzzy vault is the technique which binds ring secrete key with user's face feature to provide controlled data access to authorized user i.e. fuzzy vault provides unique identification. In this paper Section1 provides abstract of system.Section2 represents domain specific analysis and literature survey. Section 3 represents proposed techniques to provide security. Section 4 represents conclusion and section 5 is to represent references.

II. PROPOSEDSYSTEM:

As discussed earlier [9] general framework provide redirection (figure 1) but to handle security risk, proposed system helps without redirection. When the user requests for data access, user authentication and authorization issue gets solved at cloud only through worker role which is running at cloud and get controlled through company. Company is responsible to set CIA values for data classification while saving it on cloud proposed framework is shown in figure 2.

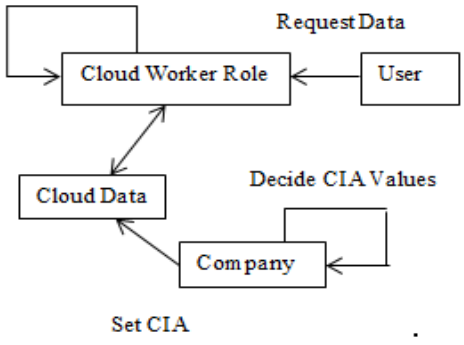

Fig. 2 : Security without redirection

2.1 CIA Technique For Ring Selection:

Let D be the set of 'n' documents to be stored on cloud database Data D= {1, 2, ……., n}Let C be the value of confidentiality where C={C|c ε N} where N is any natural number, Let I be the value of Integrity where I={I|IЄN},

Let A be the value of availability where A= {A|A Є N}1. Input: Data, protection ring, D[] array of n integer size. Array C, I, A, S, R of n integer size.2. Output: categorized data for corresponding ring. For i 1 to n C [i] = Value of Confidentiality. I [i] = Value of Integrity. A [i] =Value of Availability.

Calculate: S=Selection of Ring according to the given formula below: S (i) = [C (i) +A (i) +I (i)]/3, Let S= {1, 2, 3},Let R be ring where R= {1, 2, 3} If 0> S (i) <33Select Ring3 If 33≥ s (i) ≤66Select Ring2 Else if 66≥S(i)≤100 Select Ring1

Analysis: After applying algorithm for categorizing the data on the basis of sensitivity. Now ring rule and conflict of interest is applied in the ring to make more robust security system. Ring rules restrict data access.

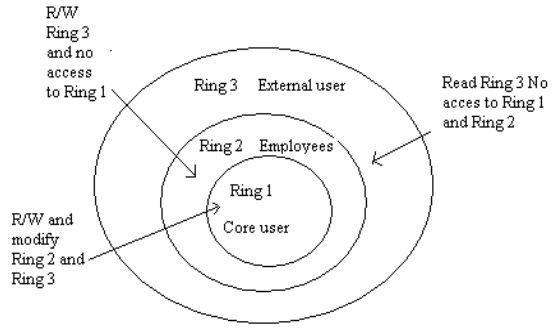

Fig. 3 : Ring Representation

Ring rule:

1. The users granted access to Ring3 is not allowed to access any R/W in lower rings.
2. The user granted access to Ring1 is allowed to access upper rings i.e. Ring 2 and Ring3 (Add, delete modify)
3. The users granted access to Ring2 is allowed to read data from ring 3 but cannot modify existing data.

2.2 Face Fuzzy Vault Encoding.

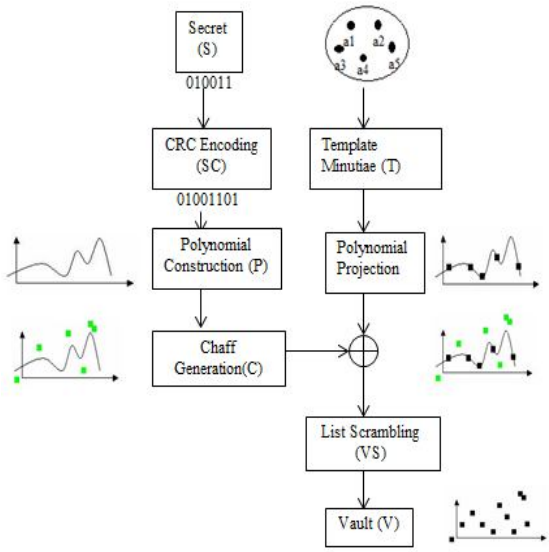

Fig. 4 : Face fuzzy vault encoding

Let Secret 'S' be 'cloud' which is to be bound with the face feature template. The characters in the secret are converted into binary format and the binary value is encoded with 16-bit Cyclic Redundancy Check (CRC) encoding. We generate 16-bit CRC data from the secret S. The 16-bit primitive polynomial we use for CRC generation, $g_{CRC}(a) = a^{16} + a^{15} + a^2 + 1$, is called "CRC-16".Appending the 16 CRC bits to the original secret S (128-bits), we construct 144-bit data SC. From this point on, all operations take place in Finite field $F(2^{16})$. We concatenate x and y coordinates of a minutia (8-bits each) as[x|y] to arrive at the 16-bit locking/unlocking data unit u. The bit string SC is used to find the coefficients of the polynomial p: 144-bit SC can be represented as a polynomial with 9 (144/16) coefficients, with degree D = 8.$p(u) = c_8u^8 + c_7u^7 + \ldots\ldots\ldots + c_1u + c_0$.In other words, SC is divided into non-overlapping 16-bitsegments, and each segment is declared as a specific coefficient c_i , i = 0, 1,2,…..,8. Two sets composed of point pairs are generated. The first one, called genuine set G, is found by evaluating p(u)on the template minutiae (T). Assuming that we have N template minutiae (if we have more than N minutia, we choose the first N sorted according to ascending u values),$u_1,u_2,\ldots\ldots\ldots\ldots\ldots u_N$, we construct $G\{(u_1,p(u_1),(u_2,p(u_2),\ldots\ldots\ldots\ldots(u_n\ p(u_n)\}$.Note that the template minutiae, $u_1,u_2,\ldots\ldots$, u_N are selected to be unique, namely, $u_i \neq u_k$, if $i \neq k$, where i = 1,2,……..,N, k = 1, 2, ……..,N. The second set, called the chaff set C, ensures the security of the system. To add M chaff points, we first generate M unique random points, c_1, c2,…….,c_M in the field $F(2^{16})$, with the constraint that they do not overlap withu_1, u_2, ……..,u_N. Then, we generate another set of M random points, d1, d2,….,d_M, with the constraint that the pairs (c_j ,d_j), j = 1,2, …..,M do not fall onto the polynomial p(u). The chaff set C is defined as $C\{(c_1,d_1),(c_2,d_2),\ldots\ldots\ldots\ldots..(c_n,d_n)\}$The union of the genuine and chaff sets, G ∪ C, is finally passed through a list scrambler that randomizes the list, with the aim of removing any stray information that can be used to separate chaff points from genuine points. This results in the vault set V

$S\{(v_1,w_1),(v_2,w_2),\ldots\ldots\ldots\ldots..(v_{N+M},w_{N+M})\}$.

2.3 Face Fuzzy Vault Decoding:

A user tries to unlock the vault V using N query minutiae Q ={ }. The points to be used in polynomial reconstruction are found by comparing, i =1,2,……,N with the abscissa values of the vault V , namely v_l, l = 1, 2,… (N + M): if any , i =1,2,…..,Nis equal to v_l; l = 1, 2,. .., (N + M), the

corresponding vault point (v_l,w_l) is added to the list of points to be used during decoding.

Assume that this list has K points, where $K \leq N$. For decoding a degree D polynomial, (D + 1) unique projections are necessary. We find all possible combinations of (D + 1) points, among the list with size K, resulting in (K/(D+1)) combinations. For each of these combinations, we construct the Lagrange interpolating polynomial. For a specific combination set given as L{(v1,w1), (v2,w2),……., (vD+1,wD+1)}. the corresponding polynomial is

$$p^*(u)=\frac{(u\,¡\,v2)(u\,¡\,v3)\cdots(u\,¡\,vD+1)}{(v1\,¡\,v2)(v1\,¡\,v3)\cdots(v1\,¡\,vD+1)}w_1\ldots\ldots\ldots+\frac{(u\,¡\,v1)(u\,¡\,v2)\cdots(u\,¡\,vD)}{(vD+1\,¡\,v1)(vD+1\,¡\,v2)\cdots(vD+1\,¡\,vD)}w_{D+1}$$

This calculation is carried out in F(216), and yields $P^*(u)=C_8^* U^8+C_7^* U^7+\ldots\ldots+C_1^* U+C_0^*$.

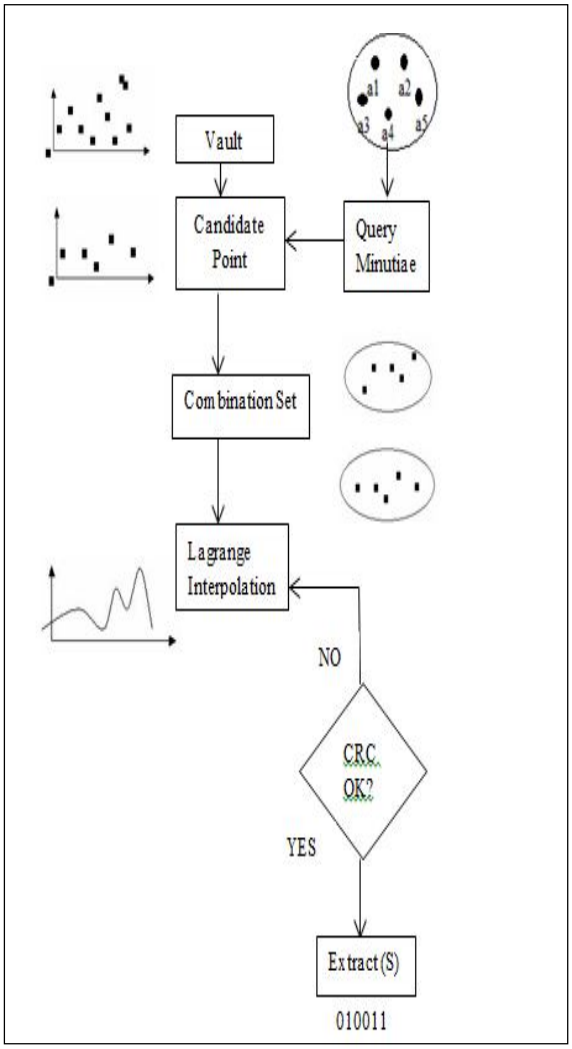

Fig. 5 : Face fuzzy vault decoding

The coefficients are mapped back to the decoded secret SC*. For checking whether there are errors in this secret, we divide the polynomial corresponding to SC*with the CRC primitive polynomial, gCRC(a) = a16 + a15 + a2 +1. Due to the definition of CRC, if the remainder is not zero, we are certain that there are errors. If the remainder is zero, with very high probability, there

2.4 Face Extraction:

Face is captured through Webcam and stored in a specified size required. The stored image is in RGB color format. The RGB format is converted to YUV chrominance format for easy extraction of face features. The skin color is detected by skin detection algorithm and the face is cropped by applying right, left, up and bottom boundaries. The cropped face is converted to grayscale so that during decoding the features are matched correctly. The features are then extracted by applying Scanning Edge Detection Algorithm to the grayscale image.

2.5 User Registration:

Company is using cloud services and data is categorized in three rings according to CIA, and the company will assign secrete key to each ring. Users are of three type Ring1 includes Core user (e.g. CEO, higher authority etc), Ring2 include company employees and Ring 3 includes external or anonymous users. When first time the user visits the company, the user has to register with the company .For that he/she provide face image and required details. Company checks user details and necessary constraints then allows the user to become part of company .According to the type of user company generates User ID(UID)which will categorize users in three layers. If UID is generated successfully then fuzzy vault encoding takes place i.e. the secret and extracted face features get combined in vault. After this users UID along with face fuzzy vault get saved on cloud database.

2.6 User Data Access:

At the time of data access user must provide the UID received during registration and face image. Firstly users face gets encrypted to ensure image gets securely travelled through internet. At the worker process, received UID gets checked with saved database. If the UID is available, saved fuzzy vault gets compared with received template, if the match is found, secret key of particular user's ring gets extracted during fuzzy vault decoding and accordingly controlled data access can be achieved. Figure represents Data access flow.

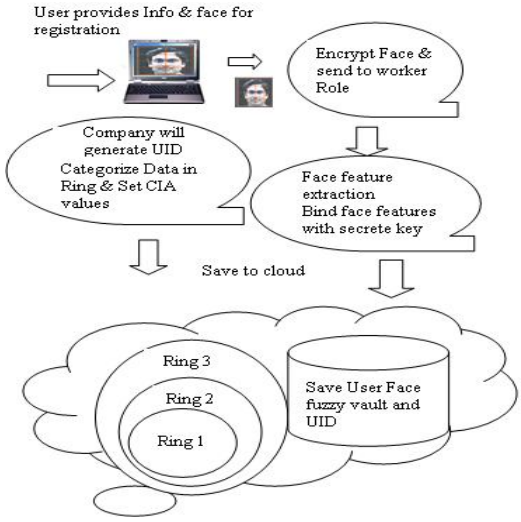

Fig. 6 : User Registration process

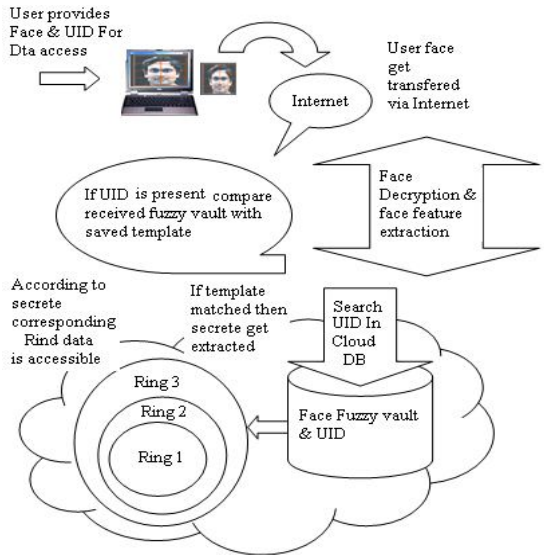

Fig.7 : User data access

III. CONCLUSION:

We will provide one of the solution to secure data stored on cloud using face fuzzy vault. The data on cloud is arranged in three layers according to CIA and accessed by authorized user of the particular layer. Hence, the data is protected from any modifications or misuse by the service provider as well as unauthorized user.

REFERENCES:

[1] Karthik Nandakumar, Student Member, IEEE, Anil K. Jain, Fellow, IEEE, and Sharath Pankanti, Senior Member, IEEE, "Fingerprint-Based Fuzzy Vault:Implementation and Performance", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 2, NO. 4, DECEMBER 2007.

[2] A. Juels and M. Sudan. "A fuzzy vault scheme," in Proc. IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, 2002, p. 408.

[3] Dacheng Xu School of Applied Technology Soochow University Suzhou 215006, Wang School of Electronics and Information Engineering Soochow University Suzhou 215006, "A Scheme for Cancelable Fingerprint Fuzzy Vault Based on Chaotic Sequence", Proceedings of the 2010 IEEE International Conference on Mechatronics and Automation August 4-7, 2010, Xi'an,China.

[4] Hosik Sohn, Yong Man Ro, Senior Member, IEEE, and Kostantinos N. Plataniotis, Senior Member, IEEE," Content Sharing between Home Networks by using PersonalInformation and Associated Fuzzy Vault Scheme ", IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009.

[5] Yongjin Wang, KN. Plataniotis The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, 10 King's College Road, Toronto, ON, Canada, M5S 3G4, "FUZZY VAULT FOR FACE BASED CRYPTOGRAPHIC KEY GENERATION", 2007 Biometrics Symposium,IEEE-2007

[6] Yi Wei and M. Brian Blake, University of Notre Dame, "Service-Oriented Computing and Cloud Computing Challenges and Opportunities", Published by the IEEE Computer Society November/December2010

[7] Tharam Dillon, chen.wu, change Digital Ecosystems and Business Intelligence Institute Curtin University of Technology Perth, Australia, "Cloud Computing: Issues and Challenges ", 2010 24th IEEE International Conference on Advanced Information Networking&Applications

[8] Michael Kretzschmar and Sebastian Hanigk Universität der Bundeswehr München, Institut für Technische Informatik, Werner-Heisenberg-Weg 39, 85577 Neubiberg, Germany "Security Management interoperability challenges for Collaborative Clouds", 2010 4th International DMTF Academic Alliance Workshop on Systems&Virtualization.Management

[9] Abhishek, utkarsh chaurasiast, badrinathojha, rajeevranjanshahi, Indian Institute of Information Technology, Allahabad U.P India. "3 Dimensional Security in Cloud Computing" 2011 IEEE.

[10] Lifang Wua,b Songlong Yuana aSchool of Electronic Information and Control Engineering, Beijing University of Technology, Beijing China 100124 Dept of Computer science and Engineering, State University of New York at Buffalo, Buffalo, New York USA 14260," A face based fuzzy vault scheme for secure online authentication", 2010 Second International Symposium on Data, Privacy, and E-Commerce

[11] V. Evelyn Brindha Associate Professor, Dept. of CSE., Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India. "Biometric Template Security using Fuzzy Vault", 2011 IEEE 15th International Symposium on Consumer Electronics

[12] Scott Dowell Computer Sciences Corporation San Diego, CA, USA. Albert Barreto III, James Bret Michael,and Man-Tak Shing Naval Postgraduate School Monterey, CA, U.S.A"Cloud to Cloud Interoperability", Proc. of the 2011 6th International Conference on System of Systems Engineering, Albuquerque, New Mexico, USA-June-27-30,2011

[13] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li."Biometric Template Security using Fuzzy Vault", 2011 IEEE 15th International Symposium on ConsumerElectronics

◈◈◈