World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 196-201
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

P. Selvarani
Research Scholar, Computer Science and Engineering
Vel Tech Dr. RR & Dr.SR Technical University, Avadi, Chennai, India

N. Malarvizhi
Associate Professor, Computer Science and Engineering
Vel Tech Dr. RR & Dr.SR Technical University, Avadi, Chennai, India

Correspondence:
P. Selvarani
Research Scholar, Computer Science and Engineering
Vel Tech Dr. RR & Dr.SR Technical University, Avadi, Chennai, India

To Enhance the Data Security in Cloud Computing Using Multimodal Biometric System

P. Selvarani, N. Malarvizhi

Abstract
To achieve higher data security in cloud computing Multimodal bio cryptography techniques can be used for data encryption and decryption to avoid the intruders to access the data. In multimodal biometric system combining both fingerprint and iris is used. The key is derived directly from the fingerprint and iris used as a key for encrtyption and decryption algorithm in cloud. In existing cloud environment password based authentication is used as a key for encryption and decryption. The intruders can easily break the password and able to access the data in cloud environment. To overcome this difficulty multimodal biometric technique can be used a key to secure the data in the cloud environment. In our research work implementation of Multimodal Biometric system is used as a key for encryption and decryption of data in the cloud environment. This approach is implemented using language of C. It can generate variable size key with minimum time complexity and higher security which is aptly suited in real time cryptography. Only authorized person will access the data.

Keywords: Cloud Computing, Data Security,Fingerprint Recognition, Iris Recognition, Cryptography, Multimodal Biometric Authentication.

Introduction
Cloud computing is an emerging computing technology that uses the internet and central remote servers to maintain data and application. Data security becomes more and more important in cloud computing. Cloud computing provides the way to share distributed resources and services that belongs to different organizations or sites. Since cloud computing share distributed resources via network in the open environments they it makes security problems. The data must be encrypted and kept safe with a highly-monitored and regulated access. Due to inherent multi-tenancy and ease of access within a cloud, the data is subjected to various security risks, which continues to be a serious concern.

The user authentication, which is an main part of the cloud computing, determines only the authorized user is to access the data.In existing system they used password based authentication.Password= Secret authentication code used for access.but many of the limitations having password based authentication:Simple pass word easy to guess / crack. Complex passwords are difficult to remember. Most of the people use same password across in different applications and thus, if single password is compromised so the hacker can access all the data. Passwords are unable to provide nonrepudiation, that is, Password is shared with a friend, and there is no way to know who the actual user is. So better security is provided need to protect the data from unauthorized users. Biometric based authentication can replace the password based authentication, because, Biometrics is more reliable than password based authentication. As biometric characteistics cannot be lost, forgetten, that are extremely difficult to copy, share and distribute. The person is to be present at the time of authentication. It is difficult to forge biometrics. Each physiological or behavioral feature can be used as a biometric characteristic for personal identification processes as long as they fulfill the following requirements:

Universality	Every person has to have this feature
Uniqueness	No two or more people with the same feature must exist
Constancy	The feature does not change significantly in the course of time.
Collectability	The feature must be measurable or collectable
Permanance	identification are uniqueness and persistence

Table 1: Requirements on a Biometric System

Biometric technology identifies the user based on behavioral and psychological features for added security. In Physiological features like Fingerprint, Iris, Hand Geometry, Face Recognition, DNA Etc. Behavioral Features like Keystroke, Voice and Handwritten Signature. There are 2 types of biometric system. Unimodal and Multimodal biometric system. In Unimodal Biometric System single biometric sample is used to recognize a user Eg: (iris/fingerprint/retina scanner/face/palm) any one of them used. of sensitiveness to noise, intraclass consistency, non-universality, lack of individuality, Susceptibility to circumvention etc. To overcome this difficulty multimodal biometric technique can be used. Multimodal Biometric System: 2 (or) more biometric sample can be used from the same person to verify an identity. Eg: (Fingerprint & Iris, Fingerprint & facial recognition/Dynamic signature verification) any combination of the above. Biometric system consists 3 steps: Enrollment Storage and comparison. (i) Enrollment: First time user can use a biometric system. It record the basic information about the user like name or id no. Then captures an image of your specific trait. Biometric sensor that detect the characteristic being used for identification. (ii)Storage: A computer that read and store the information. Software that analyze the characteristic and translate it into a binary code and perform the actual comparisons. (iii)Comparison: Next time user can use the biometric system. It compare the trait. User can present to the information on file then it either accept or reject. Multimodal biometric system can also several advantages over unimodal biometric system.

Multimodal Biocryptographic technique

In our research work proposed Multimodal biocryptographic technique like fingerprint and iris can be used as a key for data encryption and decryption in cloud environment. (Figure 1 & 2).

Fingerprint and Iris which are stable, unique, unchanged, no two people can have the same exact fingerprint or iris pattern and security level is also very high.

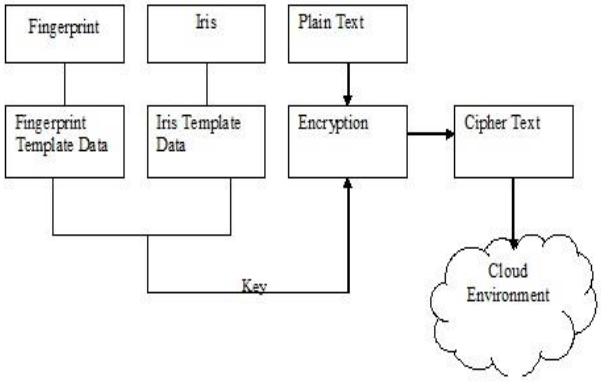

Fig. 1: Multimodal Biometric Technique using Encryption.

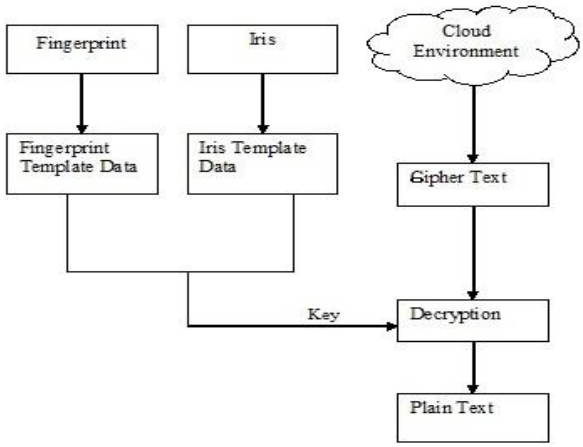

Fig. 1: Multimodal Biometric Technique using Decryption.

Cryptography technique: the original text is converted into ciphertext using encryption key. The cipher text is converted to original key along with only decryption.Our proposed work using biocryptographic technique like fingerprint and iris is used to enhance the security level and to protect the data from unauthorized users.

Workflow of Fingerprint

Fingerprint: Fingerprint is one of the secured biometric technology. Fingerprint based on key, It is an individual characteristic; no two people have been found with the exact same fingerprint pattern; A fingerprint pattern will remain unchanged for the life of an individual. Fingerprints have general characteristic ridge patterns that allow them to be systematically identified.

Working Flow of Fingerprint Process

Fingerprint systems can provide three main functionalities namely Enrollment, Verification, and Identification.

(i) Enrollment Process:

The system captures the Fingerprint data from an enrollee with sensing devices, extract features from the finger data and then record them as template with a personal information. Eg: PIN.

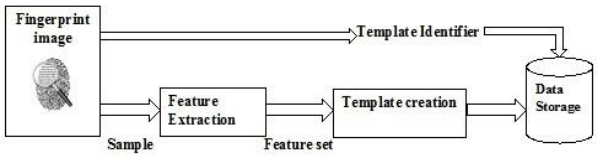

Fig. 3: Enrollment of Fingerprint Process.

(ii) Biometric Verification (1:1 Matching)

The user input which is matched against the enrolled biometric data corresponding to the ID.Identification or Verification process, the system capture finger data from a finger with sensing devices, extract features, identifies the features by comparing with template in the database, and then output a result as “Acceptance” only when the features correspond to one of the templates.

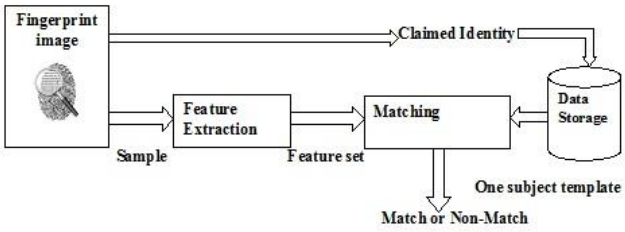

Fig. 4: Fingerprint Verification (1:1) Matching

(iii) Biometric Identification (1: N Matching)

The user only his/her biometric data, which is matched against all the biometric data in the database. (Convenience: High).

The user's input is compared with the templates of all the persons enrolled in the database and the identity of the person whose template has the highest degree of similarity with the user's input is output by the biometric system.

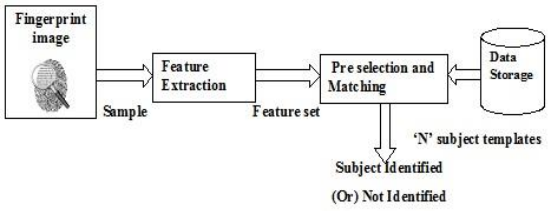

Fig. 5: Fingerprint Identification (1: N) Matching.

Eg: The user's input and the template of the claimed identity have a high degree of similarity, and then the claim is accepted as "genuine". Otherwise, the claim is rejected and the user is considered an "impostor".

Hence Therefore Multi biometric traits provide more security than traditional knowledge- based or token-based identification methods. Hence, they cannot be lost, stolen, shared, or forgotten.

Workflow of Iris

Iris is the one of the most secured and accurate biometric identification system. Iris has been preferred due to accuracy, reliability, simplicity and high security compared to other biometric system. The iris image is first captured localized for further feature extraction and segmented into binary code. Iris is then compared to a template in the system to be if a match can be found[1].

Enrollment: The iris image is captured using iris sensor. There are 4 stages of iris recognition.(i) Segmentation (ii) Normalization (iii) Encoding (iv) Matching.

Iris recognition: The performance of iris recognition system depends on segmentation and normalization technique.

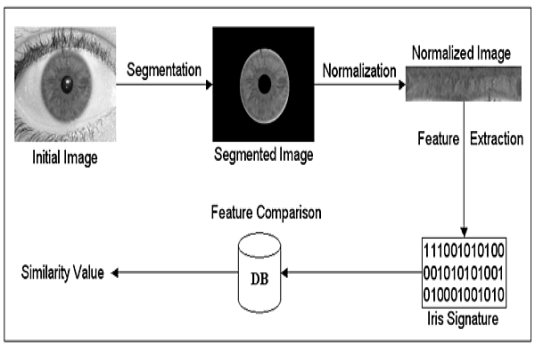

Fig. 6: Iris Recogniton

Segmentation: Iris segmentation is main part of the iris recognition system. Segmentation is a process the acquiring information from an iris image.The information of eye is foused on iris part and other part as ignored for the purpose of iris accuracy. Because accuate boundaries are needed to normalize and match iris image with the database. Hough transform and Daughman's Integro-Differential operator is used to segment the iris.

Normalization: In the normalization technique the image of iris is gathered by reducing the errors and a rectangular shape of segmented iris is produced. The output of normalization technique is stored into the database into two forms. Pixel values and iris code. Normalization refers to prepare the segmented iris image for the encoding process.

Encoding: Iris code is generated and it is stored in the database is useful for verification /matching system.

Matching: The final step is matching the iris code by using iris feature stored in the system. The matching is carried out by measuring the distance between two images of iris code. Hamming Distance is used to measure the distance between two iris code.

Fingerprint and iris identification system extreamly reliable, stable and useful for security applications.

Table 2: Description of Fingerprint and Iris

BIOMETRIC DESCRIPTION	FINGERPRINT	IRIS
How Does work	Analyzes fingertip patterns	Analyzes features of colored ring of the eye.
Devices Required	Scanner	Camera
Accuracy	High	High
Cost	Medium	High
Universality	Medium	High
Uniqueness	High	High
Permanance	High	High
Collectability	Medium	Medium
Advantages	Mature technology	Fast Processing
	Easy to use/ non-intrusive	Nearly Non-intrusive
	High accuracy	High accuracy
	Long term stability	Long term Stability
	ability to enroll multiple fingures	Highly protected

Related Work

Related works Several approaches have been developed for multimodal biometric system using key generation of fingerprint and iris.

[2] High level of security is reciprocally proportional to system performance and maintenance cost. Hence, if all data storages have to be provided with the highest level of security, it would degrade the performance of the system. So here we have proposed a framework to provide appropriate level of security to different data according to their class of sensitivity with respect to confidentiality, integrity and authenticity

[3] Hence we proposed a method for generation of cryptographic key which is generated using biometrics. Here we used fingerprint patterns, which are stable throughout person‟s lifetime. The key is derived directly from the biometric data and is not stored in the database. Since it creates more complexity to crack or guess the crypto keys. This approach has reduced the complicated sequence of the operation to generate crypto keys as in the traditional cryptography system.

[4] An efficient approach for generation of secure cryptographic key based on multimodal biometrics (Iris and

fingerprint) has been presented in this paper. The proposed approach has composed of three modules namely, 1) Feature extraction, 2) Multimodal biometric template generation and 3) Cryptographic key generation. Firstly, the features, minutiae points and texture properties have been extracted from the fingerprint and iris images respectively. Then, the extracted features have been combined together at the feature level to obtain the multibiometric template. Lastly, a 256-bit secure cryptographic key has been generated from the multi-biometric template. For experimentation, we have employed the fingerprint images obtained from publicly available sources and the iris images from CASIA Iris Database. The experimental results have demonstrated the efficiency of the proposed approach to produce user-specific strong cryptographic key.

[5] Hao et al., have presented a biometric based cryptographic key generation method utilizing the iris feature. They generated key, which were created reliably from a legitimate iris codes and hence achieved a 99.5% accuracy rate. They generated up to 140 bits of biometric key that is adequate for a 128- bit AES.

[6] Uludag et al., presented several techniques that monolithically combined a cryptographic key with the biometric template in some manner the key cannot be exposed without a valid biometric authentication. Cancellable biometrics gives a better performance of security as it facilitates with more than one template for the same biometric data.

[7] An efficient approach for the secure PKI key generation on the idea of multiple modalities Iris and fingerprint Therefore fingerprint and Iris-based PKI key generation algorithm is possible. Finger print and Iris feature code eventually generates prime range that shows no periodicity, therefore the attackers nearly impossibly found the regularity of cryptographic key to crack.

Problem Statement

Cloud data can be attacked in two ways. Insider attack and outsider attack. Insider as an administrator can have the possibility to hack the user's data. Insider attack is very difficult to be identified. So the users should be very careful while storing their data in cloud storage. Even though the data is accessed by the third party, they shouldn't get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage. The problem is while storing the data in cloud environment using password system is, it is not secured, forgotten and easily stolen. Hackers can able to trace the password through keystroke loggers and spyware. In existing method Usually unimodal biometric techniques are used. The existing unimodal bio cryptography techniques often face limitatins such as consciousness to noise, intra class consistency, data aspect, and other factors. In multi-model biometric system it is not possible to hack the data by the intruders. Biometric based Blowfish algorithm is used for both encryption and decryption. Combined biometric of both fingerprint and iris is used for protect the data from unauthorized users.Cryptography is a technique applied for encryption and decryption.

Proposed System

Initially we apply preprocessing for feature extraction from each biometric image. Then the fusion of feature level both fingerprint and iris are used for encryption.

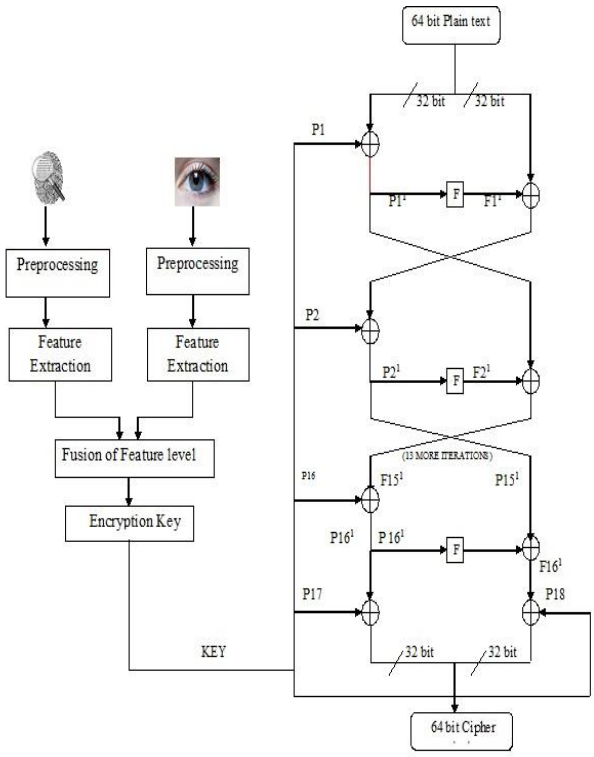

Fig. 7: Block diagram of Biometric based Blowfish Algorithm**.**

In our proposed work we mainly focus on data security on cloud. To provide data security we use bio cryptographic technique such as fingerprint, iris and secret key. Because bio-cryptographic framework, as a safer authentication mechanism for Cloud storage sharing. Blowfish algorithm for Encryption and Decryption can be implemented to enhance security framework over the network. Biometric based Blow fish algorithm is the better result algorithm which is used to secure the cloud data.

Blowfish Encryption Algorithm

Blowfish algorithm is designed in 1993 by Bruce Shnier and it is included in a large number of cipher suites and encryption products. It take variable length key from 1-448 bits. It has 16 rounds. Each round consists data dependent permutation and data dependent substitution.

Design feature of Blowfish algorithm: Blowfish is a symmetric key (same key) block cipher. It is replacement for IDEA /DES.

Platform	Cloud Computing	*Encryption*	More than 2^{32} data blocks
Designed	1993	*Key used*	Used Same key- Data Encryption & Decryption.
Author	Bruce Schenier	*Memory usage*	4 KB of data can be processed
Block Size	64 bit	*Execution time*	Lesser time to execute and reduce the time for data encryption and decryption
Key size	1-448 bits	*Authentication type*	Comparable to AES
No of rounds	16	*Usage*	Replacement for IDEA/DES. It is Unpatented, License free and it is available for all users.
Initial vector size	64 bits	*Security*	Secure for both cloud provider & user/Client side.
Network	Feistel	*Comparable to other algorithm*	It is significantly faster than DES. Very fast, Highly secure.
Possible keys	2,322,448	*Attack*	No Attack
Speed	Very fast	*Scalability*	Scalable

Blowfish algorithm handles 2 parts of the data. Expansion of the key and Encryption of the data.

The expansion of key: Split the original key into set of sub keys. Then the subkeys are combined with biometric templates. Specifically a key is no more than 448 bits is separated into 4168 bytes. The P-array contains 18-32 bit sub keys while each S-box contains 4 blocks of 256 entries.
S1,0, S1,1,..., S1,255;
S2,0, S2,1,..., S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..., S4,255.

S-box accept 8 bit input and produce 32 bit output.

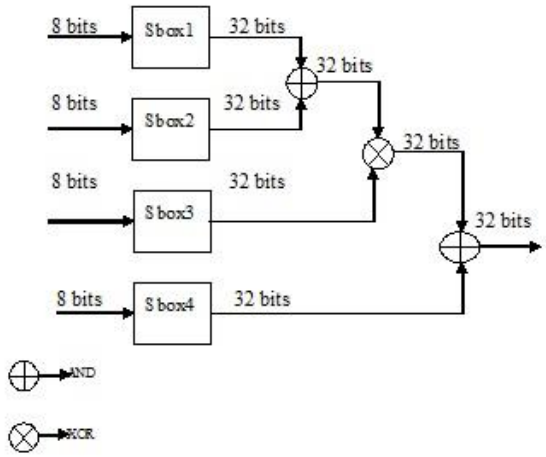

Fig. 8: S Box Function

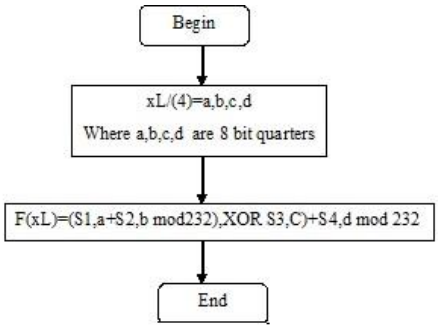

Fig. 9: F Function

Encryption of data: 64 bit input is denoted with an x, While the P-array is denoted with Pi (Where i is the iteration).
Divide x into two 32-bit halves: x**L**, x**R**
For i = 1to 16:
X**L**= X**L** XOR P**i**
x**R** = F(X**L**) XOR x**R**
Swap X**L** and x**R**
Next i
Swap X**L** and x**R** (Undo the last swap.)
x**R** = x**R** XOR P**17**
x**L** = x**L** XOR P**18**
Recombine x**L** and X**r**

4.2 Cryptographic Technique used in cloud data security.

Encryption: Initially we apply preprocessing for feature extraction from each biometric image. Then the fusion of feature level both fingerprint and iris are used for encryption key for blow fish algorithm. The output of the blow fish algorithm is cipher text which is stored in the cloud environment. The intruders cannot able to read the cipher text in the cloud environment.

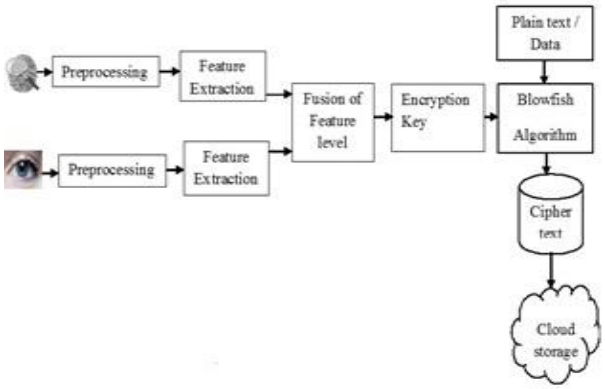

Fig. 10: Data Encryption in Cloud

Decryption: The data from cloud is accessed by corresponding user by a secret
key which is framed by the combined bio-metric of Finger print an Iris for decryption. The user will get the original message after decryption. The data can be protected from unauthorized users.

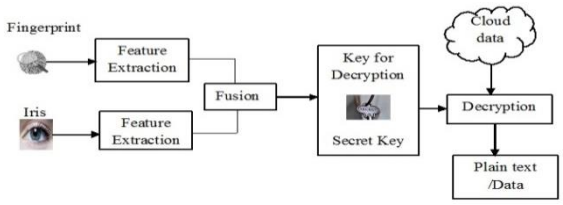

Fig. 11: Data Decryption in Cloud

Result
To achieve high data security we can use combined biometrics with cryptographic technique using blowfish algorithm. To protect and secured the high security data from unauthorized users in cloud environment. Only authorized person will access the data.

Fingerprint	3456785642359abcaf457ab
Iris	F986e745a4b31d2caf23456
Key	55 dd 0 52 f 1 3 55 6 8 5 50 0 0 0 6 6 3 54 54 0
Plaintext message string is	Fingerprint and iris based data encryption
Encrypted message string is	4459b558361b835a69ec2f94a689bb4b499de 72220a48fb98045dabce5a7dfc635afe53f8b2 035c35621ddbba5be0c8e
Decrypted message string is	Fingerprint and iris based data encryption.

Conclusion

The cloud Computing is a hopeful technology To protect the data from unauthorized users in our proposed work using multibiometric like fingerprint and iris is used for higher accuracy and more data security. In our proposed work introduce a new and novel implementation of biometric based blowfish algorithm gives as high security and more accuracy and reduce the time of data encryption and decryption. The combination of Finger print and Iris form the key for biometric based algorithm to store the secured data from unauthorized users in cloud environment. Thus by implementing biometric based blowfish algorithm in cloud environment cloud data can be secured.

References

1. Daugman. J (2009). How iris Recognition Works. The Essential Guide to image Processing, 14(1), 715-739. Doi:10.1016/B978-0-12-374457-9.00025-1.
2. The Consultative Committee for Space Data Systems, Encryption Algorithm Trade survey, Information report, CCSDS 350.2-G-1, Green Book, March, 2008.
3. Reference: Dr. R. Seshadri, T. RaghuTrivedi"Efficien Cryptographic Key generation using biometrics" international journalof Comp.Tech.Appln,Vol 2(1), 183-187.
4. A. Jagadeesan and Dr. K.Duraiswamy "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris "(IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
5. F. Hao, R. Anderson and J. Daugman, "Combining crypto with biometrics effectively", IEEE Transactions on Computers, Vol. 55, Pp. 1081-1088, 2006.
6. U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, "Biometric cryptosystems: issues and challenges", Proceedings of the IEEE, Vol. 92, No. 6, Pp. 948 – 960, 2004.
7. A. Jaya Lakshmi* Et Al. "Pki Key Generation Using Multimodal Biometrics Fusion Of Fingerprint And Iris "International Journal Of Engineering Science & Advanced Technology, Issn: 2250–3676 Volume-2, Issue-2, 285 – 290.