iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XII **Month of publication:** December 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Preserved Biometric Cloud Password Manager

Kavita V. Shingi [1], Prof. S. G. Tuppad[2]
Computer Science and Engineering, MSS's CET, Dr. Babasaheb Ambedkar Marathwada University

Abstract: Living in informative world takes you to numerous technologies growing day by day. While dealing with those require to handle personal, professional and other information. Security of such information is provided by locking it with username and password. Since inconvenience held to memorize numerous passwords, a new technology is required to handle those security dilemmas. Password manager worked as an assistant to memorize, store sensible data. Depending upon data storage whether on system or cloud password managers are categorized into two parts: Offline and Online password manager respectively. Both reside on a single master key to secure stored data in most of the password manager application. Access to master key give access to all web services accounts of user thus biometric password manager came into existence. Still the security of biometric template is one of the concerns since abuse of template will not be able to regenerate new template for any user. To provide security to biometric features to maintain uniqueness of his/her biometric trait numerous technology are mentioned in few years. In this paper a slightly different way is proposed to secure data belonging to biometric cloud password manager.

Keywords: Cloud Computing, Password Manager, Biometric Template, Hashing, AES, Chunks

I. INTRODUCTION

We are living in Informative world were in day to day life we deals with number of web services and handling sensible data in this system is currently very usual. Which data is to be considered sensible is up to the application. We can say that personal data, financial data, as well as access control data may be sensible for most of the system. Actors dealing with such Information Systems like Clients/Users, Service Provider, Integrators, Third-Party Providers and many more have to be aware of all the security threats occurring in the system and level of security archived within the system [7]. Clients for such systems could not be technical person at every time. Considering for technical or non-technical users memorizing passwords of different web services (specially having more than 4 or 5 accounts) is quietly difficult. Keeping same password for all web services are harmful, since access to password will give access to all the web services. Thus in most of the cases various web service provider suggest to keep different passwords for different web services and the level of passwords must be strong (e.g. keeping capital letter, small letter, number, special character etc.). Apart from this many researcher proposed technique to use some unique number, secure chip like smart cards etc. [6]. Residing on such Identity Cards, Personal Identification Number (e.g. pan number) cannot be beneficial because they can be stolen or hacked. Thus a password manager is designed to reduce human efforts of memorizing various passwords and giving freedom from keeping identity cards.

There are many password managers are available like lastpass, keepass, Roboform, Dashlane, M2SYS etc. There are several methods used to implement password manager such as storing passwords in the form of plain text or in encrypted form using cipher (e.g. master key, a password used to login to managers), using biometric authentication, or using two way authentication by means of a master key and biometrics. Such managers based on master key are risky since leakage of master key from client or service provider side can give secret information to adversary which can use by attacker to impersonate legitimate user. M2SYS uses biometric authentication methodology but the way this product protect biometric information is unknown [1]. In a proposed system a two way authentication method is used. A preserved biometrics are used to preserve data belonging to a single user of different web services, such as username, passwords, domain name etc. in encrypted form.

II. RELATED WORK

Bio means life and metrics means measurements. From last few years, there are so many systems are available in the market which uses Biometric phenomenon for authorization, authentication purpose. Human has too many features which identify one uniquely [12]. These features are categories into two parts:

A. Physiological Characteristics
B. Behavioral Characteristics

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

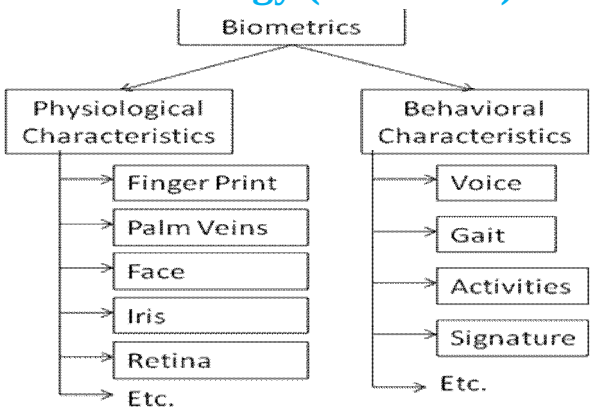


Figure 1: Classification of Biometric Features

In order to understand successful orientation of Biometric system understanding of classification of biometrics is very important for better utilization of techniques.

Work of the proposed system is based on fingerprint, which is commonly used in most of the biometric system. Crossover, core, bifurcation, ridge endings, island, delta, pore, valleys etc. total eighteen different types of features can be extracted from fingerprint impression collectively called minutiae. Commonly ridge endings and bifurcations, as shown in figure, are extracted from the gray-level input fingerprint image A three dimensional feature vector [x- coordinate, y- coordinate, the local ridge direction] is computed from each of the two features at the feature location, which is used to derive many other features. Using 3×3 pattern masks minutiae are detected for elimination of false detected minutiae. After a successful extraction of minutiae they are stored in a template. Feature extraction and matching contains processes like preprocessing, feature extraction, matching algorithms, compression of fingerprint images and special purpose architectures. Depending on all stages are carried or not, what kind of input is supplied, how is the local ridge direction computed, steps of preprocessing or enhancement, approaches to binarization or segmentation, thinning operators used, involvement of post-processing stage and performance evaluation various approaches get compared. Comparison of methodology used by Coetzee, Hung, Mehtre, O'Gorman, Sherlock, Xioa, Ratha is mentioned in [8].

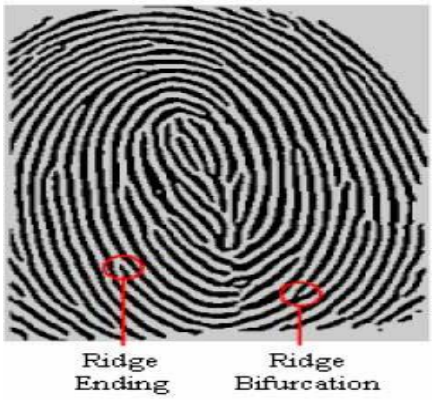


Figure 2: Features Commonly Extracted from Fingerprint Impression

Biometric is the only single solution to provide highest security to any system as it is expected to be kept the same during whole life of a human being. While a private key can be changed as desired and even cancelled but person cannot change his/her bio measurements (e.g. Fingerprint) unless changing it physically or even cancel it. Therefore, biometric systems have to be kept as secure as possible. Numerous vulnerabilities are present in any biometric system and all those have to be considered while designing biometric solution. Some of them are described here:

1) User's attitude is one of the concerns. An authorized user can provide his/her own biometric sample to an imposter knowing/ unknowingly, willing/ unwillingly.

2) Capturing device front end, such devices may not be able to detect a non-live sample, the quality of the input sample under determined threshold, degradation of its own degradation, protect the quality threshold against manipulation, resist

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

environmental factors, eliminate residual information from previous captures, deny successive and fast sample presentation, discard sample injection.

3) Capturing device back end, potential loss of captured biometric sample. Captured sample could be interpreted and/or rejected to provide replay attack and hill climbing attack can be done on captured sample by injecting successive biometric samples.
4) Viruses, Trojans, Communication interception, Data injection etc. are common concern in every IT industry. During concerns for this kind of threat sensibility related to biometric information covers not only the sample data, templates and feature vectors but also algorithms, thresholds access logs.
5) Result given by the system, this vulnerability is considered since attacker can use the information provided by the system in the form of result. Since matching result may include not only success or failure of algorithm but also about the percentage of matching acquired. This could be used to build an artificial sample [17].

Before proceeding how to secure template the property that biometric template must satisfy are: Non-invertibility or irreversibility of template to prevent from misuse, Revocability or Renewability to make possible to reissue new instances of template if stored data compromised, Non-linkability or Unlinkability to prevent cross-matching across different software. Numerous techniques are available for template protection to ensure all without compromising on performance. Proposed techniques in the literature stored data into two parts, pseudonymous identifier (PI) and auxiliary data (AD) [4]. Computation of these two components categorizes protection techniques as feature transformation or biometric cryptosystem. Feature transformation like biohashing, cancelable biometrics, robust hashing use one way function to transform biometric template. Transformed data and transformation parameter are stored as PI and AD respectively. While authentication a same transformation function is applied on queried template to generate PI' and compared with stored PI. In Biometric cryptosystems a secure sketch, obtained by binding template with error correcting codeword, is referred as AD and biometric hash is stored as PI called vaults. While authentication regenerated template used to obtain PI' and compared with stored PI. Both techniques have advantages as well as some limitations. To overcome those limitation templates are transformed using feature transformation function before applying biometric cryptosystem called hybrid cryptosystem [6].

III. IMPLEMENTATION

The proposed system architecture is shown in Figure 1. Figure shows number of steps carried while authorization and authentication. There mainly three steps are carried out:

A. Template Extraction

Template is a compact representation of the sensed biometric trait containing salient discriminatory information like minutiae position (x,y), direction (angle), type (bifurcation etc.) or quality. These templates are then used to store onto a database for application use [4]. Here concept explained below is used for extraction with reference to [8].

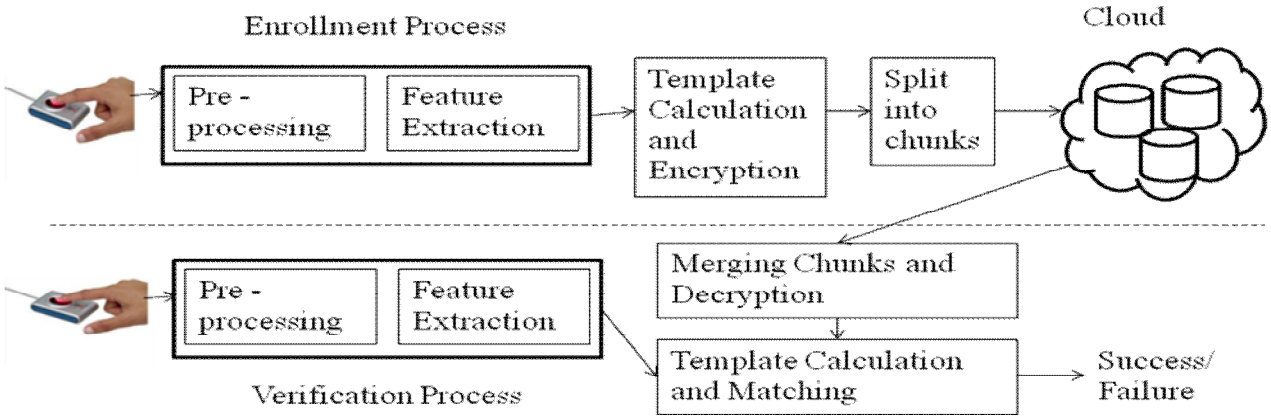


Figure 3: Architecture of the System

Viewing fingerprint images as a textured image, an orientation flow field is computed. The rest of the stages in the algorithm use the flow field to design adaptive filters for the input image. To accurately locate ridges, a waveform projection-based ridge segmentation algorithm is used. The ridge skeleton image is obtained and smoothed using morphological operators to detect the features. A large number of spurious features from the detected set of minutiae are deleted by a post-processing stage. The

significance of the observed Goodness Index values is determined by comparing the index for a set of fingerprints against the GI values obtained under a baseline distribution. The detected features are observed to be reliable and accurate [8].

B. Encryption

Now templates are used as helper data for encryption. An industry-standard high grade Advanced Encryption Standard (AES) symmetric encryption algorithm with key length of 256-bits is used for encryption. There are four steps for AES explained over [16].

1) *SubBytes:* A non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).
2) *ShiftRows:* A transposition step where each row of the state is shifted cyclically a certain number of times.
3) *MixColumns:* A mixing operation which operates on the columns of the state, combining the four bytes in each column.
4) *AddRoundKey:* An each byte of the state is combined with the round key each round key is derived from the cipher key using a key schedule.

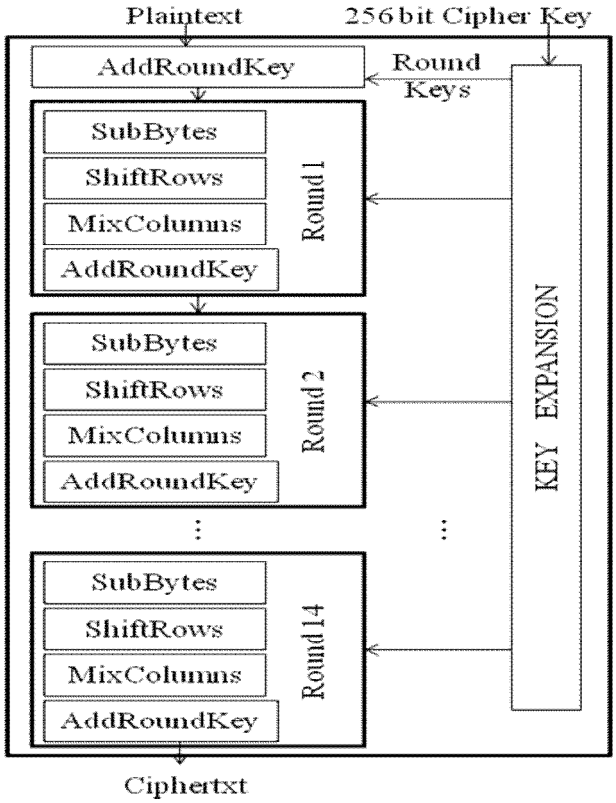


Figure 4: AES-256 bit Encryption Procedure

As the key size used for an AES cipher is 256 thus the number of repetitions of transformation rounds that convert the input (plaintext) into the final output (ciphertext) is 14 [16]. The cipher and inverse use some components which eliminates the possibility for weak keys in AES which is an existing drawback of DES. AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's. Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance. This algorithm has speedy key setup time and good key agility. It requires less memory for implementation, making it suitable for restricted-space environments. The structure has good potential for benefiting from instruction-level parallelism. There are no serious weak keys in AES. It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits). Statistical analysis of the cipher text has not been possible even after using huge number of test cases and there is no differential and linear cryptanalysis attacks have been yet proved on AES.

C. File Distribution Preparation

Now, in the last stage where data is ready to store on to cloud is distribution into chunks. Helper data encoded using AES algorithm

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

is splitted into N chunks

$$Chunks=F/N \quad (1)$$

In above equation F denotes file and N denotes no. of chunks.

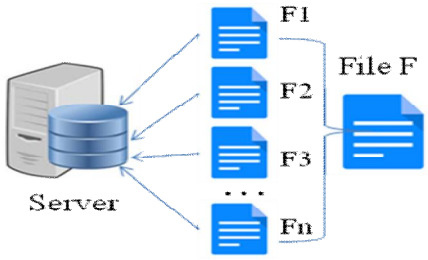


Figure 1. File Distribution to cloud Server

IV. EXPERIMENTAL ANALYSIS

The well known fingerprint databases are available in public domain called Fingerprint Verification (FVC), FVC2002, FVC2004, FVC2006 (DB1, DB2, DB3, DB4) on website. Each database contains sample of 100 users and 8 samples of each user. Comparison is adopted using two tests: For first test, first and second fingerprint impression of each user is compare with one another and for second test, first fingerprint impression of each user is compare with 8 fingerprint impression of each of them. Due to the relatively good image quality, matching received 100 score from analysis for comparison of first and second impression of the same trait. From the comparison of one with eight other samples of same trait failure is shown for score less than 75.

Popular encryption algorithm AES-256 is used to encrypt helper data and stored on cloud in the form of chunks. While authentication process, decryption of data is done on client side if the sufficient matching score is acquired as input. Following figure shows the average time taken to encrypt and decrypt data. It can be noticed from the chart that not all the modes have been tried for all the algorithms. Nonetheless, these results are good to have an indication about what the presented comparison results should look like.

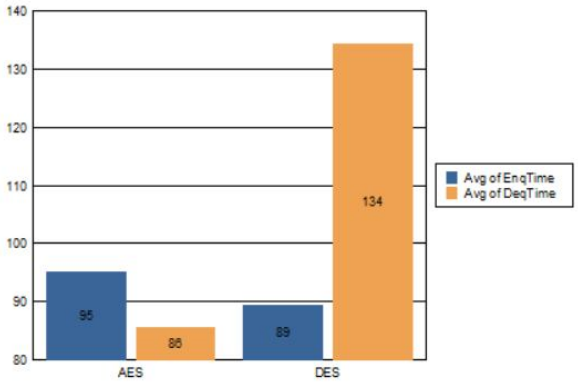


Figure 5: Result comparison of AES and DES with Average Encryption or Decryption Time

V. CONCLUSION

We investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage especially biometric data, we proposed an effective and flexible distributed system with explicit dynamic data support. The biometric helper data is encrypted using advanced encryption standard, so data is successfully and securely stored on cloud. The handling of some security issues like Fast error localization, data integrity, data security. Our design allows users to audit the data with lightweight communication and computation cost. Analysis shows that proposed system is highly efficient against malicious data modification attack and server colluding attack. Performance and extensive security analysis shows that proposed systems are provably secure and highly efficient.

VI. ACKNOWLEDGMENT

Foremost, I would like to express my sincere gratitude to my advisor Prof. S. G. Tuppad for the continuous support of my M.E. dissertation work, for her patience, motivation, enthusiasm and immense knowledge. My sincere thanks also go to Principal of the institute Dr. C. M. Sedani MSS's CET Jalna, Head of Department, M.E. coordinator, all teaching staff of the Computer science and engineering department for supporting me spiritually throughout my project work.

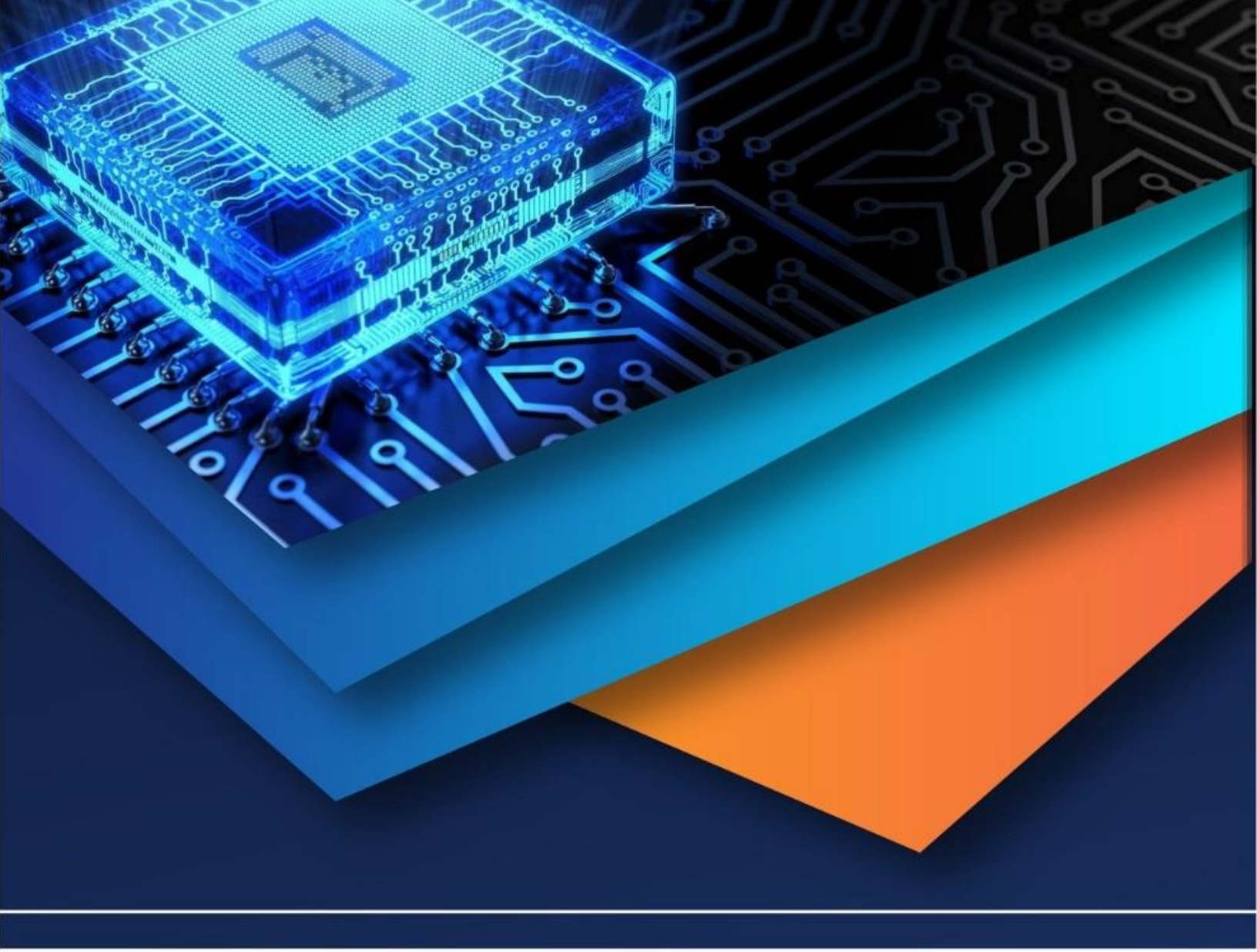
REFERENCES

[1] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch, "Cloud Password Manager Using Privacy-Preserved Biometrics", IEEE International Conference on Cloud Engineering, 2014.
[2] D.Pugazhenthi ,B.sreevidya, "Multiple Biometric Security in Cloud Computing", IJARCSSE, Volume 3, Issue 4, April 2013.
[3] Ching-Nung Yang, Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", International Symposium on Biometrics and Security Technologies, 2013.
[4] Anil K. Jain, karthiknandakumar, and Abhishek Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing Volume 2008.
[5] "www.circuitstoday.com//Working of Fingerprint Scanner - Electronic Circuits and Diagram-Electronics Projects and Design"
[6] Karthiknandakumarand Anil K. Jain, "Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice", IEEE Signal Processing Magazine, Special Issue On Biometric Security and Privacy, Sept. 2015
[7] Praveen Tiwari, Ashis Saklani, "Role of Biometric Cryptography in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 70– No.9, May 2013.
[8] Nalini K. Ratha, Shaoyun Chen and Anil K. Jain, "Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, No-11 pp 1657-1672, 1995.
[9] A.A.Yassin, H. Jin, A. Ibrahim, D. Zou, "Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing," In proceedings of Second International Conference oncloud and Green Computing, 2012.
[10] S. Gaw and E. W. Felten, "Password management strategies for online accounts," Proceedings of the second ACM symposium on usableprivacy and security, 2006.
[11] C. Rathgeb, A. Uhl. "A Survey on Biometric Cryptosystems and Cancelable Biometrics," EURASIP Journal on Information Security, 2011(3), Springer Verlag, 2011.
[12] Christina-angelikitoli and Bart Preneel, "A Survey on Multimodal Biometrics and the Protection of Their Templates", IFIP International Federation for Information Processing 2015.
[13] Drm.Gobi and D.Kannan, "A Secured Public Key Cryptosystem for Biometric Encryption", International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014.
[14] Joseph Mwema, Michael Kimwele, Stephen Kimani, "A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates", International Journal of Computer Trends and Technology (IJCTT),Volume 20, Number 1 – Feb 2015
[15] A. Juels and M. Wattenberg, "A fuzzy commitment scheme", in proceeding of 6th ACM Conference on Computer and Communications Security (ACM CCS '99), pp. 28-36, Singapore, November 1999.
[16] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[17] S.Z. Li, A.K.Jain, "Encryption of Biometrics", Springer Science Business Media New York 2015

AUTHORS PROFILE

KAVITA SHINGI is a student of M.E. Computer Science and Engineering in MSS's CET Jalna. She is currently working on Dissertation work of part-II on Cloud Computing and Security.

S. G. TUPPAD is Assistant Professor in the Department of Computer Science and Engineering, MSS's CET, Jalna in Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. She obtained her M.E. (CSE) from Government College of Engineering Aurangabad, Dr. Babasaheb Ambedkar Marathwada University, Maharashtra, India.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY