ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Multimodal Security Mechanism Using Embedded System & Cloud Computing

Shalaka K. Saboo[1], Prof. Amit Zore[2]

M.E. Student, Dept. of Computer Engineering, DPCOE, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, DPCOE, Pune, India[2]

ABSTRACT: Biometric systems are an integral part of physical access control systems. Biometric systems used in driver's license ,passport, password ,personal identification number, ATMs, voting system, aadhar card, attendance management system etc. The biometric systems use is increasing day by day because of low cost, scalable systems with high availability. In this paper a cloud based biometric system architecture is proposed, to make the system efficient and economical for remote enrolment. Biometric traits such as face and fingerprints are used and send them to cloud service by end-to–end encryption process. In this approach we combine the digital key with the biometric image to create bios crypt. These digital keys can be used as the cryptographic key. During the verification the biometric image is combining with bios crypt to retrieve the key for the encryption and decryption of the data. The cipher text is then uploading to the public cloud. And an authorized user can retrieve data by his digital key. This approach ensures the data integrity and confidentiality.

KEYWORDS: biometric system; encryption; decryption; key expansion; security; RSA; cloud service

I. INTRODUCTION

In today's world Security of computer data, information and computer networks has become very important. Biometric systems are a secure way to authenticate a person and to access to services or a system. Biometric systems are used to secure facilities and protect access to computer networks. The biometric systems are becoming ubiquitous due to the availability of low cost implementations but still the gap is there as the customer is demanding better and cheaper solutions.[1]Cloud computing is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. Cloud computing is a system for empowering ubiquitous, convenient, on-demand network access to shared & configurable computing resources. Cloud computing also known as on-demand computing.[2]The cloud based systems offer low cost, scalable and flexible solutions for next generation computing needs. In this research paper, a low cost architecture of biometric systems is proposed, which is using a low cost wireless enrolment node and the authentication is done by Biometric service hosted on the cloud.

1.1Biometric

A Biometric system is a technical scheme that uses data of a person to recognize an individual. Biometrics are the common answer to all the problems and it has been widely accepted. Positive identification of individuals is a very basic societal requirement. The user authentication is nowadays a very significant part of the web world. The value of authentic, user authentication is not restricted to just computer or network access. There are many other systems in everyday life, who also require user authentication, such as banking, e-commerce etc and could benefit from improved enhanced security. There are various types of the Biometric system like Finger print recognition, Face recognition, Speaker recognition, Iris recognition, DNA matching, Skin reflection, Foot print matching,…so on. Biometric security system is based on each and every individual's physical and behavioural characteristics.

Advantages of biometric security system are as follows:

a) Accurate authentication
b) Easy to use
c) Time saving
d) User friendly

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

1.1.1 Finger Print and Face Recognition based Biometric system

It doesn't require cost effective devices i.e. scanner while authentication. Face and finger print is used to reduce the spoofing attack of biometric.

- *Finger Print:*

Finger print module is required to scan the finger print which is not so costly. In case of finger print, comparison area is small with more information so accuracy is proper. Fingerprint identification remains as one of the most widely used and reliable biometric identification methods. Finger print consists of two parts one is lines and other one is space, lines are called as ridges and space between lines are called valleys. Finger print grows as a person grows but pattern doesn't change as the age change or change with time. It is a unique identity for each and every individual. Even pattern is unique for twins also.

- *Face*

Camera is required to capture the face for authentication. Face recognition is a process in which a portion of the person's face is photographed and the resulting picture is trimmed back to digital code. It is based on the location & shape of Facial Attributes like eyes, eyebrows, nose, lips, etc. Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication.

II. RELATED WORK

2.1 AES Basic

Advanced Encryption Standard (AES) developed by two Belgian inventors, one is Joan Daemen and another one is Vicent Rijmen in 2000. The Advanced Encryption Standard (AES) was announced by the National Institute of Standards and Technology (NIST) in November 2001. It is a symmetric block cipher which means that it works on fixed size of the block. The fixed size of the input bits is called as block. Symmetric key or Private key (same key) generation technique is used in encryption and decryption side. in AES Block cipher consists of two principles, one is diffusion and another one is confusion but AES based on confusion principle that means it doesn't change the number of block size bits only apply transformation to create confusion. It is works on principle of substitution & permutation network. Block size of AES is 128 bits which is fixed. There are three different key sizes of the AES 128, 192, 256 bits which is independent of the block size. AES divided into three versions depending on key size. Different versions have a different key size, round structure and same block size as follows.[4]

AES Version	Block Size (bits)	Key Size (bits)	No. of Rounds
AES- 128	128	128	10
AES-192	128	192	12
AES-256	128	256	14

Table 2.1Number of Rounds for different key size

2.2 Basic architecture of AES

AES is a round based algorithm. For encryption and decryption each round has four functions excepting last round. The last round operates on three major functions. The encryption algorithm has four round functions SubByte, ShiftRows, MixColumn and AddRoundKey. The decryption also contains the same number of rounds with reverse transformation, order of round function is different such as InvShiftRow, InvSubByte, AddRoundKey and InvMixColumn.The figure 2.1 represents the whole mechanism of basic AES encryption and decryption process.[4]

2.3 RSA (RIVEST-SHAMIR-ADLEMAN)

RSA developed in 1978, first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. It is based on asymmetric cryptography algorithm i.e. different key used for encryption and decryption purpose. One is called as public key and another one is called as private key. Public key is used to encrypt message and private key is used to decrypt message. Default key size of RSA is 1024 bits or 2048 bits. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

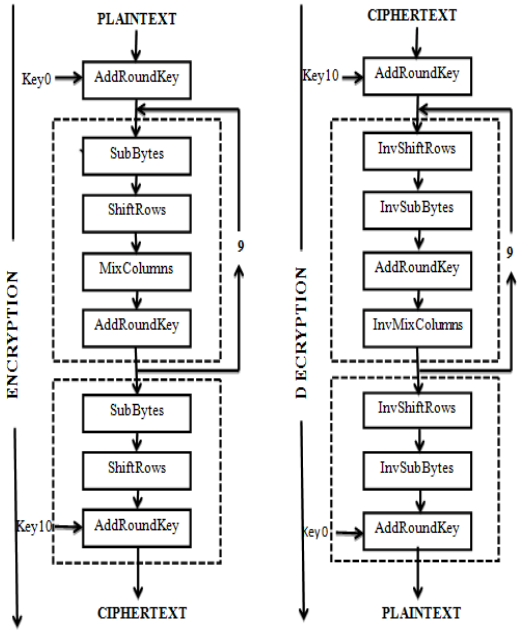

Figure 2.1 Architecture of AES

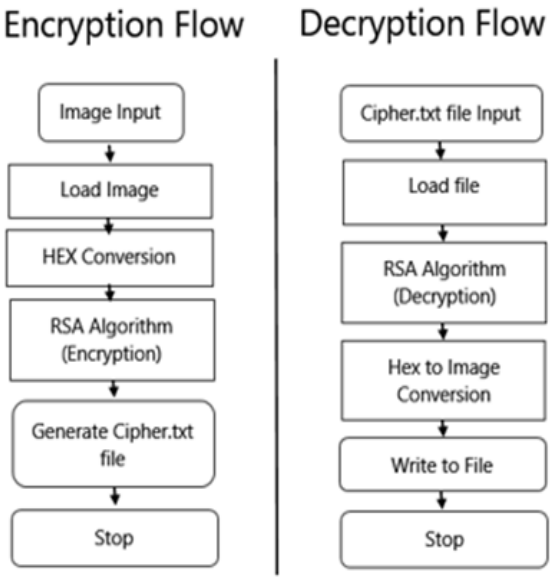

Figure 2.2 RSA Encryption and Decryption Flow chart

III. PROPOSED WORK

In this we perform a biometric based authentication to ensure that the user is an Authorized person. For the authentication purpose we use the physiological measurement as the encrypted image, here it is analysis of Fingerprint. So we can reduce the hardware cost for the registration. This generated image can be combined with a digital key and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

encrypt it to generate a bios crypt. This is uploading to the authenticating server. During the verification process both the encrypted images are compared without decryption. Here the Secure Matching Technology uses a unique algorithm to calculate the similarity between the registered data and authentication data even though they are in their encrypted format. It can ensure the security of the data even if the server were out sourced and also the system administrators also doesn't understand the original content of the data since they are not undergo any decryption.

Due to the presence of bios crypt we can assure the integrity and confidentiality of data. While uploading the data into the cloud we can classify it as whether it is a sensitive data or not. If the shared data is a sensitive one, we can encrypt the data with the bios crypt and upload to the public cloud. So only the owner has the right to read, write such type of data. Unless if the data is not confidential then we can upload it by performing encryption with the cryptographic key, which is similar to the mediated certificate less encryption.

Basic algorithm steps for face recognition:

1. Calculate a set of weights based on the input image and the M eigenfaces by projecting the input image onto each of the eigenfaces.

2. Determine if the image is a face at all by checking to see if the image is sufficiently close to "face space."

3. If it is a face, classify the weight pattern as either a known person or as unknown.

4. Update the eigenfaces and/or weight patterns. (Optional)

IV. CONCLUSION AND FUTURE WORK

In this paper we have proposed the biometric encryption scheme without pairing operations and provided its formal security. Our scheme solves the key escrow problem and revocation problem., we proposed an improved approach to securely share sensitive data in public clouds. Even though the system is secure against the active attack like data confidentiality and integrity and free from revocation and key escrow problem because of the biometric encryption and SEM mediators respectively I desired to include a new module to improve the security of data. I wish to embed the cipher text inside a noise and upload to the cloud. So when a attacker enter into cloud and try to modify the content, the actual content is not visible to him. They can only find the noise. We can use distributed systems to get better response time and time complexity. AI based algorithms can be used to improve accuracy of face recognition module.

REFERENCES

1. Omar Abdulwahabe Mohamad, Rasha Talal Hameed, Nicolae Tapus, " Access Control Using Biometrics Features with Arduino Galileo", International Journal of Advanced Research in Computer Science and Software Engineering, vol 4, issue 8, Aug 2014.
2. Hassan,Qusay(2011). "DemystifyingCloudComputing" (PDF). The Journal of Defense Software Engineering (CrossTalk) 2011 (Jan/Feb): 16–21. Retrieved 11 December2014.
3. Z. Xiao and Y. Xiao, "Security and privacy in cloud computing,"Communications Surveys & Tutorials, IEEE, vol. 15, pp. 843-859,2013.
4. Manoj. B, Manjula N Hariha"Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012
5. Eman Mohammed Mahmoud, Ahmed Abd El Hafez, Talaat A. Elgarf, AbdelhalimZekry" Dynamic AES-128 with Key-Dependent S-box" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1662-1670
6. M. A. Bamiah and S. N. Brohi, "Seven deadly threats and vulnerabilities in cloud computing," International Journal ofAdvanced Engineering Sciences and Technologies, Vol,(9), 2011.
7. T. Brooks, C. Caicedo, and J. Park, "Security challenges and countermeasures for trusted virtualized computing environments," in Internet Security (WorldCIS), 2012 World Congress on, 2012,pp. 117-122.
8. Y. Dai, X. Wang, Y. Shi, J. Ren, and Y. Qi, "Isolate secure executing environment for a safe cloud," in Communications inChina (ICCC), 2012 1st IEEE International Conference on, 2012