Implementing Enhanced AES for Cloud based Biometric SaaS on Raspberry Pi as a Remote Authentication Node

Dhvani. K. Shah
Information Technology
Thakur College of Engineering and Technology.

Vinayak Bharadi, PhD
Vikas Kaul
Information Technology Department
Thakur College of Engineering and Technology

Sameer Amrutia,
Amol Ambardekar, Phd
Technical Architect
JPMorgan Chase & Co.

ABSTRACT

Biometric systems are a vital part of physical access control systems. Biometric systems ensure that access to use a system or service is done by a valid user. These systems are used in various applications like ATMs, voting system, aadhar card, attendance management system etc. The biometric systems are in operation for a quite long time and their use is increasing. There is a requirement for low cost, scalable systems with high accessibility. In this paper a cloud based secure biometric system architecture is proposed, to make the system efficient and economical for remote enrollment on Raspberry Pi, which is a low cost computer running on Linux.

The system is capable of capturing multimodal biometric traits such as face and fingerprints and send them to cloud service by end-to–end encryption process. An enhanced encryption method with AES-256 algorithm is used for protecting the biometric traits on insecure communication path within TLS. SHA-256 is used for integrity and RSA for key exchange. Improvement is done in AES by altering the S-box. The principal component of AES block cipher is the S-Box. This S-box is used to provide the confusion factor for AES. The aim of this paper is to design dynamic S-box which depends on the secret key. To increase the difficulty of the system, AES is used in Round structure. The proposed AES algorithm can be enhanced to 1024bit key length for stronger security required in banking system.

The proposed architecture is leveraging the power of cloud to make the system scalable and pluggable. Thus the use of Raspberry Pi makes the biometric system low cost and portable and the use of the Encryption algorithm makes the system viable for secure communication and authentication.

Keywords

Raspberry Pi, AES, cloud computing, Microsoft Azure, dynamic S-Box, embedded systems.

1. INTRODUCTION

The need of increase in speed, cost-efficiency and security of electronic data has led to the application of cloud computing, embedded systems and the cryptographic algorithms. Also with the development of information technology, the world is getting electronically connected. Everyday transactions between individuals and among the organizations takes place via interconnected electronic devices. This highlights the need for identification of individuals. Biometric is a skill that recognizes an individual based on his physiological or behavioral characteristics. These systems ensures services are accessible only to the legitimate users. Biometric systems prevents identity theft, secures information stored in the PC etc.

Traditional security system used password or token that can be easily hacked or stolen through various attacks by hackers or attackers. Biometric systems depend on “who is she” rather than “what she has”. The application of biometric systems in ATMs, banks, attendance management, aadhar card etc is increasing but customers still are demanding cheaper and better solutions. Thus in the proposed architecture, the use of Raspberry Pi along with camera and the fingerprint scanner will make the system low-cost.

In recent years, optimal resource consumption has become a keyword to build the systems and this has given a drive to develop cloud based systems. The cloud based systems offer a low cost, scalable and flexible solutions for next generation computing needs. The blockages faced by the biometric systems can be solved by employing cloud based solutions.In the proposed architecture, the physiology biometric traits like face and finger are captured using RPi compatible hardware devices like PiCamera and the Futronic fingerprint scanner FS88 respectively and are sent to the Microsoft Azure cloud for better performance.

For the transmission of biometric traits to the cloud, these biometric data needs to pass through unsecure channel. There are chances that these important data may be captured or altered by intruders which will give them the right to access an important service etc. or can cause denial-of-service to the legitimate user. An end-to-end encryption is required using SSL/TLS, SSH, VPN, or a similar mechanism.AES is used most frequently in TLS because of its high efficiency, simplicity and security. Thus end-to-end encryption of these multimedia data is done and then sent to the cloud. The AES is used for encryption. The objective of this paper is to enhance the AES by increasing the complexity of AES using Round Structure and dynamic S-Box.

This system can be used for remote authentication and enrollment of a multimodal biometric system. The multimodal biometric system overcomes the limitations of the unimodal biometric system, reduces fraudulent access, and also has more accuracy, the cloud implementation provides the pluggability and scalability required by real time application of biometric authentication systems. Thus this paper develops a complete secure biometric SaaS using Raspberry Pi, enhanced AES and the Microsoft Azure cloud services.

2. LITERATURE SURVEY

In [1] authors proposed an image capturing technique in an embedded system based on Raspberry Pi boards. Most of the recognition systems are based on a PC, the portability of which is limited by its weight, size and the high power consumption. In [2] the authors have combined the cloud computing technology with the embedded system like Raspberry Pi to reduce piracy. The Embedded cloud for antipiracy ensures security of the hardware as it can be copied like disc and embedded wireless access point is constructed with cloud support. In [3] a new image encryption technique is proposed where the image is divided into blocks of pixels and then are shifted using a shift technique. This shifted image is served as an input to the AES algorithm. In another implementation [4], cipher key is used to change the standard S-Box. Here the rows are swapped with the columns of primary S-Box to generate dynamic S-Box using 128-bit cipher key. The authors [5] have proposed dynamic AES-128 key dependent S-Box. Here the secret key is input to the pseudo random sequence generator and the output is used to apply dynamic permutation on the standard S-Box. The AES secret is of crucial importance. Security is dependent on the confidentiality and the integrity of the Key. The AES is made stronger by using Dynamic S-Box, with look up table S-Box and Key expansion as modified the initial key is changed, that effectively providing a high opposition against differential cryptanalysis and especially the linear cryptanalysis [6].

3. RASPBERRY PI

The Raspberry Pi is low-cost small single board mini-computer developed in UK by the Raspberry Pi Foundation Team with the aim of teaching young students programming skills. The RPi is capable of doing everything what a PC can do. Different models of RPi are A, A+, B, B+ and the RPi 2. In this research, Raspberry Pi Model B is used which costs US $35. It has 2 USB ports, a HDMI port for connection with the display, SD/MMC/SDIO card slot as RPi model B for booting and data storage as RPidoesn't not have on-board storage. Also it has 10/100 Mbit/s Ethernet (8P8C) USB adapter for internet connection. To make RPi portable in this project wireless USB Wi-Fi adapter is used. The OS used is Raspbian (Debian wheezy). RPi model B needs power supply of 5V-700mA (3.5 W)[2] [7].

4. ENCRYPTION – AES-256

Nowadays, digital images are used in many different processes. Hence security of image data is very important. In this project, a new Image Encryption technique is proposed. Here the face and the fingerprint images are sent to the cloud for authentication purpose. Since they are transmitted via unsecure channel, it is important to have secure transmission. For this encryption is done using AES-256 CBC mode in MATLAB. The AES is cryptographically secure algorithm. It has fixed block size of 128 bits and can be used with different key length 128bits, 192bits and 256bits.

Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block. The S-box is generated by determining the multiplicative inverse for a given number in GF (2^8).

ShiftRows: A simple permutation

MixColumns: A substitution that makes use of arithmetic over GF (2^8).

AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key [9].

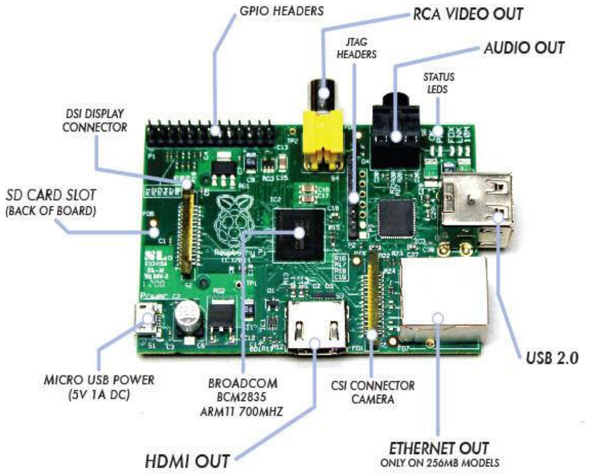

GPIO HEADERS
RCA VIDEO OUT
JTAG HEADERS
AUDIO OUT
STATUS LEDS
DSI DISPLAY CONNECTOR
SD CARD SLOT (BACK OF BOARD)
USB 2.0
MICRO USB POWER (5V 1A DC)
BROADCOM BCM2835 ARM11 700MHZ
CSI CONNECTOR CAMERA
HDMI OUT
ETHERNET OUT ONLY ON 256MB MODELS

Figure 1: Raspberry Pi Model B [8]

In this research, enhancement is done using Round Structure and the dynamic S-Box which will overcome the linear and the differential cryptanalysis.In Round structured AES, S-box changes in every round. The cipher key is used to convert static S-box into dynamic. The inverse S-box is also changes according to the S-box.

5. CLOUD COMPUTING

Cloud Computing is a catch word of the new world. The RPimodel B is not capable of performing the extensive calculations because of less processor speed and available RAM involved in extracting the feature vector, storing and retrieval of biometric traits from large databases etc. The cloud service overcomes this weakness and further add to security, device management and so on [10].

In this work, the encrypted images are sent to a Microsoft Azure cloud where the images are decrypted and the original image is retrieved. The cloud service is implemented as a software-as-a-service (SaaS).

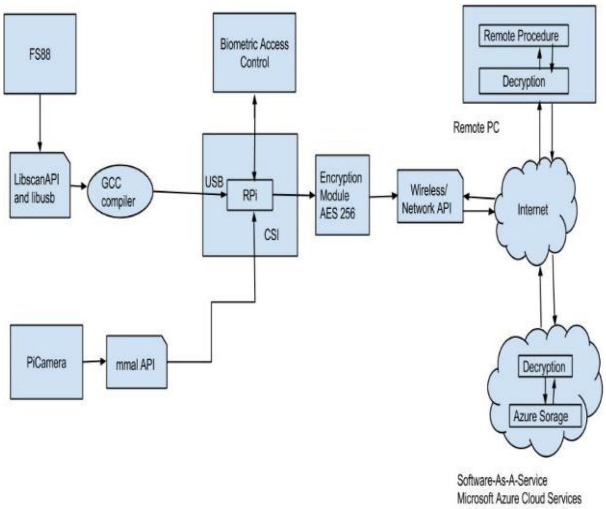


Fig 2: Architecture of the cloud based Biometric Saas.

6. PROPOSED SYSTEM

Figure 2 shows the architecture of the cloud based Biometric SaaS using Raspberry Pi. Figure 5 shows the structure of the proposed AES for encrypting the biometric traits and sending them to the cloud.

Figure 3 depicts the proposed hardware setup interfacing the PiCamera and the FS88 with the RPi along with power source and the USB Wi-Fi adapter.

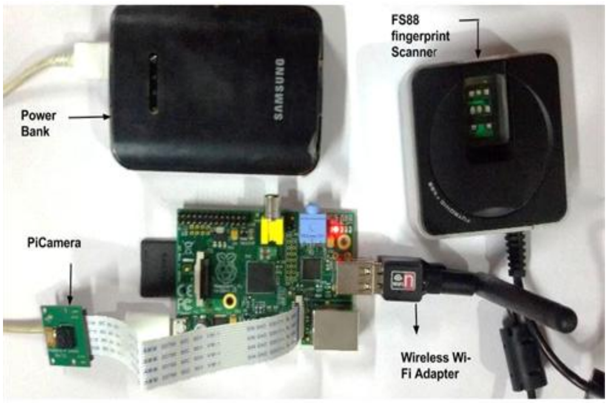


Figure 3: Hardware Setup

In this research, RPi Model B is used to capture biometric traits like face and fingerprint using the PiCamera and the Futronic FS88. The PiCamera is connected to the RPi via by way of a 15 pin Ribbon Cable, to the dedicated 15 pin MIPI Camera Serial Interface. The Camera Serial Interface (CSI) bus is capable of high speed data transfer, and it exclusively carries pixel data to the BCM2835 processing unit [11]. The FS88 is connected to the RPi via the USB port. For interfacing FS88 with RPi libScanAPI.so and the libusb.so needs to be installed on the RPi. Libusb is a library which allows user space applications access to USB devices [12].

After successfully capturing the biometric traits, they are encrypted using the proposed Round structure AES with dynamic S-Box.

Post encryption, the encrypted traits are sent to the Azure cloud along with the Shared Access Signature (SAS) key to the Blob storage wherein they are decrypted for authentication purposes.

Now let’s focus on the encryption module which is the main core of this research.

7. THE ENHANCED AES 256 WITH ROUND STRUCTURE AND THE DYNAMIC S-BOX

The 256bits input and the 512bits key length is given to the enhanced AES system. The 512bits key length is divided into 256bits each. First 256bits are given to the round structure and the next 256bits are given to the AES algorithm. The AES secret key is modified and used as an initial state to the pseudo random sequence generator. Also XOR operation of all the bytes of the round key is taken to produce a new value. This new value along with the output of the pseudo random sequence generator is used to produce dynamic S-Box.

8. THE PN SEQUENCE GENERATOR

The AES secret key is modified and given as input to the pseudo noise PN generator. The proposed generator consists of three maximal length linear feedback shift registers (LFSR) with thirty one, nineteen and fourteen taps. The feedback functions are chosen primitive to achieve a maximum period for each register [5]. The output of the generator is two 16 hexadecimal values, *PNseq*.

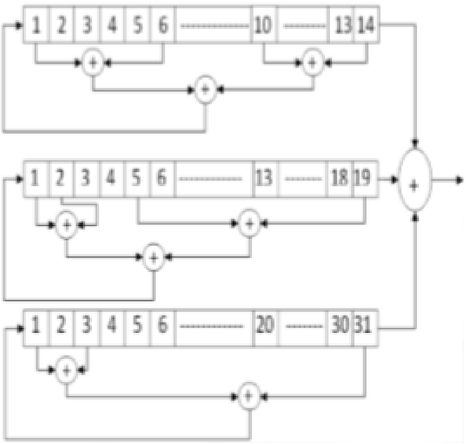


Fig 4: PN sequence Generator

The key length of this PN generator is (14+19+31) 64 so this generator needs 64 initial values. The AES-256bits secret key is reshaped to four vector of 64 bit length and these four vectors are XORed with each other and the result is fed to PN generator as initial state.

The Dynamic S-Box generation

The round key and the *PNseq*are used to produce a new number which is used as a shift value. The S-Box is rotated by that shift value. Thus the static S-Box is dynamically changed using the cipher key and the pseudo random sequence generator. The inverse S-Box is also revised after the S-Box to get the correct inverse values.

In this paper, the enhanced AES can be used depending on the level of security required. In demand of moderate security Case 1 is used and when high security is required Case 2 is used. For the both the cases, the similar part is: Let modified AES secret key be the input to the pseudo random sequence generated where the output is 32 hexadecimal values, *PNseq*.

Case 1: Select the first byte of the *PNseq*and the first byte of the round key generated using the key expansion algorithm and XOR them. Use the resulting value as the shift value. Now the standard S-Box is rotated using this shift value.

Case 2: XOR all the bytes of *PNseq.* Let the new number be called as *PNvalue.* Also XOR all the bytes of the round key call it as *round Value.* Get the shift value by XORing the *PNvalue*and the*roundValue*.Finally the standard S-Box is shifted using the shift value.

One important thing to note here is roundkey and hence the *roundValue*will change in each round. The *PNseq*and hence the*PNvalue*will be fixed throughout the algorithm.

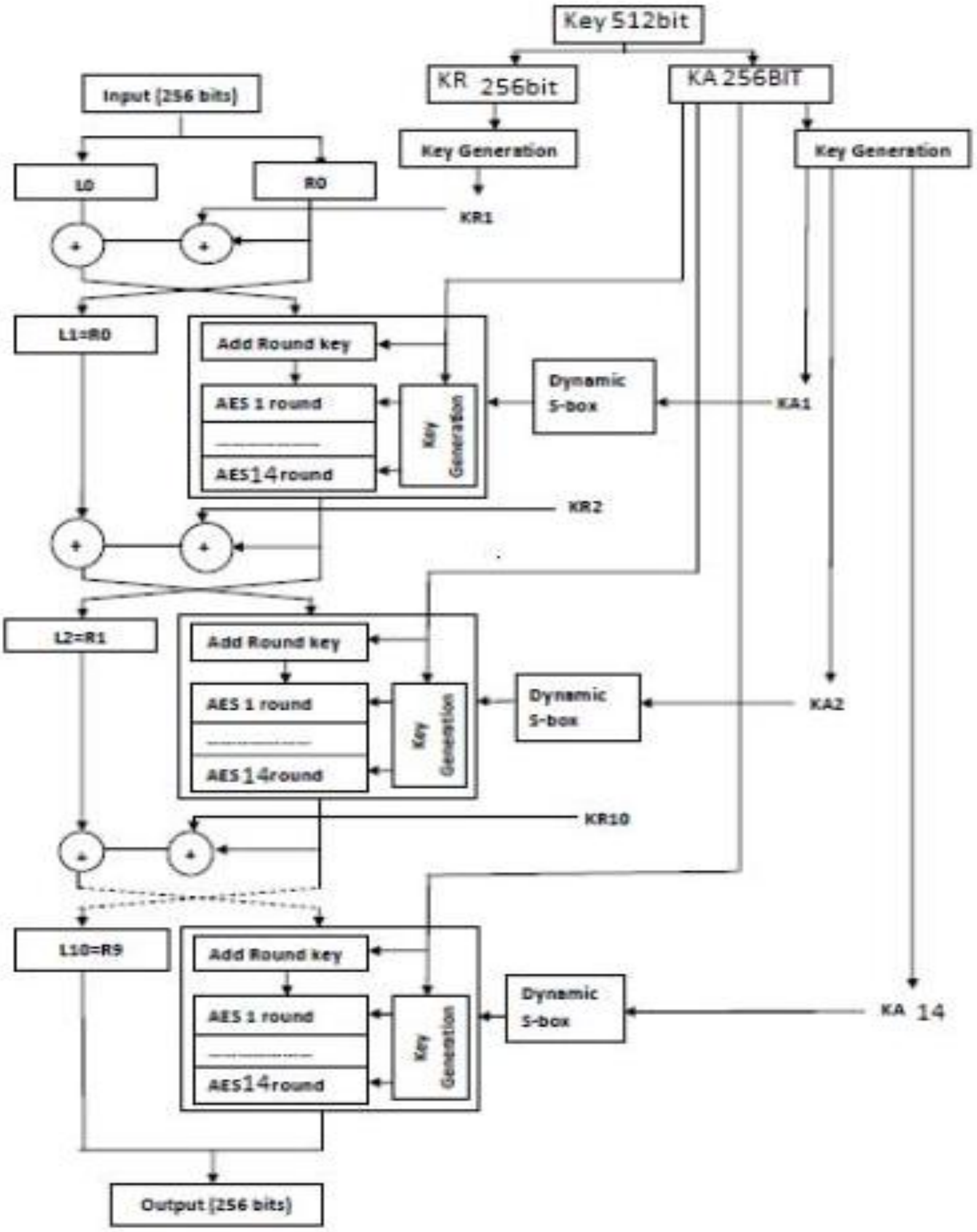


Fig 5: Round AES with Dynamic S-Box

1. The Round structure of AES is used as shown in Fig. 4. Here the Input Data is split into two blocks of 128 bits each.

2. One Block is given as Input to the AES section of the System. The other Block is given as Input to the AES section of the System in the next round as per the Round structure.

3. This is done for all fourteen rounds respectively. These outputs are then combined together to form 256 bit block of encrypted data.

4. Dynamic S-box is applied to the Round structure of AES as shown in Fig. 5.

5. In the round structure, AES is applied n times to the block of data hence total n different S-boxes is created hence it is called dynamic S-box.

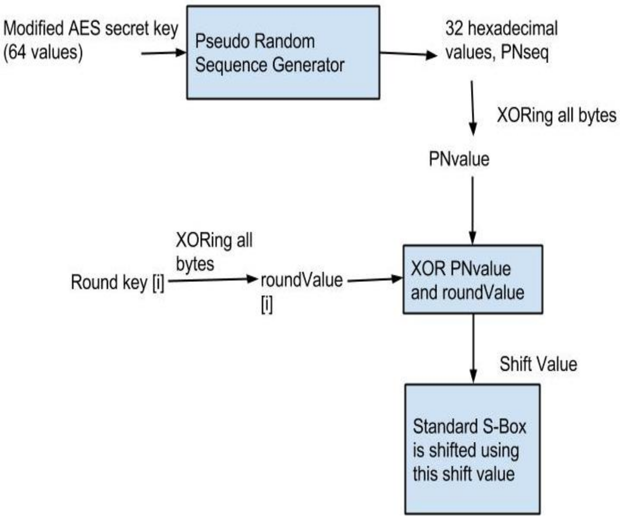

Modified AES secret key
(64 values)
Pseudo Random Sequence Generator
32 hexadecimal values, PNseq
XORing all bytes
PNvalue
XORing all bytes
Round key [i]
roundValue [i]
XOR PNvalue and roundValue
Shift Value
Standard S-Box is shifted using this shift value

Fig 6: Proposed Dynamic S-Box generation for High Security

9. RESULTS

9.1 Biometric traits captured by RPi

The image capturing by Raspberry Pi is successfully implemented.

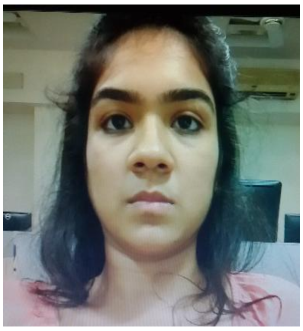


Fig 7: Face captured by RPi

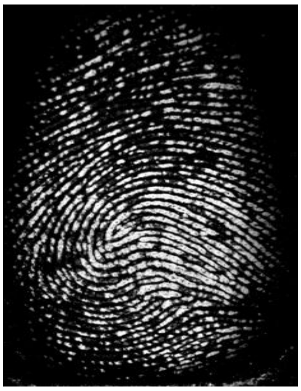


Fig.6 Fingerprint image captured FS88 interfaced with RPi

9.2 Encryption of Biometric traits

The biometric traits will be encrypted on RPi client. The round structure with 256bits input data and 128bits secret key with 10rounds along with dynamic S-Box using cipher key is successfully implemented using MATLAB.

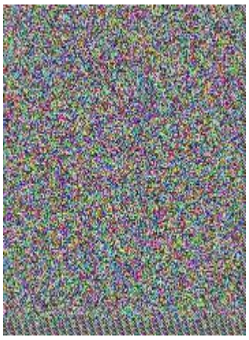


Fig 8: Encrypted Image of face

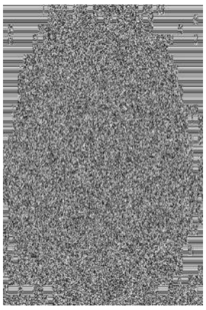


Fig 9: Encrypted Image of fingerprint

The S-Box implementation for the above results is:The hexadecimal digits of cipher key are XORed with each other and obtained number is used as the shift value. S-box is rotated by that shift value. Before sub byte stage, the static S-box is converted into dynamic using cipher key. Since the cipher key changes in each round, the S-Box values will differ in each round. The inverse S-box is also modified after S-box to obtain correct inverse values. The Table 1. Shows the encryption and the decryption time using the Round structure (10 rounds) AES with dynamic S-Box and the input being 256bits along with 256bit key length. Table 2 shows the encryption and the decryption time using basic AES-128 with 128bit as input.

Table 1 Encryption and Decryption Time using Enhanced AES

Images	Size (kb)	Encryption Time (secs)	Decryption Time (secs)
Face	555	76.3078	78.4525
Finger	81	7.16624	9.07029

Table 2Encryption and Decryption Time using basic AES

Images	Size (kb)	Encryption Time (secs)	Decryption Time (secs)
Face	555	70.2564	71.6804
Finger	81	5.2049	6.5301

9.3 Cloud Computing

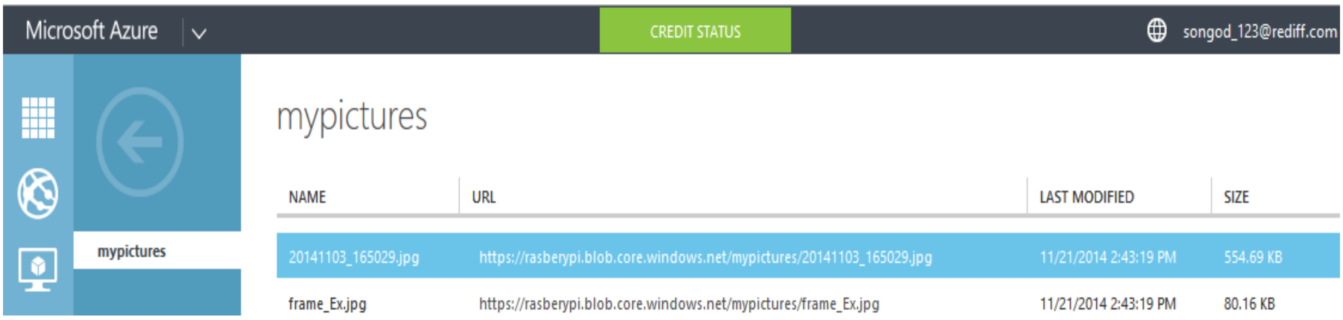
The encrypted images will be sent to the Azure storage where the images will be decrypted. Before decryption hash code will be produced using SHA-256 to check the integrity of the biometric traits. The uploading of captured biometric traits on the Microsoft Azure Server is completed and then uploaded.

Fig. 10 shows the blob storage summary of the Microsoft Azure account. It can be seen that the two images 'Frame_ex.jpg' (Face) and '20141103_165029.jpg' (Fingerprint) are uploaded to the cloud service successfully. The encrypted biometric traits will be sent to the cloud and then decrypted there in the future.

10. CONCLUSION AND FUTURE WORK

Thus in this research Raspberry Pi is implemented as a remote authentication node. The AES is implemented in MATLAB and the biometric traits are encrypted using Round Structure and the dynamic S-box.Using AES in Round structure with more no of rounds, runtime is increased but complexity of network is also increased. Increasing complexity will make the system attack resistant and secure data from attackers. So this system can be used in the application where time is not the constraint. The time taken by the AES in Round structure with one round is nearly same as traditional AES hence it can be used in the applications where speed is required with complexity. This is a low-cost system which will ensure high security and high scalability. Also the biometric images are successfully uploaded to the Azure platform.

Future work includes implementing AES in C#. Also the proposed dynamic S-Box using pseudo random sequence generator will be implemented which will strengthen the security using 512bits key length. Also round structure with 14rounds will be done.The encrypted images will be sent to the cloud and decrypted there and feature vector extractions will be done. Performance measures of the enhanced AES will be calculated based on encryption and decryption time, Avalanche effect, and Memory and CPU usage. Proposed system has application in all the biometric access control systems, which requires transportability, scalability and low implementation cost.



mypictures

NAME	URL	LAST MODIFIED	SIZE
20141103_165029.jpg	https://rasberypi.blob.core.windows.net/mypictures/20141103_165029.jpg	11/21/2014 2:43:19 PM	554.69 KB
frame_Ex.jpg	https://rasberypi.blob.core.windows.net/mypictures/frame_Ex.jpg	11/21/2014 2:43:19 PM	80.16 KB

Fig 10:Snapshot showing biometric traits which are uploaded on Azure Storage

11. REFERENCES

[1] G.Senthilkumar, K.Gopalakrishnan, V.Sathish Kumar, "Embedded Image Capturing System Using Raspberry Pi System", International Journal of Emerging Trends & Technology in Computer Science, vol. 3, issue 2, April 2014

[2] Rushikesh Tade, "Embedded Cloud For Antipiracy", International Journal of Science and Technology Reasearch vol. 2, issue 6, Jun 2013.

[3] A. Abugharsa, A. Basari, H. Almangush, "A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm", International Journal of Computer Applications, vol. 42-No.9, Mar 2012

[4] R. Hosseinkhani& H. Javadi, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System", IJCSS, vol. 6, issue 1, 2012

[5] E. Mahmoud, A. Hafez, T. Elgarf, A. Zekry, "Dynamic AES-128 with Key-Dependent S-box", IJERA vol. 3, Issue 1, January -February 2013, pp.1662-1670

[6] S. Arrag, A. Hamdoun, A. Tragha, S. Khamlich,

"Implementation of Stronger Aes by Using Dynamic S-Box Dependent of Master Key", Journal of Theoretical and Applied Information Technology, vol. 53 No.2, 20th July 2013.

[7] Raspberry Pi, Available: http://en.Wikipedia.org/wiki/Raspberry_Pi

[8] Available: http://www.siongboon.com/projects/2013-07-08_raspberry_pi/images/raspberry_pi_circuit.jpg

[9] Available: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[10] Soup to Nuts: From Raw Hardware to Cloud-Enabled Device, Available: http://msdn.microsoft.com/en-us/magazine/dn781356.aspx

[11] Camera Module, Available: http://www.raspberrypi.org/ documentation/ usage/camera/README.md.

[12] RPi Verified Peripherals, Available: http://elinux.org /RPi_VerifiedPeripherals#Fingerprint_Scanners