International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

An Implementation of New Qr Based Encryption Algorithm For Secure Medical Data In Cloud Storage

L.Ramesh, R.A.Roseline

Abstract: ***Healthcare Information technology encryption is more and more popular alternative in terms of retaining sensational records inclusive of patient PHI. With more carriers implementing IOT, EHR-Connectivity and usage of linked gadgets, the problem over whether encryption is important is important is an extra widely wide-spread. Encryption of health data is while companies change information into encoded textual content, which makes the facts unreadable unless a person has a key or code to decrypt it. This could be a terrific choice for covered entities or commercial enterprise buddies that regularly manage electronic PHI (ePHI) and want to make sure unauthorized customer can't admit to get the information. In this paper discussed about the new QR based encryption Algorithm for secure medical data which is stored inside of the cloud.***

Keywords: QR, Encryption, Medical data,

I. INTRODUCTION

Health care information technology has been described in many ways as a framework for managing health information, as a mechanism to improve patient case and as an enable of patient case conditions. All of these descriptions convey the results of using healthcare information technology but fundamentally, health care information technology is the application of information technology to the healthcare industry.At the conceptual level, Information technology or the use of hardware and software in an effort to manage and manipulate data and information, consist of devices that input, process and output data and information. At the physical level, these devices could include keyboard, mouse, computers, printers and network devices, which are collectively known as hardware. In addition to hardware, information technologies consist of software. Software contains the logic that makes computer do what they do and also it helps hardware to process data to information. Together hardware and software used in healthcare information technology.

1.1 Uses of Healthcare Information Technology:

As countries face ever more challenging budget crises healthcare costs continue to be at the forefront. A report from the CBO called "Evidence on the costs and benefits of healthcare information technology" states that the use of an Electronic Medical record for patient care would have several efficiency benefits.

Eliminating the use of transcription Reducing the need to physically retrieval patient charts or records Reminding prescribe to prescribe Reducing the number of duplicated data

1.2 HIPPA

The health insurance portability and accountability of 1996 is a very broad federal regulation that way developed in order toImprove portability and continuity of health insurance

Manage waste, fraud and abuse of health care delivery Reduce cost and increase efficiency by standardizing the interchange of Electronic data Protect the privacy of PHR

Unlike the privacy rule, the security rule focus on electronically transmitted or stored PHI(e-PHI) used by covered entities. HIPPA security rule concentrate especially for e-PHI.

II. PROBLEM DEFINITION

In 2018, the health sector recorded 15 million records of patients involved in 503 offenses, three times more than in 2017, according to the Protenus non-compliance Barometer. But little more than half of 2019, and the number has soared with potentially more than 25 million records of violated patients. The medical assistance was punctuated by enormous data breaches and each of the 10 largest suffered the violation of over 200,000 records. What is worse is that many of these lasted for long periods of time, while others did not report within the mandatory 60 days of HIPAA. Third-party vendors and phishing attacks have been at the root of most of these security incidents and investigations against major vendor breaches are still ongoing. At present, 2019 may be the worst cyber health security visa.

2.1 Techniques to secure medical data

2.1.1 Encryption

The raise of malicious attacks from insiders and outsiders and the turn from nuisance hacking to profit-driven hacking has dramatically increased the likelihood of vulnerabilities being exploited in damaging ways, reducing the margin of error on technical controls. Failures of information security routinely make headlines and involve increasingly costly response efforts. Information security is now a broad level concern, which has focused the interest in a variety of technical solution.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
L.Ramesh, M.Phil*, Computer Science, Specialization, Information Security, Bharathiar University, Tmail Nadu.
R.A.Roseline, Associate Professor, Head, PG and Research Department of Computer Applications.

Technical solution has become a critical component to every health care organization- Encryption. According to HIPPA security rule, "Encryption means the probability of assigning meaning without use of confidential process or Key".Encryption technologies are used to store and transfer data in secure format, ensuring its protection against compromise of unauthorized access. Health care organization can use any encryption algorithm by NIST as an approved security functions.

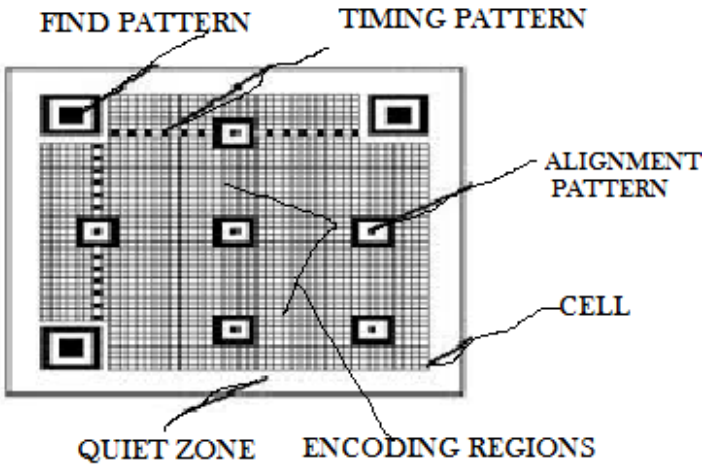

Fig 1. Encryption process

2.1.2 QR code:

QR codes are small, harmless models printed on a surface (billboard, poster, etc.) and its intention is only to help you get data from a print media to a digital medium. They cannot be read easily with the naked eye, so they are particularly difficult to manipulate after publication.

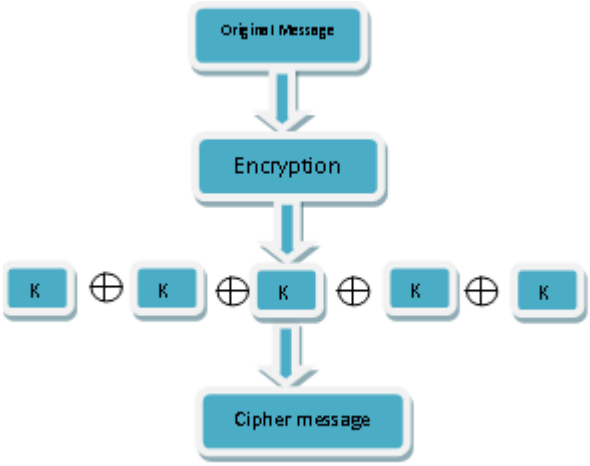

Fig 2. Structure of QR code

III. IMPLEMENTATION OF NEW QR ENCRYPTION ALGORITHMS

In computer age, cryptography has been essential to protecting against the falsification, destruction, and interception of information. Encryption is the conversion of plain text data (plain text) into cryptographic encoding that can't be access without key (encrypted form). Decryption is the reverse process of encrypted form.There are two common types of encryption algorithm used to transfer original message into scrambled. In symmetric key encryption the same key is used for encryption and decryption whereas asymmetric key encryption different key is used for the process of encryption and decryption. Main purpose of encrypt algorithm to protect secure data and use difficult key to decrypt. The algorithm is a valid one is must pass test with all possible keys, when the data is used longer key for encryption is too difficult to access the data. The quality of an encryption algorithm is difficult to determine. Algorithms that look promising are sometimes simple to crack, specified the correct techniques of attack. While choosing an encryption algorithm, it is a great idea to select prosperous prevent from all attacks.

Steps in new QR based encryption algorithm techniques:

Step 1: Scan the medical records
Step 2: Encrypt the medical record by using new encryption algorithm
Step 3: Get Encrypted medical records
Step 4: Convert Encrypt medical records into QR code
Step 5: Get QR code based encrypted medical record
Step 6: Stored QR Encrypted medical records in HIPPA suggest cloud storage

Decryption process:
Step 7: Scan the QR Code
Step 8: Get the Result of Step 7
Step 9: Decode the QR code
Step 10: Reverse the New encryption algorithm to get original image

Step 11: Get the Original medical record

IV. RESULTS & DISCUSSION

Encryption process and QR code generation:

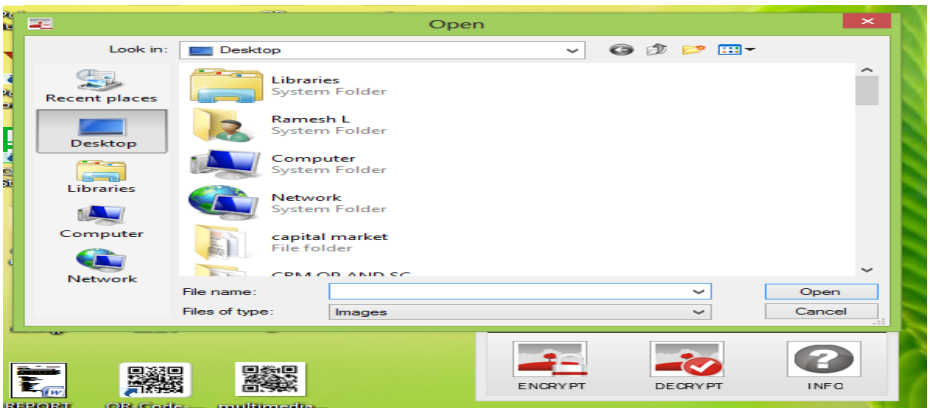

Fig 3. Encryption of image

In Fig.3 shows the upload the encryption with the help of new encryption algorithm scheme

Fig 4.Upload the image

Fig 4 shows

upload the sample medical image into cipher image by using encryption process

Fig 5. Encryption process of image

Fig 5 reveals the encryption process of original medical record image to cipher image

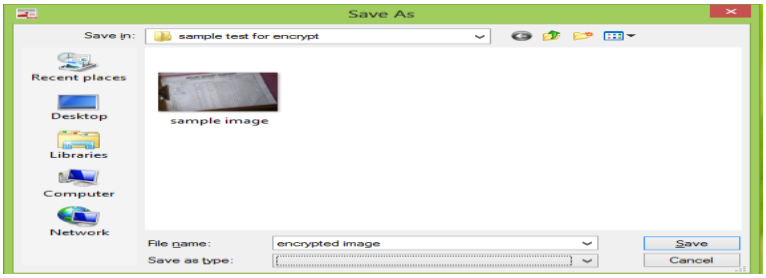

Fig 6. Saving of Encrypted image

Fig 6 shows the saving of cipher image of original medical report

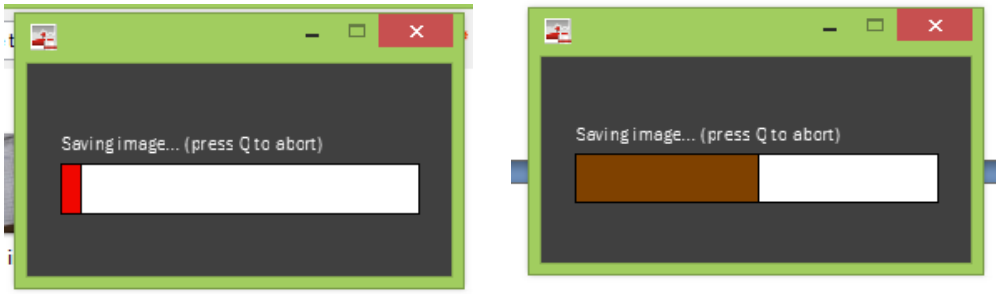

Fig 7. Saving Process of encryption image

Once the saving process is done after that the encrypted image is saved in local drive which is show in Fig 7.

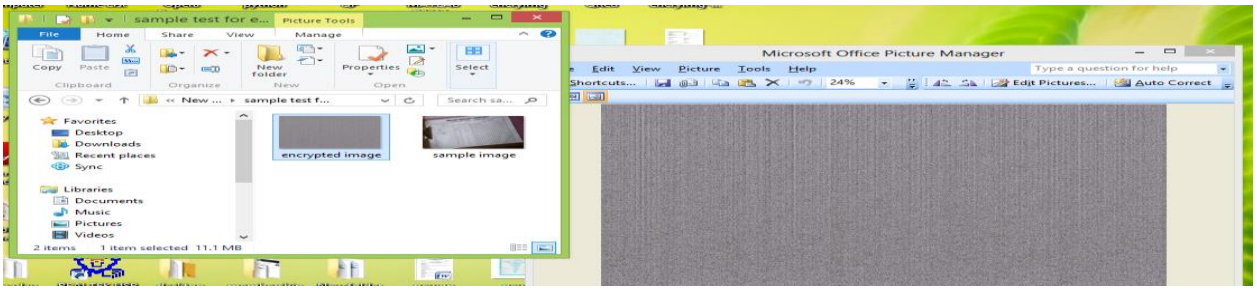

Fig8. Successful saving of Encrypted image

The original Medical record is successfully converted as encrypted image for more security purpose. The encrypted image showed in Fig.8. Once the Encryption process is over user is create QR code for an respective encrypted image

Process of create QR code:

The encryption process is successfully done, after that creates QR code for encrypted medical image, that the process is shown in below

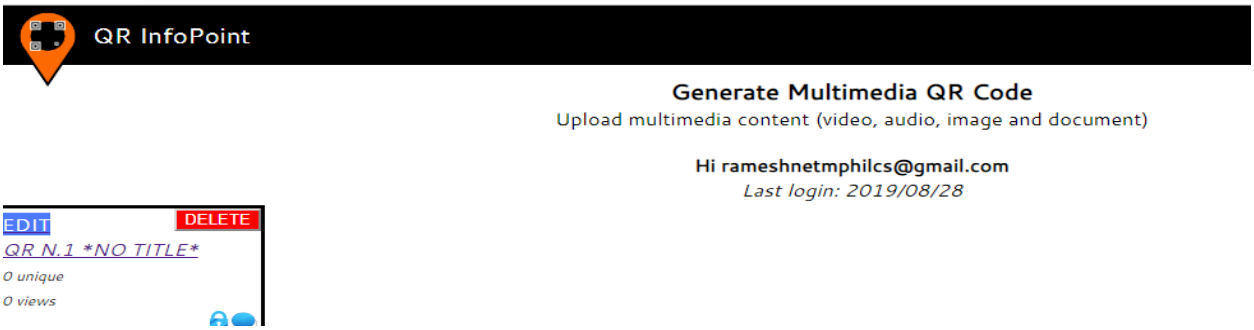

Fig 9. QR Info Point for create QR code

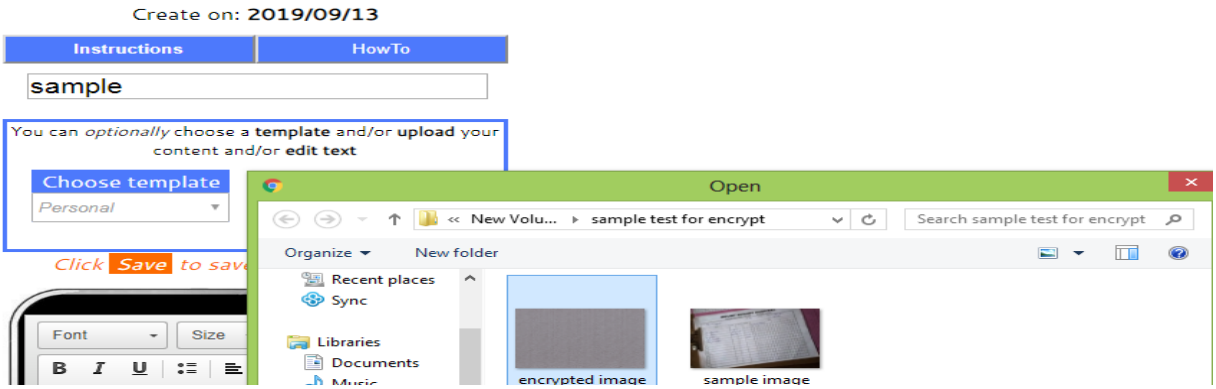

Fig 10. Upload encrypted file to Create QR code

Fig 11. Uploading Process

Fig12. Successful creation of QR code with Password

In this paper we create the QR code with the help of QR point which is safe and secure from unauthorized access. Once the encrypted file is successfully upload in the QR point its automatically convert the encrypted image with password. Fig12. Shows the successfully creation of QR code with password.

Decoding QR code and Decryption Process:

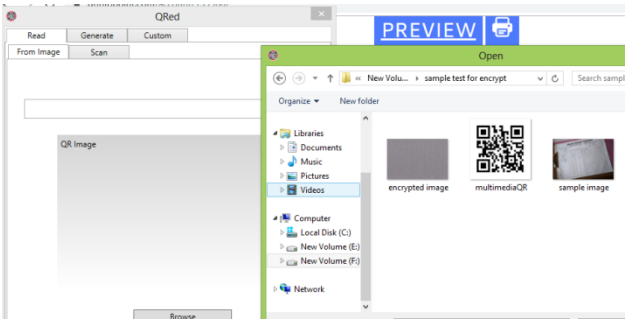

Fig 13. Read QR code using QRed

In this section discussed the process of decode the QR code and decryption of encrypted medical records. For decode the QR code here we used the QRed app instead of this user can used to scan with the help of any QR code reader. Once the decode is successful the user can get the encrypted medical record by using respective password for authentication verification. Fig 16 shows the successful decode of QR code

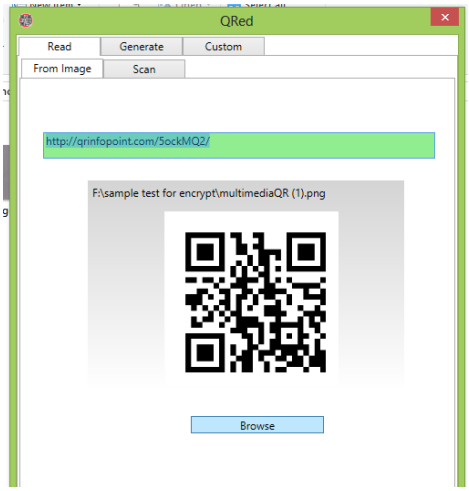

Fig 14. Retrival QR code using QRed

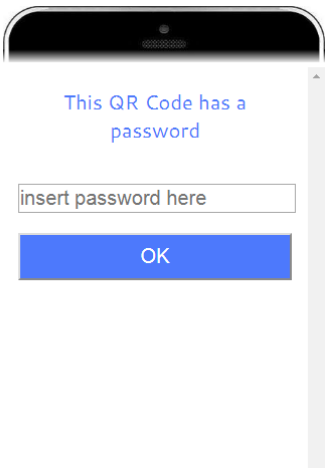

Fig15. QR code contains Password

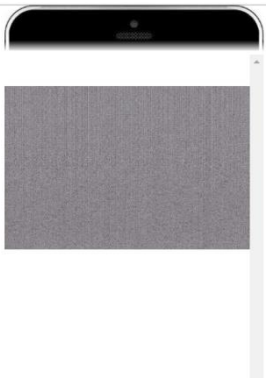

Fig16. Successful Decode of QRcode

After the Decode of QR code reverse the encryption process for get original medical record from Fig 17 and Fig 18 shows the upload of encryption file, decryption process respectively for conversion of Encrypted data to Original data. Fig 19 shows the Final Original report which is similar as Sample report.

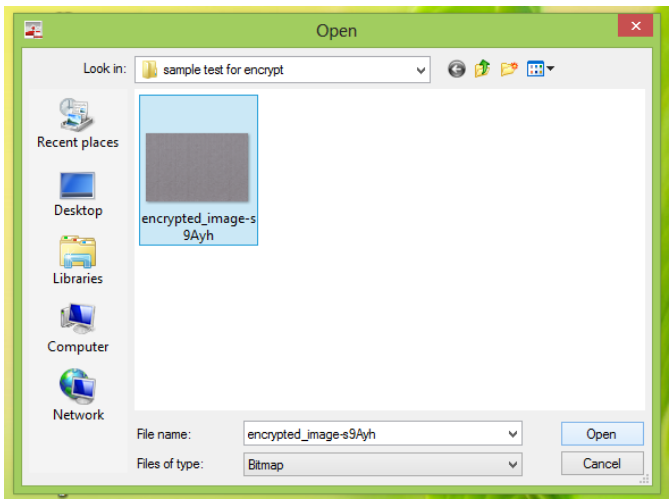

Fig 17. Upload encrypted file for Decryption

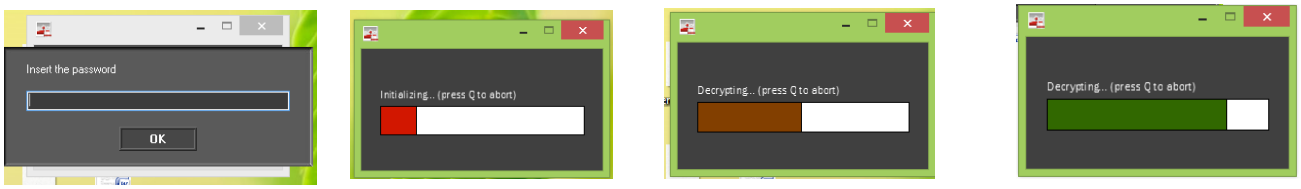

Fig 18. Decryption Process

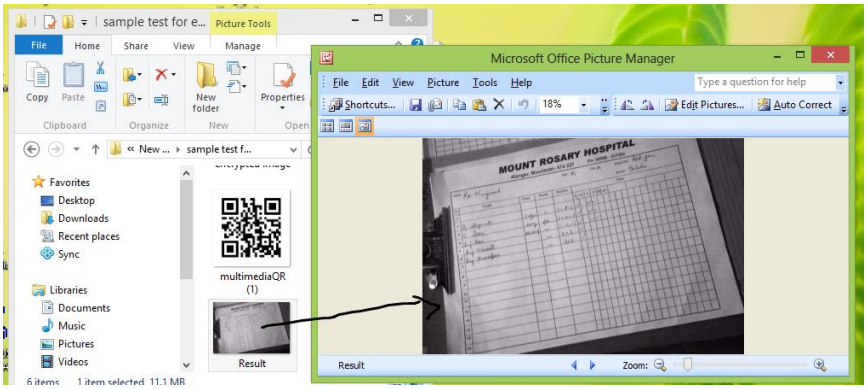

Fig19. Original Medical Report

V. CONCLUSION

This Paper presents a secure and efficient image recovery scheme on encrypted cloud data. The new techniques deal with a new QR based encryption algorithm to construct a secure medical record in cloud storage. Firstly, to encrypt original medical record into encrypted file by using confusion and diffusion technique after generation of 5 level key generations, in this case, the proposed model is secure. After that, generate QR code with password for encrypted image by using QRpoint. Finally decode the QR code and reverse the encryption technique to retrieval the original medical data.

REFERENCES

1. A. E. Standard, "Federal information processing standards publication 197," FIPS PUB, pp. 46–3, 2001.
2. J. Daemen, R. Govaerts, and J. Vandewalle, "A new approach to block cipher design," in International Workshop on Fast Software Encryption. Springer, 1993, pp. 18–32.
3. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, "The cipher shark," in International Workshop on Fast Software Encryption. Springer, 1996, pp. 99–111.
4. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2007, pp. 450–466.
5. J. L. Massey, "Safer k-64: A byte-oriented block-ciphering algorithm," in International Workshop on Fast Software Encryption. Springer, 1993, pp. 1–17.
6. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, "The cipher shark," in International Workshop on Fast Software Encryption. Springer, 1996, pp. 99–111.
7. J. Daemen, L. Knudsen, and V. Rijmen, "The block cipher square," in International Workshop on Fast Software Encryption. Springer, 1997, pp. 149–165.

AUTHOR PROFILE

Ramesh L is a Research scholar, PG and Research Department of Computer Applications. He did his M.Phil in Computer Science with specialization in the area of information security at Bharathiar University. He has published about 7 papers in international journals. His research interests include Networks, Information security, Cloud computing and IoT. He has presented papers in international conferences at Malaysia. He has been an active member of the society of digital information and wireless communications, internet society, Indian Academician and Researcher Association, International society for research and development, International Association of Engineers, International Economics Development Research Center, International Computer science and Engineering society and the institute of Research Engineers and Doctors.

Dr. R.A. Roseline is Associate Professor and Head, PG and Research Department of Computer Applications. She did her PhD in Computer Science in the area of Wireless Sensor Networks at Bharathiar University . She received M. Phil in Computer Science from Periyar University specialising in Mobile Adhoc Networks. She has published about 22 pa pers in international journals. She has completed a UGC Minor Project in Pollution monitoring using Sensor networks with a funding of 1.7 lacs. Her research interests include Sensor Networks, Cloud computing, Data mining and IoT. She has presented papers in international conferences at Australia and Malaysia .