EFFICIENT METHOD OF PRESERVING MEDICAL DATA BASED ON CLOUD COMPUTING AND IOT.

[1]Sagar Sen, [2]Ajay Singh, [3]Shraddha Singh, [4]Vrushali Yadav, [5]Prof.Saurabh Suman
[1]Author, [2]Author, [3]Author, [4]Author, [5]Author

Department of Information Technology
Mumbai University
Slrtce, Mumbai, India

Abstract : In the healthcare industry, NFC can make a significant difference by providing faster retrieval of the patient's medical data. Additionally, it provides access to medical history along with emergency medical details. NFC card is used to fetch the patient's data from cloud storage (Amazon Web Service) which can be directly accessible to the doctor for further assessment. The major concern of any medical hospital or clinic integrating with this system is the security of their sensitive data. Hence, one of the main contributions of our paper is providing security to medical data. In order to double the degree of security, we are making use of AES 256 algorithm twice, firstly to hide the identity of the medical data and secondly the default AES 256 encryption provided by the AWS. AES generates a 256-bit long cryptographic ciphertext using the block cipher algorithm which has 1.1*10^77 possible combinations which makes it nearly impossible to hack. In this paper, we also emphasize on providing an android application which encapsulates a number of medical services which is required in case of an emergency and also includes secure access of medical information enabling a renewed focus on patient-centered care.

***IndexTerms* -** Cloud Computing, Cloud of things, Near Field Communication (NFC), Internet of Things, Smart healthcare.

I. Introduction

Healthcare is a domain which has been gaining immense scrutiny nowadays. Various ongoing advancements made in computing and network technologies have been stemming the domain of medicine to grow from hospital-centered towards wellbeing centered care. This paper emphasizes on delivering healthcare services in a more efficient, smarter, quality focused and secured way. To accomplish this, we are adopting technologies like cloud computing and the internet of things. Amalgamation of cloud computing and IoT is referred to as CoT which aims to unfold Things as services via applications.

Our proposed system keeps track of patient's health records delivering a low cost and quality focused treatment by speeding up the process of diagnosis. The patient provides all the necessary details required for registration to the Admin of the System. Admin writes this information to a blank NFC card and permits the card to the patient. With one tap system, NFC card fetches the unique key and the name of the patient and compares it with the data stored on the Amazon cloud. Patient's data are stored in the form of pdf of the name matching with the unique key and Patient name. The data matching with this key is then retrieved from the cloud and loaded on the doctor's device.

For easier access of services from user's end, we have designed an android based application consisting of a number of services such as an emergency button, pharmacy-related general information, booking appointments, and tracing the hospital's location.

1.1) Technology

A. Near Field Communication (NFC)

NFC is a code that defines rules, definition, pattern and simultaneity of communication which is basically a set of connecting protocols. This protocol enables two electronic devices such that one is a portable device and establishes the communication with another device while they are approximately 1.6 inches or less than 10cm close to one another. The conveying rate of information is 106-424 kbps. Electromagnetic induction is used in NFC to transmit the data which is established from former technology of RFID.

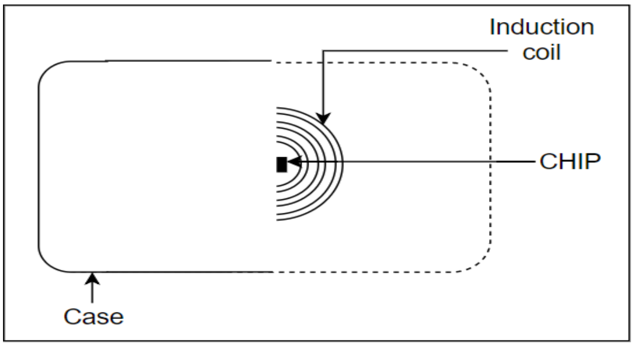


Fig.1: Inside an NFC Card

NFC works on three distinct Operating methods:

1. Peer to Peer mode (P2P): P2P allows exchange of information or files between two NFC-enabled devices.
2. Reader/Writer mode: In this mode, most of the time NFC device acts as readers. This mode uses one way transmission of data. The functioning device such as the latest mobile phones also called as Smartphone connects with some other device to read/write data of a tag. It uses anti-collision algorithm to select one tag when the device detects two or more tags.
3. Card simulation mode: In this form of communication, the NFC device is in inactive mode. The device that is authorized with NFC behaves like a contact-less smart card.

In our proposed system,” MIFARE classic 1 k” tag is used. 1k defines the size of data that a tag can stock. It contains 16 sectors. There are 3 blocks of data processing and 1 block for accumulating access commands and unrevealed access key in each of these subdivision.16 bytes of data is stored in each block. With the assistance of a secret connection key, the reader verifies the tag before reading a part. The sectors can define its own access right and for a particular action, the need of a particular key is defined.

B. Cloud Computing

Estimating accounts such as servers, depository, databases, perception, analysis, networking and moreover the internet are the services delivered in CC. Cloud computing provides speedy access and modernization, malleable resources and economies of scale. We only pay for the cloud services which we use which helps to lower the function cost and also the framework runs more efficiently and escalation of the services can be done easily as organization needs changes.

Merits of cloud computing are: 1. It eradicates the cost of buying software and hardware the eliminating the requirement to invest in data centers and servers.2. The information technology assets are made available on a snap which means only a few minutes is required to make resources accessible to the developers3. Deployment of applications in multiple areas has become easy allowing to go global within minutes 4.Broad set of procedures, technologies and commands are decided by the cloud providers and provides benefit by protecting the data, applications, and framework from various risk.

We are using AWS which is a platform of cloud service. It maintains network connected hardware which is required for application services. Amazon S3 is an object repository assistance provided by Amazon web services. It proposes industry dominance, safety, effciency, scalability and possibility. S3 provides convenient administration features to organize the information and access commands are set up to meet managerial, business and agreement requirements. S3 is designed for 99.99999999999% of persistency. Abundance amount of applications and data are stored for companies all around the world on cloud.

In this paper, Section II gives brief idea about the literature review. Section III describes overview of proposed system. Section IV gives the system analysis and results. And Section V provides Conclusion.

II. REVIEW OF LITERATURE

The work by Renyou MEI and Xiaoli QIU have emphasized on introducing the concept of cloud computing into the medical information system[1], by designing a concept which applies the generic medical data management structure in order to improve the effectiveness and medical service. Their proposed system drew lessons on distributed storage and efficient processing of general medical data by provides data management services for users.

In paper[2] the author proposes that for accumulating the therapeutic data history, which may inculcate huge intermedia big data such as radiology images, blood reports etc to be store on cloud. Their organization allows the connection to the electronic medical records (ERM) and provides confidentiality of the information in the cloud. Pairing based cryptography is an algorithm that generates a session key amongst the participants and it introduces an authenticated key exchange protocol which is a one round tri party repo process, and allows the communication securely.

In paper[3] Functional design of healthcare which is a nfc based system has proposed the improve access to patients medical documents and history which is updated automatically, and in our record the knowledge is been added.

In paper[4] a scheme is implemented that is the efficient sharing of medical data. To overcome the user’s privacy issues and the limitation of computing power of smart terminals attribute based encryption is utilized to enable data sharing in this system. By this the security and the performance analysis of the IOT is improved as it securely enables the data processing and sharing.

In paper[5]the author emphasizes the need to preserve the patients privacy during the collection of data. Identity based encryption [IBE] which is similar to the Boneh-Franklin cryptosystem in terms of security algorithm and has the root on bilinear maps of elliptic curves is the model used for encryption which allows sharing of data on big data platform efficiently by providing data for research and future references maintaining the privacy of patient.

In paper[6] for the transaction of the payment through mobile, the author have developed a security solution over NFC radio interface. NFC doesn’t have any specification related to the communication security. Therefore the devices which have limited memory and CPU resources, the author uses symmetric cryptographic fundamentals as the solution, which leads to the security of Near Field Communications and also proves that the solution is simple, cost effective, scalable and also minimizes the refinement of computational overheads.

In paper[7] authors have developed a technology of NFC which is a clarification ,that prevents medication errors such as false medication, wrong patient, miscalculated time, erroneous dose and misguided routes. During the administration stage of medication ,error occurs which would lead to series issues in the medication process related to a patient, deteriorating the condition of the person.In such case the application alarms the staff or the nurse prior to carry out the aid to the patient and also provides an alternative to nurse which allows him/her to alarm the physician who has prescribed the aid.

III. PROPOSED APPROACH

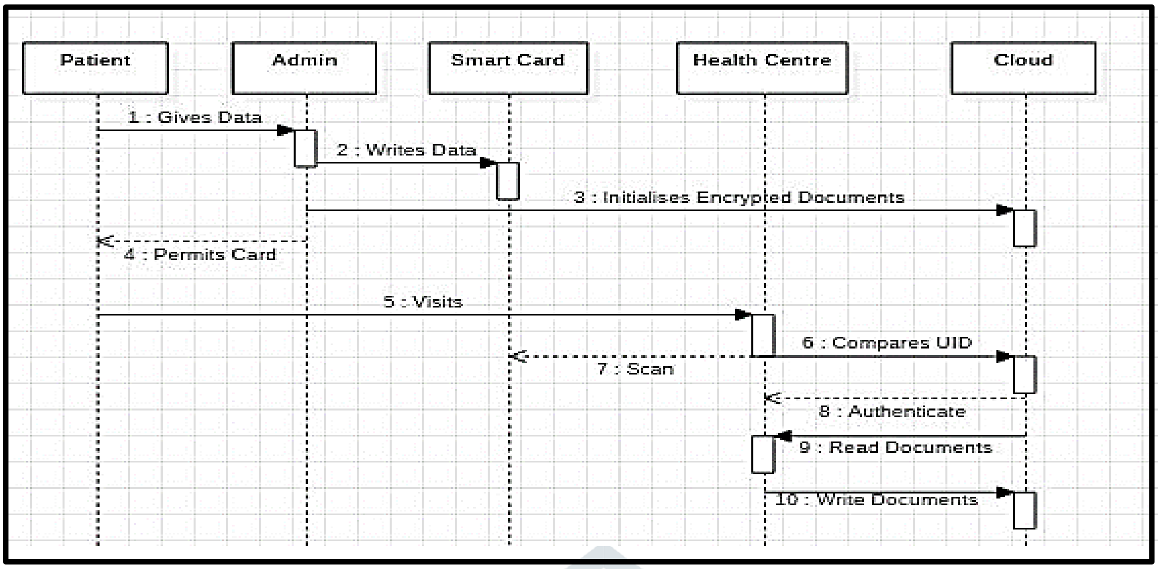


Fig.2: Sequence diagram of the Proposed System.

3.1) Problem Statement

Designing a smart healthcare system by implementing NFC and AWS to authenticate patient's identity and store their data securely. The legitimate users will have access to their medical documents which is stored in an encrypted form in S3 which avoids unauthorized access.

3.2) Sequence of Operation of the system(Fig.2)

1. Patient provides with all the information needed by the admin in order to issue the smart health card (MIFARE).
2. The Admin of the System write the data i.e the patient's name and the unique key (UID) provided to him/her on the smart health card
3. Using the AES algorithm, the Admin encrypts the UID provided by the patient as well as writes it on a blank NFC card and initializes the document (PDF) on Amazon cloud. The PDF, stored in a bucket on AWS will contain all the medical information and reports of a patient. The name of the pdf will be set exactly the same as the UID of the patient.
4. The Admin will thereafter sanction the NFC smart health card to the respective patient.
5. The patient visits the healthcare center with the smart health card for diagnosis or regular checkup.
6. The System installed in the healthcare center scans the smart health card and fetches the UID of the patient.
7. The System compares the scanned UID with the data (name of the pdf) stored on AWS.
8. If the UID of the patient matches with the name of the pdf, the patient is authenticated and the data is retrieved from the cloud.
9. The data retrieved from the cloud will be available on the concerned authority's(doctor/nurse/hospital staff) device for a read operation.
10. Authorized authorities can also perform a write operation on the data if needed.

3.3) Algorithm

In proposed work, we have enforced double security by encrypting the data twice using the AES 256 algorithm. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that uses a block cipher in which every message is mapped as an integer. The implementation of AES 256 algorithm Encryption process involves 13 general rounds. Each round comprises of four Subprocesses:
Byte substitution, ShiftRows, MixColumns, AddRoundKey.
The Final Round (14th) consists of three Subprocesses SubBytes, ShiftRows, AddRoundKey.
The decryption process of AES Ciphertext is the converse of the encryption process. Each round comprises of four Subprocesses: AddRoundKey, Inv.MixColumns,Inv.ShiftRows, Inv.Byte substitution.
There are a total of three 256-bit keys involved in the overall process in which two keys are provided default by the Amazon cloud service. The third key is a derived key from details provided by the patient along with the secret key of AWS.

Pat_Priv_key= Unique Identity of the patient + AWS Secret
Key
= P_UID + AWS_Skey

Health_Rec_Name= P_Name + P_UID

This derived key is used to Encrypt the Identity of the health record before uploading it on the cloud.

Pat_Priv_key →Health_Rec_Name →Encrypted_HRName

This encrypted identity is then used to upload the health record to the cloud where the default encryption takes place.

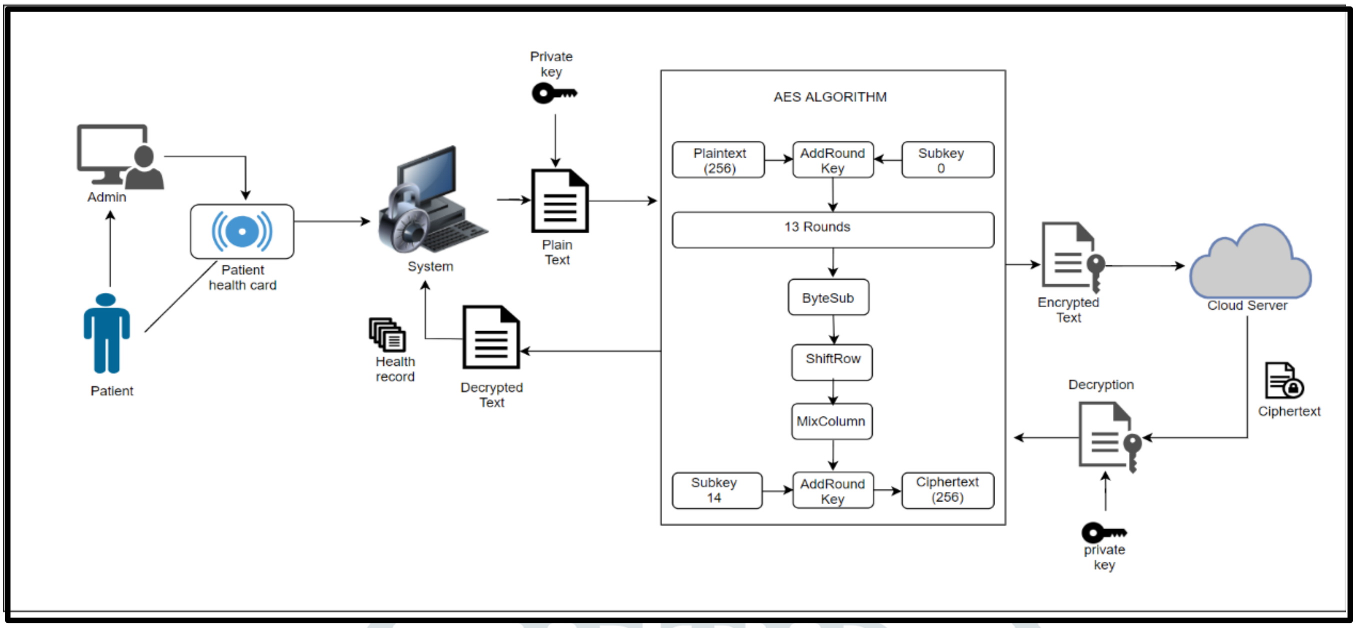


Fig.3: Architecture of the Proposed Systen

In the above architecture, the entire concept of our proposed system is showcased. Patient provides the details to the Admin for registration. Admin writes the data (name and UID) on a blank smart health card (MIFARE). Admin initializes the document (PDF) and permits the card to the patient. The PDF is stored in a S3 bucket, having the capacity of 5TB and with the name matching the combination of the UID and the name of the patient. The combination of the UID and the name of a patient (plaintext) is encrypted using a private key by AES algorithm. The private key is derived from the UID of the patient and their AWS Secret key. AES 256 performs 14 rounds while encrypting and as soon as the smart health card is scanned by the system installed in the healthcare centre, the system compares the UID fetched with the data stored in the bucket on Amazon cloud. If they match, patient gets authenticated and the process of data retrieval begins. The medical data stored on Amazon cloud is also in

encrypted form (by AES), built in security feature provided by AWS which enables double degree of security. The encrypted data which is being retrieved enters the AES cipher block algorithm for decryption. Using private key i.e the access key and the secret key of AWS or the credentials of AWS the encrypted data is again converted into plaintext as shown. This decrypted data is visible to doctor/nurse/hospital staff.

IV.SYSTEM ANALYSIS

4.1) Health Application

Health Applications allow all the healthcare providers to connect with each and every patient, dynamically and quickly, reaching out to them according to their convenience. The application (Fig.4) is made easy for end users to use as they can store and access their information and can be used for various systems like phones, tablets etc. The app will engage with the patients, offering them ubiquitous access to the products and services which serve as a part of user experience. The user can store their past health records and the staff of the hospital can directly upload the patient’s current reports and data according to the profiles. Basically, all the health records would be maintained which can be accessed anywhere and anytime by the patients, doctors or recommendations can be provided. The Data will be secured as it would be encrypted so there would be no security issues. With one touch click on “EMERGENCY" icon on Home screen, Emergency SMS of your approximate location can be sent to the nearby ambulance services and even the notifications would be sent to nearby hospitals.

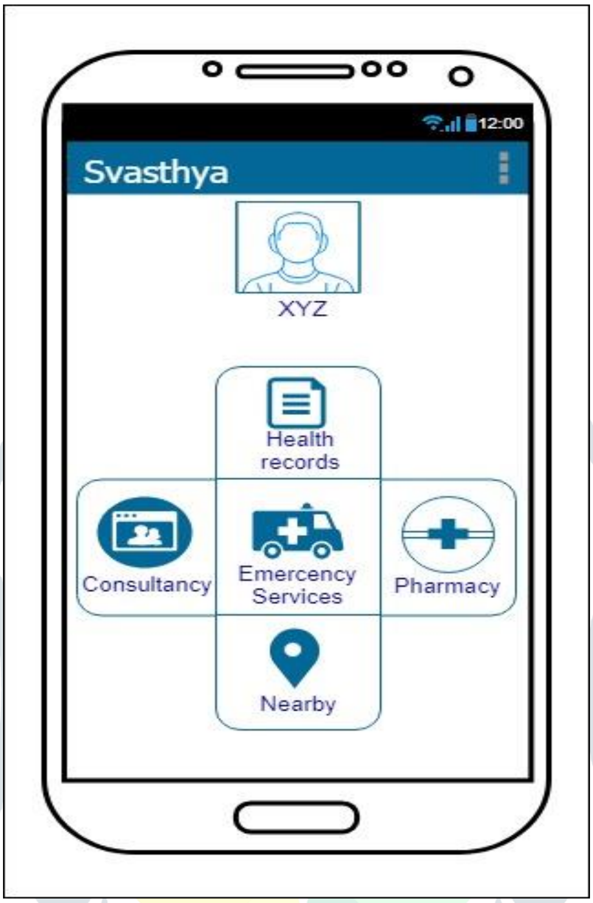
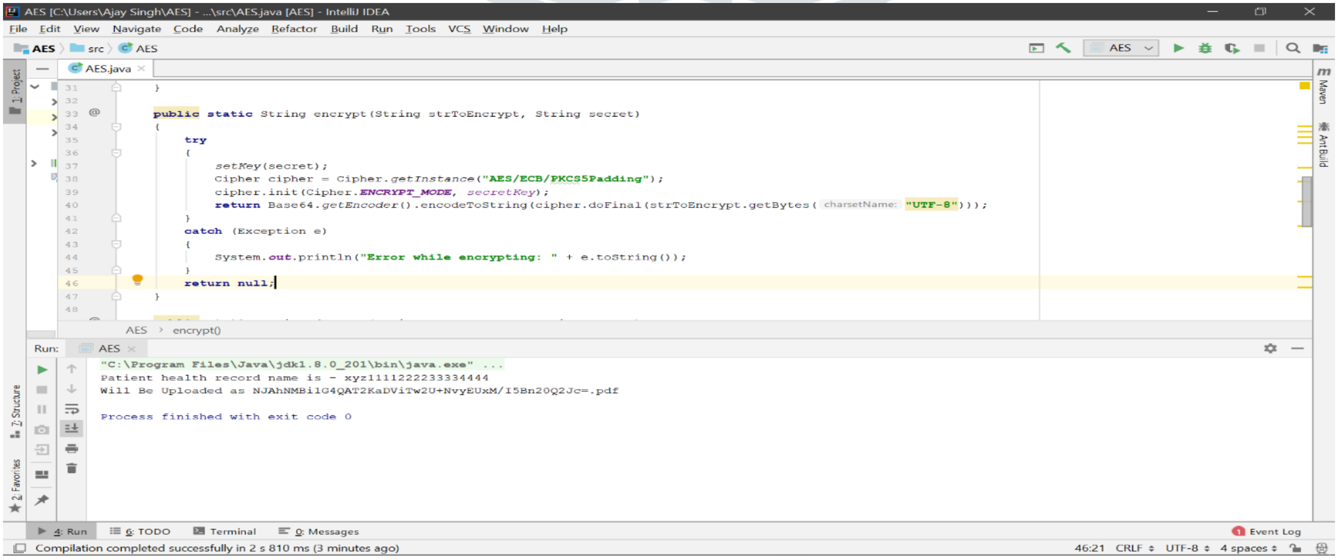


Fig.4: Snapshot of the mobile Application.


AES [C:\Users\Ajay Singh\AES] - ...\src\AES.java [AES] - IntelliJ IDEA
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
AES src AES
AES.java
1: Project
7: Structure
2: Favorites
Maven
Ant Build
AES › encrypt()
Run: AES
4: Run
6: TODO
Terminal
0: Messages
Event Log
46:21 CRLF UTF-8 4 spaces

```
}

public static String encrypt(String strToEncrypt, String secret)
{
    try
    {
        setKey(secret);
        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);
        return Base64.getEncoder().encodeToString(cipher.doFinal(strToEncrypt.getBytes( charsetName: "UTF-8")));
    }
    catch (Exception e)
    {
        System.out.println("Error while encrypting: " + e.toString());
    }
    return null;
}
```

```
"C:\Program Files\Java\jdk1.8.0_201\bin\java.exe" ...
Patient health record name is - xyz111122223333444
Will Be Uploaded as NJAhNMBi1G4QAT2KaDViTw2U+NvyEUxM/I5Bn20Q2Jc=.pdf

Process finished with exit code 0
```

Compilation completed successfully in 2 s 810 ms (3 minutes ago)

Fig.5: Snapshot of Encryption of health record name

4.2) System encryption

Fig 5. Shows the process of encrypting the health record name to a 256 bit cipher-text using the AES algorithm.

IV. CONCLUSION

We have proposed a Cloud-based NFC Smart Health Card System with the aim of providing quality-focused patient-centered care. Every NFC card (MIFARE) has a unique identification number (UID) of individual which helps the system to keep data confidential and by card simulation technique the data is available within milli-seconds, which is helpful in the case of an emergency. We use AES 256 algorithm to encrypt the UID and the Name provided by the patient. Moreover, by saving his/her data under the same name on the cloud makes it easier to retrieve the data while raising the level of security by avoiding the Man-in-the-Middle attack. Introduction of AWS cloud in our system helps to store a large amount of medical data and provides security of the information as it protects it from unauthorized users by using AES and SSL protocol. It also enables the patient to access the data anywhere and anytime.

V. REFERENCES:

1. Renyou MEI, Xiaoli QIU, *"General Medical Information Management System Design Based on Cloud Computing,"* International Conference on Network and Information Systems for Computers 2016.
2. Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman,M. Shamim Hossain, Ahmad Almogren, and Atif Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare.
3. lthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography"2017
4. Danco Davcev, Goran Jakimovski, "Ergonomics Design of Healthcare NFC-based System, Procedia Manufacturing", Volume 3, 2015, Pages 5631-5638, ISSN 2351-9789.
5. Kissi Mireku Kingsford, Fengli Zhang, Mensah Dennis Nii Ayeh, Armah MaryMargaret," A Mathematical Model for a Hybrid System Framework for Privacy Preservation of Patient Health Records,"2017.
6. *Mohamad Badra, Rouba Borghol Badra,"A Lightweight security protocol for NFC based mobile payments," Procedia Computer Science, Volume 83, 2016, Pages 705-711.*
7. *Maali Alabdulhafith, Srinivas Sampalli,"NFC based framework for check-ing the five rights of medication administeration,"Procedia Computer Science, Volume 37, 2014, Pages 434-438.*
8. Mukhtar M. E. Mahmoud, Joel J. P. C. Rodrigues, Syed H. Ahmed, Sayed C. Shah, Jalal Al-Muhtadi, Valery Korotaev, Victor H. Albuquerque, *"Enabling Technologies on Cloud of Things for Smart Healthcare," 2018.*
9. Abdel Fattah Awad, Mohammed Bakri Bashir, Tawheed Hassan Ahmed , Adil Yousif, *"Distributed Medical Image Retrieval*
10. *Techniques: A Review",* Sudan Conference on Computer Science and Information Technology (SCCSIT) 2017.
11. Stephanie Baker, Wei Xiang, Senior Member, IEEE, and Ian Atkinson *"Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities,"* 2017.
12. Wenbing Zhao , Xiong Luo and Tie Qiu "Smart Healthcare" Appl. Sci. 2017
13. Java Card™ Platform Security, http://www.oracle.com/technetwork/java/javacard/documentation/javacardsecuritywhitepaper-149957.pdf
14. A. Vasquez , M. Huerta , R. Clotet ,R. Gonzlez , D. Rivas and V. Bautista,"Using NFC Technology for Monitoring Patients and Identifica-tion Health Services", Conference Paper in IFMBE proceedings ,October 2014.
15. Utsav Jambusaria, Neerja Katwala, Dharmeshkumar Mistry,"Secure smartphone unlocking using NFC",Procedia Computer Science, Volume 45, 2015, Pages 465-469.
16. B. Asma Khatoon and Dr. Ataul Aziz Ikram,"Performance Evaluation of RSA Algorithm in Cloud Computing Security", International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 12 No. 1 Nov. 2014, pp. 336-345.
17. NFC and working of it, https://www.androidauthority.com/what-is-nfc-270730/
18. Amazon Cloud Computing [AWS] https://aws.amazon.com/what-is-cloud-computing/
19. Working on Android Identifiers https://developer.android.com/training/articles/user-data-ids
20. D. Sethia, D. Gupta, T. Mittal, U. Arora and H. Saran, "NFC based secure mobile healthcare system," 2014 Sixth International Conference on Communication Systems and Networks, Bangalore, 2014, pp. 1-6