Vol 8. No. 3 Issue 2 – October, 2015
African Journal of Computing & ICT

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781

www.ajocict.net

Secure Approach for Healthcare System with Integration of NFC and Cloud Computing

G.D. Ganesh & A. D. Potgantwar
Department of Computer Engineering
Sandip Institute of Technology and Research Centre
Nashik, Maharashtra, India
gdighe00@gmail.com, amol.potgantwar@sitrc.org

ABSTRACT

Main anxiety in the data sharing based systems is security and efficiency. Online network of Healthcare system is also comes under its shelter. Cipher Text-Policy Attribute-Based Encryption (CP-ABE) and use of Near Field Communication Technology (NFC) handles these aspects effectively. NFC Technology is a small-range high-frequency wireless communication technology. RFID technology (Radio Frequency Identification Technology) has been used in NFC tag. This NFC tag stores some amount of information in it with a unique identification number, therefore, it is useful in many different real-time applications likes transport system, the smart postures system etc. One main issue in data sharing systems is the application access policies and support for policy updates. Using NFC in Healthcare Application System (HAS) and the key attribute of NFC Tag ID for Cipher Text-Policy Attribute-Based Encryption removes existing disadvantage of key escrow problems. NFC technology allows intelligent devices; NFC Tag, NFC Enable Smart Phone, MIFARE card in hospitals is a big step for the automation of the healthcare system.

Keywords: CP-ABE, NFC, RFID, HAS, MIFARE card

African Journal of Computing & ICT Reference Format:
G.D. Ganesh & A. D. Potgantwar (2015): Secure Approach for Healthcare System with Integration of NFC and Cloud Computing.
Afri J Comp & ICTs Vol 8, No.3 Issue 2 Pp 171-176

1. INTRODUCTION

In the hospital during patient's treatments doctor needs to operate on every patient differently because every patient may have a different illness and different symptoms are chances of getting confusion between patient's disease and treatment. Along with this issue patient, health records [1] which depict patient treatment history and reports are retained on paper which is difficult to maintain and unreliable for a longer period. Building healthcare system [2], [3], [4], [5], [6] using NFC Technology it may protect patients record and helps the doctor to side out such fatal mistakes while doing treatment. But security is a major concern in data storage. CP-ABE provides a cryptographic solution for data security on the cloud network.

Use of NFC technology makes the insurance claim nation faster with complete transparency and credibility by connecting it with unique ID of NFC tag and CP-ABE encryption standard for security. NFC is a high frequency secure wireless communication technology [7]. NFC works in a short range of about 4 inches between two devices. NFC operates at 13.56 MHz NFC operates several data broadcast rates; 106 kbps, 212 kbps, and 424 kbps. NFC enables communication between the tags and electronic equipment, which means that reader and writers [8]. NFC is already used for applications related to financial payments [9] and ticketing. We are proposing a new use of NFC mobile devices to access medical external tags to identify patient health cards.

NFC allowing users to do safely contactless transactions, the spontaneous digital content, access and connect electronic devices simply by touching or in close taking devices proximity [8]. NFC technology allows three modes: read / write mode, peer-to-peer mode, and card emulation mode [10]. Radio Frequency Identification Technology (RFID) has been used in NFC tag. This RFID technology and various wireless technologies are able to support users in different service sectors [11]. An application on an NFC device can read data from and write data to the tag detected using read-write mode operations [8]. This tag also has to run different applications with the support of NFC device. The supported data rate in this mode is 106 Kbit / s. The second mode is peer to peer mode. In this mode, data are exchanged between the two devices. This mode is based on ISO 18092 standards and rope two communication modes: passive and active.

In passive mode, it begins by creating the communication RF signal and the target respond to the command of the sender. In the active mode, to start communication, it must generate their RF signals. The NFCIP-1 initiator starts communication session and target responses to the control of the initiator. The third operating mode is the emulation mode of the card. In emulation mode, the camera will stop producing a RF wave and convert into passive mode. NFC has two types of communication. One is the active communication mode and the passive communication. In the active mode of communication throughout the data transmission procedure and the parties themselves generate a carrier.

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

In active mode communication information are sent using the modulation amplitude shift keying (ASK). This means that the base signal RF (13.56 MHz) is moderate with numbers in accordance with a coding arrangement. If the baud rate is 106 bauds, the encoding device is the encoding said, modified Miller. If the transmission rate is greater than 106 k Bauds Manchester coding device is applied. Attribute-based encryption (ABE) is a promising approach that achieves a cryptographic access control to fine-grained data [12], [13], [14]. It provides a way to set access policies [15], [16] based on different attributes of the requester, the environment, or the data object. In CP-ABE Standard encryptor defines their own attribute set over a group of attributes that must be possessed with decryptor in order to decrypt the ciphertext [17], [18], [19] and enforce it on the contents [20], [21]. Thus, each user with a different set of attributes is authorized to decrypt the individual data items by the security policy. It eliminates the need to depend on the data storage server to prevent unauthorized data access. Also, it removes existing disadvantage of key escrow problems [22].

2. RELATED WORK

2.1 BSW CP-ABE

In BSW CP-ABE [13] scheme, If user inputs valid set of attributes then only he will be able to retrieve encrypted data. But, secure element concept has not been considered in this scheme.

2.2 YWRL-CP-ABE

In YWRL CP-ABE [23] scheme has suggested a solution to give rights to revoke user with different attributes in less effort. It uses proxy re-encryption with CP-ABE standard scheme to achieve expected output.

In the previous health surveillance system, the doctor needs to attend patients when they take medication at home. NFC medium formed the NFC Data Exchange Format (NDEF) and NFC tag operations. NFC tags are contactless cards based on RFID architecture [24]. NFC phone may communicate with RFID tags distributed by [25] environment. Little research has focused on improving the value of patients' treatment. For example, storage of the separate drug dosing information and the avoidance of a pharmacy out of stock in the Voter circumstances [26]. Smart poster applications are one of the biggest important applications of this mode. In this application, users are able to read data from NFC posters and spend their NFC mobile strategies. Review of Literature Survey [27], depicts NFC has been used in different service sectors like smart posters system, payment services system, electronic wallet system, loyalty management system etc.

2.3 Existing Systems Based On Nfc Technology

Following are some application areas where NFC Technology has been used for automation.

- Public Transport System
- Mobile Payment Using NFC Technology [28]
- Entrance Control System
- NFC in Tourism
- Smart Postures

2.3.1 Public Transport System

Nowadays many countries are using NFC in public transport systems. Tapping your phone with kiosk gives you up-to-date information about schedule and delays. Contactless cards which used for ticketing options. Many transport agencies from worldwide countries have been using NFC-enabled mobile phones.

2.3.2 Mobile Payment System

The system provides adequate security level for payments [28], ubiquitous implementation using new available technical components.

2.3.3 Entrance Control System

Entrance controls system validates the entry into transport control system, monitoring in the railway station, corporate offices etc. It reduces efforts required for manually checking. NFC enables the right way to control and validate or invalidate tickets or passes in the entrance control system. Tickets can be checked or validate it by touching a control device (like an RFID, NFC Tag etc.) with your mobile phone.

2.3.4 NFC In Tourism

NFC technology is a key point for various stakeholders in tourism industry sector. NFC device provides more information on the spot about different places and makes all things easier for tourists. NFC tags placed on monuments for checking can give more information about its monument. NFC technology will be a key point for various stakeholders in the tourism industry.

2.3.5 Smart Postures

NFC smart posters are the objects in or on which readable NFC tags have been placed. Various smart posters are developed using secure NFC tags. It can be done by using web server for securely retain the details of the poster.

3. ARCHITECTURE OF PROPOSED HEALTHCARE APPLICATION SYSTEM WITH NFC TECHNOLOGY, CP-ABE ENCRYPTION STANDARD AND CLOUD NETWORK

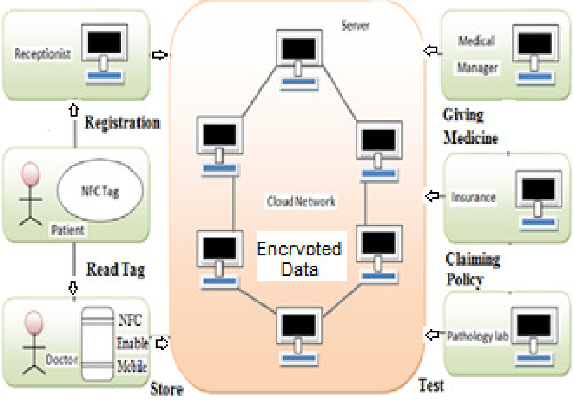

Fig: 1. Architecture of Proposed Healthcare Application System with NFC Technology, CP-ABE Encryption Standard and Cloud Network

If the patient comes first time in the hospital for treatment, his information will be filled at the receptionist counter such as names, addresses, phone numbers and relatives phone number, initial amount to be filled in the card, ward number; bed number etc. such way the patient will be admitted. After registration, the patient will be given the NFC enabled wristband tag and MIFARE card. At the same time all that information will be stored in encrypted form with CP-ABE standard scheme.

If in case the admitted patient has been registered earlier, then he will be given the wristband with unique ID contains in it and MIFARE card directly and will be allotted with an appropriate bed number. NFC tag ID will become the patient's unique identification number for further reference and CP-ABE Standard to provide security for all data over the cloud. During patient registration his/her claim nation sends to the respective insurance agency via SMS and Email for speed up the claim nation procedure, increasing transparency and credibility in the healthcare. While claiming insurance when the patient admitted to the hospital, his detail information includes his Policy No, Name, Disease, Hospital Name etc. will be sent to the respective insurance agency. When doctor will go for the checkup he will just tap his NFC-enabled mobile phone to the patient wristband and he will get all the details regarding patient's disorder or disease, consultation with the doctor, prescriptions given previously, the test conducted etc. After checkup new prescription given by doctor will be stored on the server for further reference. Doctor himself can see the patient's previous treatments reports on his NFC enable smartphones and write which test to be conducted. Detail Architecture Representation of the system as shown in Figure 1.

To take medicine from the store he can use his MIFARE card for payment. Medical manager taps his/her NFC enable mobile phone to retrieve information of which medicine has to give to the patient. He also receives SMS about which medicines have to give a patient. The MIFARE card will be swapped and the respective charges will be deducted from amount and changes will be stored on a server at regular interval. Medical manager and the pathologist can only retrieve information about prescription and tests to be conducted respectively. When the patient will be discharged all his dues like rent of the bed etc. for appropriate number of days he or she spent in the hospital, and doctors consulting fees will be calculated. After clearing all the dues, he will be discharged from the hospital. This all patient's record will be accessible in any hospital for their reference. It results into reduces the headache of patients to keep their previous treatments record with him and the doctor can refer it with a single touch. This globalizes accessibility makes the healthcare very effective and it takes less time and efforts.

3.1 Work Model Of Healthcare Application System

Nurse/Receptionist will launch the application of NFC Based Hospital Management System by providing the IP address of the server. Once connected to the server. NFC Tags' unique identification number of the affected patients is permanent and stored in the server.

The doctor must log successfully to view the patient's request. The doctor is able to see the patient's application form and patient information. If the patient is already registered, then the doctor can also see patients' previous symptom and medication prescribed for this symptom. Doctor prescribed the patient and sends the prescription to the mobile phone of the nurse and medical manager. Lastly, Nurse will check the payment and if it is paid, receptionist will clear the account.

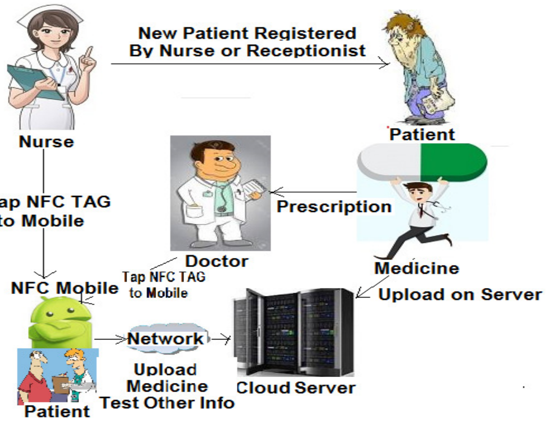

Fig: 2.Work Model of Healthcare Application System.

4. KEY INCENTIVE FOR HEALTHCARE APPLICATION SYSTEM

4.1 Secure Element

The proposed Healthcare application system secure element [29], [30] is based on the following assumptions: The SE is part of the NFC Tag, The Cloud is part of the HAS, The HAS manages the SE/NFC Tag, Hospitals are linked to the HAS, Communication is carried over a single channel: HAS, NFC Reader, and NFC Tag.

4.2 Security Over Cloud With Cp-Abe Standard Scheme

Cipher Text Policy Attribute-based encryption (CP-ABE) is a promising approach that achieves a cryptographic access control to fine-grained data [12], [13], [14]. It provides a way to set access policies based on different attributes of the requester, the environment, or the data object. CP-ABE Standard enables an encryptor to define the attribute set over a group of attributes [31], [32] that a decryptor need to possess to decrypt the ciphertext [33], [34] and apply it on the contents [20], [21]. Thus, each user with a different set of attributes is authorized to decrypt the individual data items by the security policy.

5. DATA SHARING ARCHITECTURE

Following Fig. 3 shows the architecture of the data sharing system and their entities.

5.1 Key Generation Center (KGC)

It is a key authority which is use to give public and secret parameters. It also has control for revoking, issuing, and updating the attribute set for different users [35]. It gives different authorized access rights to users based on their attributes.

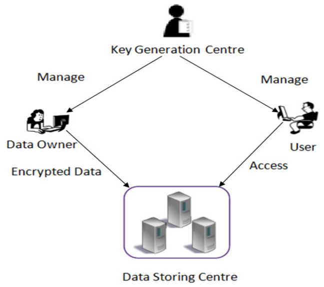

Fig: 3.Architecture of Data Sharing System.

5.2 Data Storing Center

Data Storing Center provides a data sharing service. It is responsible for monitoring external user access to data storage and provision of corresponding content services. The data storage center is another key authority that generates custom user key with the KGC. It also issues and revokes attribute group keys for users attribute, which is used to apply a thin validated user access control.

5.3. Data Owner

It owns data information. Data Owner wanted ease of sharing or cost-saving, therefore, it uploads data into the external storing center for ease of accessibility. It defines access policy and encrypts data before it is delivered to storing center. To access information of user's encrypted content, decryptor needs to possess a set of attributes, only then, he will be able to receive and decrypt the text data.

5.4. Healthcare Management

HAS has depended on the following entities for the good management of patient data:

- Cloud Service Provider (CSP): a CSP has important resources to manage distributed cloud storage servers and to direct its database servers. These services can be used by the HAS to manage patient data stored in the cloud servers.
- HAS: HAS handles interaction between doctor and patient, and use to store and retrieve data over cloud servers.
- Users/Doctor: The users are able to access the data stored in the cloud, according to access rights decided by the system, such as rights to write, read etc. The web interface [36] is used by the users to modify, retrieve, and restore data from the cloud network, based on their access rights.

6. NFC INTEGRATION

The proposed system is based on cloud architecture with NFC Tags/Readers. NFC Tag in HAS is mainly used for authentication of a patient over the cloud, whereas the other section, that is a cloud is used to store patient sensitive information using CP-ABE Standard. Each Patient is identified by a unique ID of NFC Tag, AccID. The AccID is intimated to a Patient when he registers himself with the HAS. Healthcare Application System stores these details in a cloud server. The NFC Enabled mobile device/readers are used to authenticating patients to his account over the cloud network. The communication and all data exchange over the cloud network will be encrypted using CP-ABE Standard.

7. CONCLUSION

This proposed system with CP-ABE standard scheme provides adequate strong security using SE input key. This integration helps a lot to improve healthcare sector. With a use of new emerging NFC technology, all hospitals can better track patient's treatment information. It makes the Healthcare sector with proper management and easier for good treatment of patients with reducing medication errors.

REFERENCES

[37] Divyashikha SETHIA, Shantanu JAIN, Himadri KAKKAR, "Automated NFC Enabled Rural Healthcare for Reliable Patient Record Maintainance." *Global Telehealth A.C. Smith et al. (Eds.)* © 2012.

[38] Amol D. Potgantwar, Vijay M. Wadhai, "A Standalone RFID and NFC based Healthcare System", iJIM Volume 7, Issue 2, April 2013.

[39] Vishal Patil, Nikhil Varma, Shantanu Vinchurkar, Bhushan Patil, "NFC Based Health Monitoring and Controlling System." *IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2014.*

[40] Divyashikha Sethial, Daya Gupta, Huzur Saran, "NFC Based Secure Mobile Healthcare System", 2014.

[41] A Devendran, Dr T Bhuvaneswari and Arun Kumar Krishnan, "Mobile Healthcare System using NFC Technology", Giambastiani, B.M.S.. *Evoluzione Idrologica ed Idrogeologica Della Pineta di san Vitale (Ravenna). Ph.D. Thesis, Bologna University, Bologna,* 2007.

[42] Atluri Venkata Gopi Krishna, Cheerla Sreevardhan, S. Karun, S.Pranava Kumar, "NFC-based Hospital Real-time Patient Management System", 2013.

[43] Ernst Haselsteiner and Klemens Breitfuß "Security in Near Field Communication (NFC)", 2007.

[44] nfc forum Device Test Application Specification, 2013.

[45] Pardis Pourghomi, Muhammad Qasim Saeed, Gheorghita Ghinea, “A Secure Cloud-Based Nfc Mobile Payment Protocol (IJACSA).” *International Journal of Advanced Computer Science and Applications, Vol. 5, No. 10.* 2014.

[46] Roland, Michael Hölz, “Technical Report Evaluation of Contactless Smartcard Antennas”, 2015.

[47] Amol D.Potgantwar, V.M.Wadhai, "Location Based System For Mobile Devices With Integration of RFID and Wireless Technology-Issues and Proposed System”, 2011 International Conference on Process Automation Control and Computing, 2011 PP 1-5.

[48] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”, 2009.

[49] John Bethencourt, Amit Sahai, Brent Waters. “Ciphertext-Policy Attribute-Based Encryption”, 2009.

[50] Mrs. Deepali, A. Gondkar, Mr. V.S. Kadam, “Attribute Based Encryption for Securing Personal Health Record on Cloud”. *2nd International Conference on Devices, Circuits and Systems (ICDCS)* 2014.

[51] Chia-Hui Liu, Fong-Qi Lin, Chin-Sheng Chen, Tzer-Shyong Chen, “Design of secure access control scheme for personal health record-based cloud healthcare service Security and Communication Networks.” *Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1087* 2014.

[52] Sebastian Zickau, Dirk Thatmann, Tatiana Ermakova, Jonas Repschl ager, R¨udiger Zarnekow, Axel K¨upper, “ Enabling Location-based Policies in a Healthcare Cloud Computing Environment.” *IEEE 3rd International Conference on Cloud Networking (CloudNet)* 2014.

[53] Peng-Loon Teh, Huo-Chong Ling, Soon-Nyean Cheong, “NFC Smartphone Based Access Control System Using Information Hiding”, *IEEE Conference on Open Systems (ICOS), December 2 - 4, Sarawak, Malaysia* 2013.

[54] Suhair Alshehri, Stanisław P. Radziszowski, Rajendra K. Raj, “Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption”. *IEEE 28th International Conference on Data Engineering Workshops* 2012.

[55] Lan Zhou, Vijay Varadharajan, Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage”. *IEEE Transaction on Information Forensics and Security, Vol. 8, No.12,* 2013.

[56] Ming Li, Shucheng Yu, Yao Zheng Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”. *IEEE Transaction on Parallel and Distributed Systems, Vol. 24, No.1.* 2013.

[57] Linke Guo, Chi Zhang, Jinyuan Sun, “A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks”. *IEEE Transaction on Mobile Computing, Vol. 13, No. 9.* 2014.

[58] Junbeom Hur, “Improving Security and Efficiency in Attribute-Based Data Sharing”. *IEEE Transaction on Knowledge and Data Engineering, Vol. 25, No 10.* 2013.

[59] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou,”Attribute Based Data Sharing with Attribute Revocation”, ASIACCS’10 April 13-16, 2010, Beijing, China. ACM 978-1-60558-936-7.

[60] Nicolas T. Courtois, Daniel Hulme, Kumail Hussain, Jerzy A. Gawinecki, Marek Grajek, “On Bad Randomness and Cloning of Contactless Payment and Building Smart Cards”. *IEEE Security and Privacy Workshops.* 2013.

[61] Nawaf Alharbe, Anthony S. Atkins, Akbar Sheikh Akbari, “Application of ZigBee and RFID Technologies in Healthcare in Conjunction with the Internet of Things”, 2014.

[62] Steve Hodges and Duncan McFarlane, “Radio frequency identification: technology, applications and impact”. White Paper Series/Edition 1, 2004.

[63] Vedat Coskun, Busra Ozdenizci, Kerem Ok, “A Survey on Near Field Communication (NFC) Technology”. *Coskun, V., Ozdenizci, B., & Ok, K. A Survey on Near Field Communication (NFC) Technology. Wireless personal communications, 71(3), 2259-2294,* 2013.

[64] Pardis Pourghomi, Muhammad Qasim Saeed, Gheorghta Ghinea, “A Secure Cloud-Based Nfc Mobile Payment Protocol”. (*IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 10.* 2014.

[65] Pascal Urien, Selwyn Piramuthu Towards a Secure Cloud of Secure Elements Concepts and Experiments with NFC Mobiles”, 2013.

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

[66] T. Ali, M. Abdul Awal, "Secure Mobile Communication in m-payment system using NFC Technology". *IEEE International Conference on Informatics, Electronics & Vision.* 2012.

[67] Yan Zhu, Di Ma, Chang-Jun Hu, Dijiang Huang, "How to Use Attribute-Based Encryption to Implement Role-based Access Control in the Cloud". 2013.

[68] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases. IEEE Transaction on Parallel and Distributed Systems" Vol. 25, No. 2. 2014.

[69] An-Ping Xiong, Qi-Xian Gan, Xin-Xin HE, Quan Zhao, "A searchable Encryption of CP-ABE Scheme in Cloud Storage". 2013.

[70] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", *IEEE Transactions on Information Forensics and Security.* 2015.

[71] V.Sreenivas, C.Narasimham, K. Subrahmanyam, P.Yellamma, "Performance Evaluation of Encryption Techniques and Uploading of Encrypted Data in Cloud". 2013.

[72] Yasaman Amannejad, Diwakar Krishnamurthy, Behrouz Far, "Managing Performance Interference in Cloud-Based Web Services", *IEEE Transactions on Network and Service Management.* 2015.

Authors' Brief

Prof. Amol D. Potgantwar is working as Head of Department of Computer Engineering, Sandip Foundation's, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India. The focus of his research in the last decade has been to explore problems at Near Field Communication and it's various application In particular, he is interested in applications of Mobile computing, wireless technology, near field communication, Image Processing and Parallel Computing. He has registered patents like Indoor Localization System for Mobile Device Using RFID & Wireless Technology, RFID Based Vehicle Identification System and Access Control into Parking, A Standalone RFID and NFC Based Healthcare System. He has recently completed a book entitled Artificial Intelligence, Operating System, and Intelligent System. He has been an active scientific collaborator with ESDS, Carrot Technology, Techno vision and Research Lab including NVIDIA CUDA, USA. He is a member of CSI, ISTE, and IACSIT.
Email: amol.potgantwar@sitrc.org

Mr. Ganesh G. Dighe has completed BE Degree in Computer Engineering and pursuing Master Degree in Computer Engineering, Sandip Foundation's, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India.
Email: gdighe00@gmail.com