Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Patient Privacy E-Health Care System Using RFID and Cloud

Anagha Wagh, Rozmin Shaikh, Pratiksha Vyawahare, Preeti Yadav, Prof. Ajit P. Shiralkar
Department of Computer Engineering, G.E.S.R.H.SAPAT.C.O.E
Nashik, Maharashtra, India

Abstract*— Today in India there is no such system which would maintain the medical data of patients centrally. All the data of the patient is maintained in files and every time the patient has to carry his medical file with him. Now the problem with system is that if the patient is at the remote location then he cannot access his documents. Hence we have come up with a solution which would help patients to maintain their files centrally on the cloud and can be accessed anywhere in the world. In our system a RFID card would be issued to every patient for maintain the integrity of the data. At that time the doctor would enter all the basic details of the patients such as age, blood group contact details etc on the server. Now this data would be stored onto the server. The doctor would examine the patient and all his diagnosis would be stored onto the server. Now if the doctor prescribes any kind of medical test to the patient then that details would also be maintained on the server. This system can also useful in the medical test, billing system and updation of the information is done on cloud server centrally.

***Keywords*— Cloud computing, E-health, Privacy, RFID, Attribute Based Encryption (ABE) Algorithm**

I. INTRODUCTION

Radio Frequency Identification (RFID) [1] is a state of the art technology that uses electromagnetic fields attached to a tag to identify objects. These tags are typically used for product tracking and product identification. RFID is a growing trend in the health care industry, driven by a greater emphasis on patient safety than has ever been seen before. RFID technology can help ensure that every patient is treated properly and that patients get the services they pay for. There are two common types of RFID tags, active and passive. Active tags are more expensive, because they have an internal power source and allow two way flow of information, from tag to server and back. Active tags can transmit over 100 feet. Passive tags are less expensive, but must be activated by an outside power source. They are shorter in range than active tags, and only transmit data from RFID to server. Radio frequency identification (RFID) has been used in a number of practical applications, such as improving supply chain management, tracking household pets, accessing office buildings, and speeding up toll collection on roadways. RFID is used to automatically identify people, objects, and animals using short range radio technology to communicate digital information between a stationary location (reader) and a movable object (tag).[1]RFID technology can be used to track products in a manner similar to using bar codes for product identification, but RFID also carries additional benefits.

In this paper, we focus on RFID technology integrated with the process for medicine error reducing, patient (and inpatient) safety enhancement, and health care management. In particular, the issues of performance efficiency, system security and user privacy will be thoroughly investigated. We intend to deliver a patient privacy-aware e-Health system based on passive RFID technology and cloud to simultaneously enhance system efficiency and patient privacy.

Cloud computing is a conceptual model. Based on users needs, data are stored in a super computer through the internet to be processed. And users can access shared resources conveniently (e.g. the internet, server, storage, application, and service) and can achieve rapid configuration and deployment with the least management possible. The Cloud system would be helpful for old age people as they do not have to carry files with them. Moreover as the database is central the information can be accessed anywhere in the world. This enables you to access the patients information even if he is away from his native place. Moreover in case of road accidents or railway accidents the doctor is unaware of the patients previous history. In such a situation the system would be very beneficial as the system would provide the necessary information like blood group, sugar level etc, to the doctor. Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. In this context, the outsourcing of computation and storage resources to general IT providers (cloud computing) has become very appealing. E-health clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models. However, they also bear new risks and raise challenges with respect to security and privacy aspects. Embracing cloud technology in healthcare may be the answer to enabling healthcare organizations to focus their efforts on clinically relevant services and improved patient outcomes. Additionally, it may reduce and even remove the burden of infrastructure management.

II. RELATED WORK

This section provides detail study and analysis of technologies which can be use to cater same concept and its advantages and disadvantages. This chapter also includes shortcomings of these technologies.

© 2015, IJARCSSE All Rights Reserved

A. Existing System Review

In 2009 [2] An RFID and Multi-agent Based System for Improving Efficiency in Patient Identification and Monitoring paper proposes an RFID-based system (named SIMOPAC) that integrates RFID and multi-agent technologies in health care in order to make patient emergency care as efficient and risk-free as possible, by providing doctors with as much information about a patient as quickly as possible. Every hospital could use SIMOPAC with their existing system in order to promote patient safety and optimize hospital workflow. This paper will concentrate on the RFID technology and how it could be used in emergency care in order to identify patients and to achieve real time information concerning the patients' biometric data, which might be used in different points of the health system (laboratory, family physician, etc.). It describe a general purpose architecture and data model that is designed for collecting ambulatory data from various existing devices and systems, as well as for storing and presenting clinically significant information to the emergency care physician

In 2010, two tag coexistence schemes had been proposed by Chien et al. [6] to eliminate medication errors and enhance patient's safety. An on-line based administration protocol and an off-line version are proposed, respectively. However, the authors in [6] did not consider several important security and privacy issues [9]. In addition, the implementation of such two schemes is still doubted as only design ideas are provided. Later, Peris-Lopez et al. [8] implemented an Inpatient Safety RFID System (IS-RFID) which takes into account the information technology infrastructure of real hospital environment and completely covers the whole drug administration process. The system efficiency can be guaranteed as only lightweight cryptography modules such as random number generator and exclusive-or operations are exploited in IS-RFID. However, the insecurity of IS-RFID has been pointed by Yen et al. [11] in 2011.

Next, Yu et al. [12] developed a mechanism utilizing only simple logic gates, e.g. AND, XOR, ADD, to construct an e- Health system. Their scheme is efficient as it does not need any complicated security modules. However, Wu et al. [10] have pointed the robustness vulnerability, i.e. impersonation attacks, of their protocol. A lightweight binding proof protocol is then proposed to overcome the weakness identified in Yu et al.'s algorithm. Then, Lin and Zhang [7] introduced an ECC based solution to prove the coexistence of multiple RF tags and improve patient's drug security. Yet, as the heavy computation cost of ECC module cannot still be afforded on resource constrained RF tags, there remains a doubt on the feasibility of the proposed scheme.

In 2013 [3] Scalable and secure sharing of personal health records in cloud computing using ABE paper proposes an Personal health record (PHR) is an emerging patient centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. This paper also proposes a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, it leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, it focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. The scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

In 2013 [4] A Cloud-based Approach for Interoperable Electronic Health Records (EHRs) present a cloud-based approach for the design of interoperable electronic health record (EHR) systems. Cloud computing environments provide several benefits to all the stake holders in the healthcare ecosystem (patients, providers, payers, etc.).Lack of data interoperability standards and solutions has been a major obstacle in the exchange of healthcare data between different stakeholders.

We propose an EHR system—cloud health information systems technology architecture (CHISTAR) that achieves semantic interoperability through the use of a generic design methodology which uses a reference model that defines a general purpose set of data structures and an archetype model that defines the clinical data attributes. CHISTAR application components are designed using the cloud component model approach that comprises of loosely coupled components that communicate asynchronously. This paper describe the high-level design of CHISTAR and the approaches for semantic interoperability, data integration, and security.

In 2013 [5] Attribute-Based Encryption with Fast Decryption paper proposes an Attribute based encryption(ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes. This functionality comes at a cost. In a typical implementation, the size of the cipher text is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption.

In the conventional method, the patient's record is stored either in the database or the server of the particular hospital or on the server of the third party vendor. In the former method, patient data will not be available to the hospital, which is at a different location. If the server is used by the hospital, other hospitals cannot view patient details when a patient is admitted in the new hospital. A patient-centric data is stored in a cloud environment so that patient, doctors and other relevant people can view the record. Before the data is outsourced to the third party vendor's, data are encrypted. Attribute based encryption is used for encryption as the patient can grant access to the person to whom they want to share data. In order to reduce the key management complexity among patient and other users, multiple security domains are

© 2015, IJARCSSE All Rights Reserved

created. The patient will have complete control of his/her medical records patient can share his/her data to family or friends or to other doctors. This method increases the availability, portability and security of the patient record.

Sahai and Waters proposed Attribute-Based Encryption as a new concept of encryption algorithms. Attribute-Based Encryption can be viewed as a generalization of Identity-Based Encryption. It allow the encryptor to set a policy describing who should be able to read the data. In an attribute-based encryption system, private keys distributed by an authority are associated with sets of attributes and cipher texts are associated with formulas over attributes. A user should be able to decrypt a cipher text if and only if their private key attributes satisfy the formula. For example, a user's identity could consist of attributes describing their university, department, and job function. A party in the system can then specify another set of attributes so such that a receiver can only decrypt a message if his identity S has at least k attributes in common with the set S0, where k is a parameter set by the system.

As specifying a threshold Attribute-Based Encryption system as a collection of four algorithms:

- Setup (k): The Setup algorithm is run by an authority in order to create a new ABE system. Setup takes as input a threshold value, k and outputs a master key MK and a set of public parameters PK.
- Key-Gen(S,MK): The authority executes the Key-Gen algorithm for the purpose of generating a new secret key SK. The algorithm takes as input the users identity, S, as a set of strings representing a users Attributes and the master-key MK and outputs S's secret key SK.
- Encrypt (M, S0,PK): The Encrypt algorithm is run by a user to encrypt a message M, with a target set S0, and the public parameters. It outputs a cipher text, C.
- Decrypt(C, S0, S, SK): The Decrypt algorithm is run by a user with identity S and secret key SK to attempt to decrypt a cipher text C that has been encrypted with S0. If the set overlap $|S \setminus S0|$ is greater than or equal to k the algorithm will output the decrypted message M.

B. Barcode Technology

Barcode technology [13] works of a principle called symbology. Symbology at its basic form is what defines the barcode; it determines the mapping and interpretation of the encoded information or data. This encoding allows the scanning device to know when a digit or character starts and when it stops, similar to a binary representation. We recognize barcodes as an array of parallel lines alternating between white and black lines. Barcode technology provides a simple and inexpensive method of recording data or information in a number of applications. The symbologies of the barcode technology can be arranged or mapped in a variety of ways. A continuous symbology is marked by the characters beginning with a black line and ending with a white line or space, while discreet symbologies have characters encoded as a black line a space and then another black line. In order to read the data of barcode technology it needs to be scanned by a laser and then interpreted. The scanners, or lasers, used to read the barcodes measures the light reflected form the linear barcode technology and can distinguish between the white and black lines. Calibration of the laser and system needs to be done to ensure the proper interpretation of the code itself.

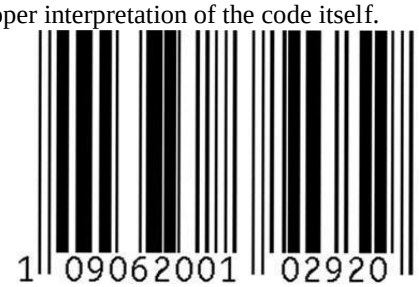

Fig. 1 Barcode Technology

C. Mifare Technology (Smart Card)

MIFARE [14] is the NXP Semiconductors-owned trademark of a series of chips widely used in contactless smart cards and proximity cards. According to the producers, billions of smart card chips and many millions of reader modules have been sold. The technology is owned by NXP Semiconductors. The technology is embodied in both cards and reader. The MIFARE card is fundamentally just a memory storage device, where the memory is divided into segments and blocks with simple security mechanisms for access control. They are ASIC-based and have limited computational power. Thanks to their reliability and low cost, those cards are widely used for electronic wallet, access control, corporate ID cards, transportation or stadium ticketing.

The MIFARE DESFire (MF3ICD40) was introduced in 2002 and is based on a core similar to SmartMX, with more hardware and software security features than MIFARE Classic. It comes preprogrammed with the general purpose MIFARE DESFire operating system which offers a simple directory structure and files. The MIFARE Card was designed to provide additional key diversification, authentication, encryption and portability for advanced applications, unprecedented mobility, heightened security and enhanced performance. HID Globe's next-generation access control platform goes beyond the traditional smart card model to offer a secure, standards- based, technology-independent and flexible identity data structure based on Secure Identity Object (SIO).

D. RFID Technology

Radio-frequency identification (RFID) [15] is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. Utilizing radio frequency waves, an RFID tag can be

© 2015, IJARCSSE All Rights Reserved

applied to or incorporated into a product for the purpose of location and identification. UHF Passive RFID can be read from several meters away and beyond the line of sight of the reader. Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a (RF) signal and can also be used for other specialized functions. The second is an antenna for receiving and transmitting the signal. RFID technology is in increasing use in enterprise supply chain management, improving the efficiency of inventory tracking and management .RFID encapsulates the data accuracy advantages inherent In all types of automatic identification technology (AIT).Additionally, RFID is a totally non- intrusive methodology for data capture (requires no human intervention), is non- line of sight technology, and is a technology that possesses both read and write options within the same equipment item.

RFID (both active and passive) is required to:
1. Provide near-real time in-transit visibility for all classes of supplies and materiel.
2. Provide "in the box" content level detail for all classes of supplies and materiel.
3. Provide quality, non- intrusive identification and data collection that enables enhanced inventory management.
4. Provide enhanced item level visibility

III. THE PROPOSED WORK

In this section, we introduce an efficient and patient privacy-aware e-Health system based on passive RFID and cloud. Radio Frequency Identification (RFID) is a state of the art technology that uses electromagnetic fields attached to a tag to identify objects. The RFID-based procedures are more efficient than traditional e-Health process, patient's information may be explored in the data transmission period and this will cause inappropriate medication use or medical errors. In this, we propose a RFID-based e-Health system which strengthens patient's privacy as well as enhances the efficiency of out-patient clinic procedure using Attribute Based Encryption Algorithm (ABE). In Our system we would be providing a RFID card to every patient. There would be central server cloud where all the patient information would be stored. When the patient visits the doctor for the first time his all identity details would be fetched from the database. Then the doctor would issue the patient an RFID card. Then he would examine the patient and may advice him to undergo some medical tests. The doctor would then upload all this information on the central server cloud or he can upload the patient reports in the cloud .The doctor would also upload the medicine prescribed by him to the patient. The Pathologist can also upload the reports in the cloud. The patient also views his/her own history with the help of website.

IV. CONCLUSIONS

In this paper, we have introduced an e-Health system consisting of RFID-based procedures for enhancing the efficiency of the patient as well as protecting the patient's privacy. Several techniques such as RFID identification and authentication, security algorithm and centralized backup of information are adopted as core designs in the proposed system. All the procedures in our system are secure and easy to implement and use. We believe that our e-Health system will be one of the most promising solutions which simultaneously provide the system robustness, user/patient privacy and the process efficiency on the medical administration.

REFERENCES

[1] Kuo-Hui Yeh1 Hualien,National Dong Hwa University Hualien, Taiwan R.O.C. Taiwan R.O.C."A Patient Privacy-aware e-Health System based on Passive RFID." 2013.
[2] Cristina Turcu, Tudor Cerlinca , "An RFID and Multi-agent Based System for Improving Efficiency in Patient Identification and Monitoring ",volume 6, Nov 2009.
[3] Ming Li , Shucheng Yu, "Scalable and secure sharing of personal health records in cloud computing using ABE" VOL 24,NO.1,Jan 2013.
[4] Arshdeep Bahga,Vijay K. Madisetti, Fellow, IEEE,"A Cloud-based Approach for Interoperable Electronic Health Records (EHRs)", VOL. 17, NO. 5, SEPTEMBER 2013.
[5] Susan Hohenberger, Brent Waters,"Attribute-Based Encryption with Fast Decryption"May 8, 2013.
[6] H.-Y. Chien, C.-C. Yang, T.-C. Wu, "Two RFID-based Solutions to Enhance Inpatient Medication Safety," Journal of Medical System, vol.35, no. 3, pp.369-375, 2010.971.
[7] Q.P. Lin, Q.G. Zhang, "ECC-based Grouping-Proof RFID for Inpatient Medication Safety," Journal of Medical System, DOI: 10.1007/s10916-011-9757-3, 2011.
[8] P. Peris-Lopez, A. Orfila, A. Mitrokotsa, J. C.A. van der Lubbe, "A Comprehensive RFID Solution to Enhance Inpatient Medication Safety," International Journal of Medical Informatics, vol. 80, issue 1, pp.13-20, 2011.
[9] A.-K. Wickboldt, S. Piramuthu, "Patient Safety Through RFID: Vulnerabilities in Recently Proposed Grouping Protocols," Journal of Medical System, DOI: 10.1007/s10916-010-9487-y, 2010.
[10] S.H. Wu, K.F. Chen, Y.F. Zhu, "A Secure Lightweight RFID Binding Proof Protocol for Medication Errors and Patient Safety," Journal of Medical System, DOI: 10.1007/s10916-011-9750- x, 2011.
[11] Y.-C. Yen, N.W. Lo, T.-C. Wu, "Two RFID-Based Solutions for Secure Inpatient Medication Administration," Journal of Medical System, DOI 10.1007/s10916-011-9753-7, 2011.
[12] Y.-C. Yu, T.-W. Hou, T.-C. Chiang, "Low Cost RFID Real Lightweight Binding Proof Protocol for Medication Errors and Patient Safety," Journal of Medical System, DOI: 10.1007/s10916- 010-9546-4, 2010.

© 2015, IJARCSSE All Rights Reserved

[13] C.L. Chen, C.Y. Wu, "Using RFID Yoking Proof Protocol and Barcode technology to Enhance Inpatient Medication Safety," Journal of Medical System, DOI: 10.1007/s10916-011-9763-5, 2011.

[14] C.C. Lo, C.H. Chen, D.Y. Cheng, H.Y. Kung,"Ubiquitous Healthcare Service System with Context-awareness Capability: Design and Implementation using MIFARE Technology"Expert Systems with Applications, 38, 4416-4436, 2011.

[15] H.Y. Chien, C.C. Yang, T.C. Wu, "Two RFIDbased Solutions to Enhance Inpatient Medication Safety," Journal of Medical System, vol.35, no. 3,pp.369-375, 2010.971.

© 2015, IJARCSSE All Rights Reserved