International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.05, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Secure And Dynamic Data Dissemination Protocol For Wireless Network

Pooja Bibe[1], Snehal Divekar[2], Pooja Kumbhar[3], Prachi Waghmare[4], Assistant Prof. Krishna Tayade[5]

[1,2,3,4,5]A Thesis Submitted To The Department Of Computer Engineering
And The Institute Of Engineering And Technology
Of Sppu University In Partial Fulfillment Of The Requirements
For The Degree Of Computer Engineering

ABSTRACT

Today wireless body area networks (WBAN) offers a competent resolution to real-time monitoring and exposure of patient's fitness information. The configuration parameters adjustment requires the data dissemination through WBAN. For data dissemination different protocols are proposed. A multiple one-way key hash chains were proposed for secure data dissemination. In this protocol, SHA-1 based hash functions and AES based encryption was utilized to provide security. However, the complexity of SHA-1 is overhead for WBAN. In this paper the complexity is reduced by introducing simple hash chain based protocol which is utilizing Chaos baker map for security. This Chaos baker map method randomizing data before hashing. Hence, this protocol presents instant authentication and competent to tolerate node compromise. This paper also provides the experimental consequences of Chaos baker map based simple hash function protocol in a network of source restricted sensor nodes, which proves its effectiveness.

Keywords :, Chaos Baker Map ,Data Discovery and Dissemination, Hash Function, SHA-1,. Wireless Body Area Network

I.INTRODUCTION

Maintain the patients data with reports is not easy. There is possibility of misplace patient document. For patients carry reports every time when he comes in hospital is very hectic. Lots of paper work required to maintain patient data. Because of this reasonswedevelopthissystem. Thissystemusefultomaintainpatientdata. Patient data available for hospitals and also for patients. Hospitals can see patient history, report,previoushospitalandprevioustreatment. Patientcanseehisownhistoryand download report.Proposed system provide streamlined operations, upgraded administration and control, predominant patient care, strict cost control and enhanced profitability this all facilities are very beneficial for hospitals. HMS is powerful, flexible, and easy to utilize and is designed and developed to deliver real conceivable benefits to hospitals. More importantly it is backed by reliable and dependable support.

So to implement this model we are using RC6 algorithm. Using this algorithm, we are providing security to avoid it from various types of attacks. So we achieve this by encryption and decryption. There are two types of encryptions. First is symmetric and other is asymmetric. In symmetric algorithm there is only one key used to do

the encryption as well as decryption. In asymmetric encryption two keys are used for encryption and decryption, one is private key and the other is public key.

So security to the patients data is provided at the time of saving as well as transfer.

II.LITERATURE SURVEY

Smart Hospital Management System: An Integration of Enterprise Level Solutions Utilising Open Group Architecture Framework (TOGAF)[1].In year 2010 ,describes a significant factor of the Hospital Information Systems now comprises of various individual inheritance applications that must be incorporated, to deliver a more unified solution. The performance, reliability and other factors of these applications can adjust the performance, reliability and other characteristics of integrated Solution, the Smart Hospital Management System(SHS).The actual evaluation of these parameters of these applications is outside the scope of this document. The SHS being an infrastructure component relies heavily on the actual resources made available to it for its proper functioning, operation and maintenance. This article aims to deliver an approachinarchitectingsolutionswhichcanbeutilisedasframeworktoaddressCommonissuesinintegrationofenterpriselevelsolutions. Themethodologies discussed in TOGAF version 9 are utilised to demonstrate the feasibility of proposed solution.This paper presents the problem space/scenarios, limitations, prerequisites, empowering, risks, sample legacy application design and proposed integration solution presented with TOGAF parts. Increase the number of patients day by day is increase pressure on medical system/ hospital system. On this problem proposed system provide effective solution.

Design and Implementation of Hospital Management System[2].Inyear 2008, describestheproposed framework built upanautomatedsystemthatisutilizedtomanage patient information and its document at administrator level. This was with a view to eliminatetheproblemofinsuitabledataKeeping,in exactports,timewastage instoring,processingandretrievinginformationencounteredbythetraditional hospital system in order to improve the overall efficiency of the particular organization. The ToolsusedtoimplementthesystemareHypertextMarkupLanguage (HTML), Cascading Style Sheets (CSS), Hypertext Preprocessor (PHP), and My Structured Query Language(MySQ). The Proposed system was comparedwith traditional and currently used system usingtheinformationcollectedfromMurabHospital,Ilorin,kwaraState,Nigeria. The design provides excellent patient services and improved information infrastructure.

Design and Implementation of Hospital Management System Using Java[3]. In Year 2015, describes his research work is on design and construction of Hospital Management System (HMS). The system provides the benefits of streamlined operations, enhanced administration and control, superior patient care, strict costcontrolandimprovedprofitability. This system use java for front end development and give connectivity with the back end software because java is object oriented language and it is platform independent.

AnE HospitalManagementandHospitalInformationSystems Changing Trends[4]. In year 2013,describes the rapid growth in Information and Communication Technology (ICT), and the power of Internet has strongly impacted the business and service delivery models of todays global environment. E-Hospital Management Systems provide the benefits of streamlined operations, enhanced administration and control, superior patient

care, strict cost control and improved profitability. Globally accepted medicinal services frameworks need to agree to Healthcare Insurance Portability and Accountability Act (HIPAA) standardoftheUSandthathasbecomethenormoftheHealthcarebusinesswhen itcomestomedicalrecordsmanagementandpatientinformationprivacy and its security. The proposed system focused on performance of Hospital Information System, summarizing the latest commonly agreed standards and protocols like Health Level Seven (HL7) standards for mutual message exchange, HIS components, etc. The study is qualitative and descriptive in nature and most of the data is based on secondary sources of survey data. To arrive at a conclusive idea of the larger picture on E- Hospital Management andHospitalinformationsystems,existingsurveydataandspecificsuccessful case studies of HIS are considered in the study.

With such a large number of redid adaptations of E clinic administration arrangements (E HMS) and Hospital Information frameworks (HIS) accessible in the market, a nonexclusive module shrewd rendition of E Hospital administration framework is charte doutto give an unmistakable comprehension for specialists and industry specialists. From the specific effective contextual analyses broke down in the investigation, the achievement factors and difficulties looked in fruitful EHMS execution are featured. A portion of the obligatory measures like HIPAA are examined in detail for clearness on Healthcare framework usage necessities.

Designing A Web Based Hospital Management System For MOUAU Clinic[5].In year 2015 describes,thispaperisproposinganefficientweb-basedreal-timesystem for the betterment of medical research and analysis, this will bring about ease of accessing medical record and the ease of getting treatment. Today some problemspersistsinthehospitalsuchaslosspatientsmedicalrecordandother important files, this paper is going to tackle these problems. This system will help to replace the manual method, then speeding up the processing, storing andretrievalofinformation,whichwillgreatlyassistthemedicalpersonnelin performingtheirduties. Aboveallthehospitalswillbenefitfromconstantcost savingsasarelots ofincreasedproductivityandoverallefficiency. Thesystem is web based and is designed with mysql database and C hash programming language.

III.RESEARCH METHODOLOGY

In our system, there are two options for registration(for patient and for hospital), once a patient/hospitals gets registered into the system, they are provided with a unique ID which can used as a patients unique identity.

By using the profile of every patient doctor can directly save all the information related to that patient which can be further used by the same/different doctor and can be stored for long period for future use.

As the every detail of patient is stored in the system, there is no need to carry hard copies of reports,other data. It reduces risk of misplacing and also reduce manual work as well as time.

The system also has facility to transfer patients data whenever required.

This can be done by creating a network of different hospitals which are ready to share the data. By which treatment can be decided by the doctor before the patient enters into the hospital which may help to save the life of any patient in emergencies by saving extra time require to do the investigations.

Feasibility can be measure on following basis:

Economical Feasibility:

The system being developed is economic with the hospitals point of view. It is cost effective in the sense that has eliminated the paper work completely. The result obtained contains minimum errors and are highly accurate as the data is required.

Technical Feasibility:

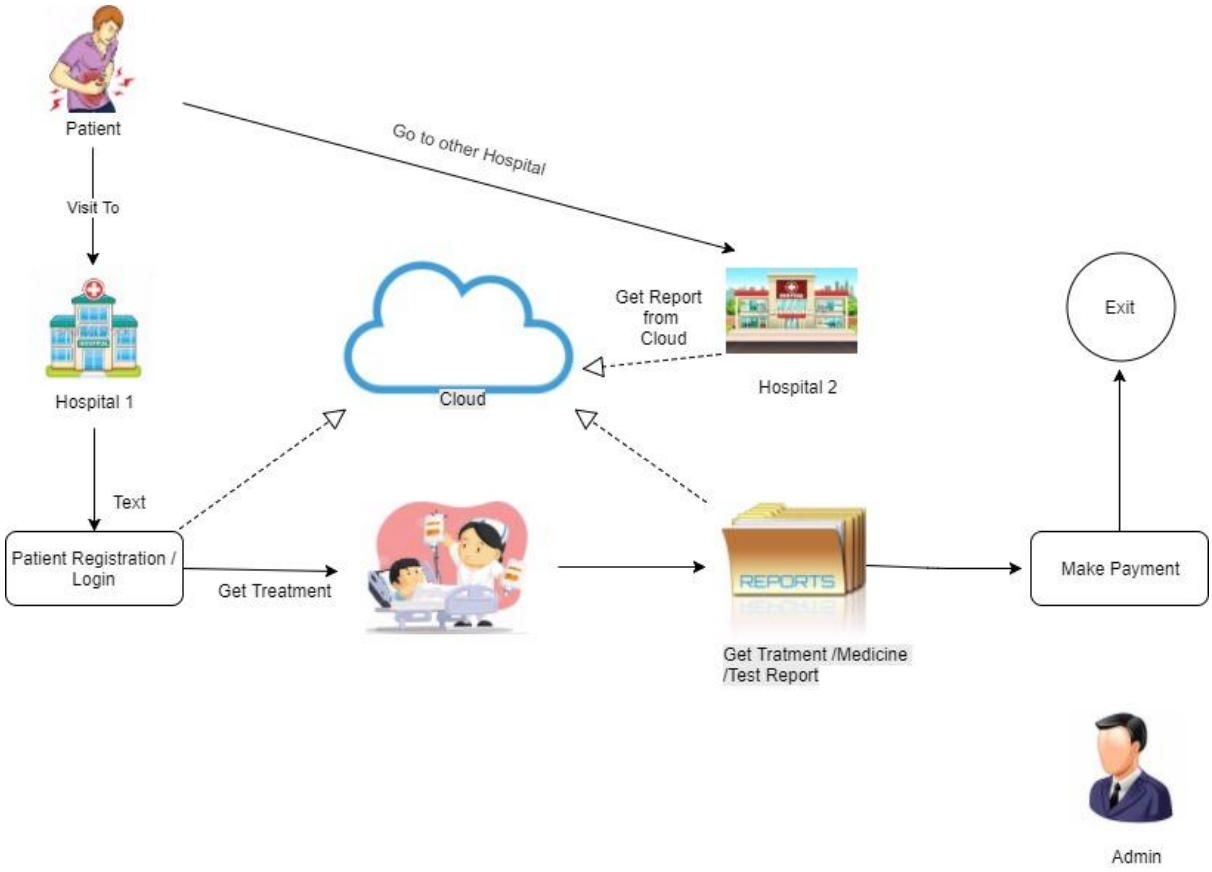
The technical requirement for the system is economic and it does not use any other additional hardware and software.

Behavioural feasibility:The system working is quite easy to use and learn due to its simple and attractive interface.

System Module:

This system is to creates a successful model in order to reduce the workload of hospital staff by avoiding lot of paper work and also avoids attacks to make the data secure and also avoid time wastage of patient ,while the patient goes from one hospital to another for treatment.

IV.ARCHITECTURE



Hence the system uses RC6 algorithm to provide security.

V.DATA ENCRYPTION AND DECRYPTION

Encryption is the process of translating plain text data (plaintext) into something that appears to be un-understandable and meaningless (ciphertext). Decryption is the process of converting ciphertext to plaintext.

To encrypt more than small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.

The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used there is no technique which is better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.

It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in the use for several years and has successfully resisted all attacks.

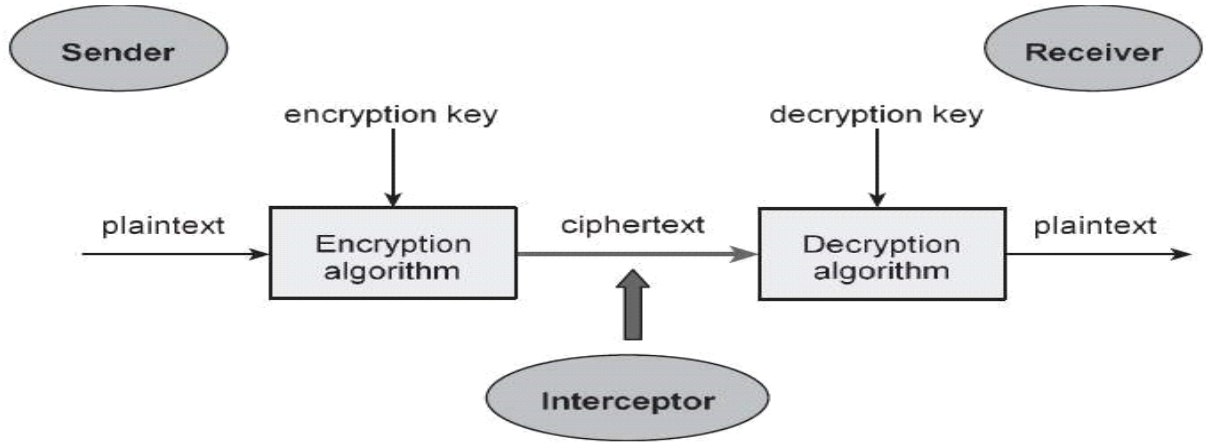


Fig. Encryption-Decryption process.

VI.TYPES OF ENCRYPTION

1)symmetric cryptography

There are two main ways to do encryption today. The first kind of encryption, called symmetric cryptography or shared secret encryption, has been used. This form of encryption uses a secret key, called the shared secret, to scramble the data into unintelligible gibberish. The person on the other end needs the shared secret (key) to unlock the data, the encryption algorithm. You can change the key and change the results of the encryption. It is called symmetric cryptography because the same key is used on both ends for both encryption and decryption.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.05, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

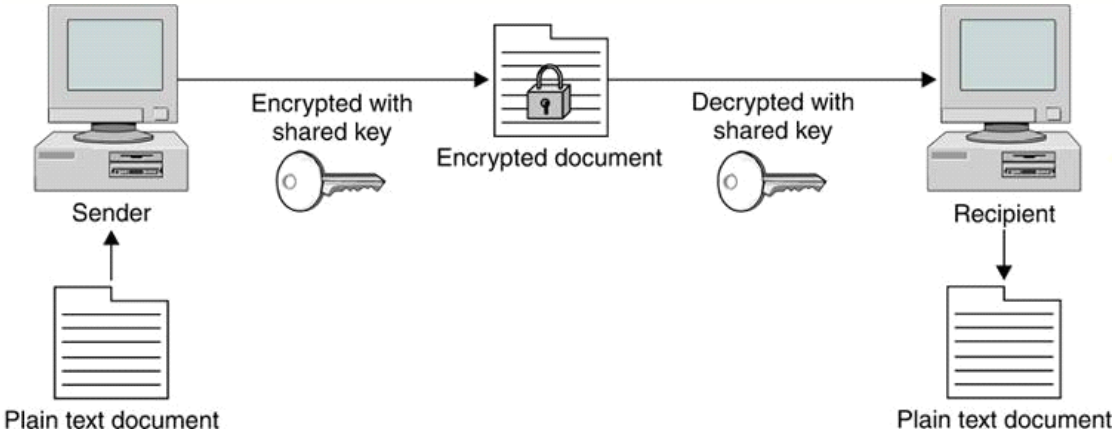


Fig. Symmetric Cryptography

The problem with this method is that you have to communicate the secret key securely to your recipient. If your enemy hack the key, he can read the message. All kinds of systems were invented to try to get around this basic weakness, but the fact remained: you still had to communicate the secret key in some way to your recipient before you could commence secure communications.

2)Asymmetric cryptography

Asymmetric cryptography uses encryption that splits the key into two smaller keys. One of the keys is made public and one is private. You can encrypt a message with the recipient's public key. The recipient can then decrypt it with their private key. And they can do the same for you, encrypting a message with your public key so you can decrypt it with your private key . The difference here is that you don't need someone's private key to send him a secure message. You use his public key, which doesn't have to be kept secure. By using your recipient's public key, you know that only that person can encrypt it using his or her private key. This system allows two entities to communicate securely without any prior exchange of keys.

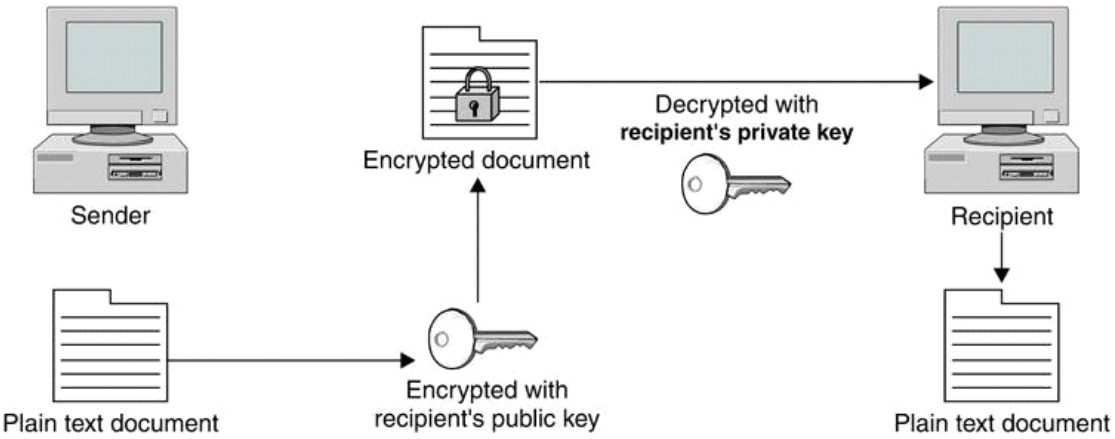


fig. Asymmetric cryptography

Asymmetric cryptography is usually implemented by the use of one-way functions. In mathematic terms, these are functions that are easy to compute in one direction but very difficult to compute in reverse. This is what allows you to publish your public key, which is derived from your private key. A common one-way function used today is factoring large prime numbers. It is easy to multiply two prime numbers together and get a product. However, to determine which of the many possibilities are the two factors of the product is one of the great mathematical problems. If anyone were to invent a method for easily deducing factors of large prime numbers, it could make obsolete much of the public key encryption used today. Fortunately, other one-way functions work for this application, such as calculations on elliptical curves or computation of inverse logarithms over a finite field.

RC6 specifications:

RC 6 (Rivest Cipher 6) is a symmetric key block cipher derived from RC 5.It was designed by Ron Rivest, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advance Encryption Standard (AES) competition

Algorithm:

RC6Algorithm

• RC6 is a symmetric key block cipher derived from RC5.

• Block size of 128 bits. Flexibility of key size.

• No key separation. Operators involved are simple in function favorably.

• High speed with minimal code memory.

• Provides a solid well-tuned margin for security against well-known differential & linear attacks.

• Max potential for parallelism when multiple streams are processed.

RC6 algorithm basic operations:

• a + b: integer addition modulo 2w.

• a - b: integer subtraction modulo 2w.

• A ˆb: bitwise exclusive-or of w-bit words.

• An x b: integer multiplication modulo 2w.

• a ¡¡¡ b: rotate the w-bit word a to the left by the amount given by the least significant law bits of b.

• a ¿¿¿ b: rotate the w-bit word a to the right by the amount given by the least significant law bits of b.

VII.MATHEMATICAL MODEL

System Description: Let S be a system that describes System

• S= Hospital Management System.

• Identify input as S={I,...}, Let I=i input will be reports of patients.

• Identify output as O S ={I,O,}O= patient history display

• Identify the processes as P S={I,O,P,..} P={E,D} E={parameter, Patient ID} D={parameter, Patient Report}

• Identify failure cases as F S={I,O,P,F,.} F=Failure occurs when the internet not available.

• Identify success as s. S={I,O,P,F,s,}s=Patient details display successfully

• Identify the initial condition as Ic S={I,O,P,F,s, Ic,} Ic=GPS tracking.

VIII.COMPARISON

Algorithms	Key size	Block size	Round	Structure	Flexible	Features
DES	64 bits	64 bits	16	Feistel	No	Not structure, Enough
3DES	112 or 118 bits	64 bits	48	Feistel	Yes	Adequate security
AES	128,192,256 bits	128 bits	10,12,14	Substitution, Permutation	Yes	Replacement for DES, Excellent security
RC4	Variable	40-2048 bits	256	Feistel	Yes	Fast cipher in SSL
RC6	128-256 bits	128 bits	20	Feistel	Yes	Excellent Security
BLOW FISH	32-448 bits	64 bits	16	Feistel	Yes	Good Security

IX.CONCLUSION

Existing system contains lot of paper work because of manual entries also there are chances of attacks on the patients data at the time of data transfer.

Proposed system provides the facility to store large amount of data securely.This would enable to improve the response time to the demands of patient care because it automates the process of collecting, collating and retrieving patient information. It reduced the manpower. This System provides security against DDos attack by using RC6 algorithm with encryption and decryption technique.

Future scope:

In future we can connect various labs and multiple hospitals in the network.

REFERENCE PAPER

[1] SmartHospitalManagementSystem: AnIntegrationofEnterpriseLevelSolutions Utilising Open Group architecture Framework (TOGAF). 2007

[2] Design and Implementation of Hospital Management System. 2008

[3] DesignandImplementationofHospitalManagementSystemUsingJava.2015

[4] An E Hospital Management and Hospital Information Systems Changing Trends. 2013

[5] Designing A Web Based Hospital Management System For MOUAU Clinic. 2015