International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Globalized Medi-Care and Organ Transplantation System

Aparna Reji[1], Athira S[2], R. Suji Pramila[3]

[1,2] *Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil, Tamilnadu, India.*

[3]*Assistant Professor, Department of Computer Science and Engineering, Noorul Islam University, Tamilnadu, India.*

[1]*aparnarl721@gmail.com,* [2]*meenunair74@gmail.com,* [3]*sujisymon@gmail.com*

Abstract- *Globalized Medi-Care and Organ Transplantation System is a new system for managing the patients globally. It is a portal and through this multi special hospitals can enter the availability of organs to transplant, they can instantly inform all the hospitals which are registered in this portal. The hospitals can also enter the patient details. Each patient details contain a Global Identification Number(GIN) so that if a patient is admitted in a hospital by seriously injured, using his GIN doctors can find his previous case history like any allergy , heart patient or not, previous surgery details if any etc. So treatment will be easy and faster. It also aims in promoting blood donation. Those who are willing to donate their blood can register with this site so that it satisfies the urgent need of many ones. In order to protect the misuse of this portal from hackers, the Rijndael security algorithm is implemented.*

Keywords- Portal, Global identification number, Rijndael security algorithm, Organ transplantation, Blood donation.

1. INTRODUCTION

Aiming at promoting and the process of organ donation, the government amended the Transplantation of Human Organs Act, in order to simplify rules and extend the ambit of donors to grandparents and grandchildren. The Bill, which may be called Transplantation of Human Organs and Tissues Act (THOTA), proposes to allow swap donation, tissue donation and expands the definition of near relatives. Now a day's organ transplantation has become an important issue.

Globalized medi care and organ transplantation system is a portal which helps in thetreatment of patients globally. There are many people in the world that may need special treatments in emergency situation. But it might be difficult for them to find the apt doctor at the apt time. In this case, this portal helps in providing the details of efficient doctors including the hospitals in which they are working.

Now a days a major problem our society facing is the unavailability of organs to transplant. There are many persons who are willing to transplant their organ but those who are in need of the organ might not know them. This portal prevents the problem by making the hospital registered with this site to enter the availability of organ in their hospital so that those persons who are in emergency need can contact with them.

Another issue our society face is the unavailability of blood in emergency situation. There are many people who are dying day by day without getting blood of correct blood group in the emergency situations such as in accidents. In this situation they can seek the help of this website as this portal contains the information's of people who are willing to donate their blood with their details and contact number.

Another feature is the global identification number (GIN). The GIN helps to enter each patient's details to the website. There are many situations occur where the patients' medical history should be referred. Any doctor can use the GIN and find that persons medical history.

The Rijndael algorithm with a modification is implemented to increase the security of the website. Sometimes a problem which may occur with this site is that any hacker can enter to the site and can do some malfunctions like changing the availability of one organ to other. But the hospital may not be having that particular organ available. This may even cause to the loss of lives. In order to escape from the security issue the Rijndael algorithm is implemented. To be more secured a modification is also made in Rijndael algorithm. Actually in a Rijndael algorithm, the bits of the key are numbered from 1 through 64 where every eighth bit is ignored and is subjected to a permutation.

The resulting 56-bit key is then treated as two 28–bit quantities, labeled C_0 and D_0 .At each round C_{i-1} and D_{i-1} are separately subjected to left shift or rotation of 1 or 2 bit. These shifted values serve as input to the next round. They also serve as input to permuted choice 2 which produces a 48-bit output that serves as input to the function $F(R_{i-1}, K_i)$. Now a modification is made on the key size to make the

Rijndael algorithm more secured. The actual key size will be increased from 56 to 64 by adding an extra bit after every eighth bit. After including bits for permutation the outcomewill be a total of 72 bit key. At the time of decryption, we need to fetch and skip these extra added bits from the cipher text.

2. LITERATURE SURVEY

A study about the Rijndael algorithm is made in [1]. It is a new Advanced Encryption Standard (AES) which is approved by the US National Institute of Standards and Technology (NIST). This algorithm supports significantly larger key sizes as compared with DES (Data Encryption Standard). NIST believes that the AES has a potential to remain secure for the next few decades. In overall performance, based on the amount of speed for encrypting and decrypting on key set-up time, the Rijndael algorithm attains top scores in the test conducted by NIST. The belief is that almost all of the US government agencies will be shifting to the AES algorithm for their data security needs in the next few years. Also, that the algorithm is possible to find its way in smartcards and other security oriented applications which is used for safely storing individual's private information.

A modified version of A5/3 based on Rijndael was made on [2]. In communication a system, encryption is used to protect the information that is transmitted over a channel. A5 is the encryption algorithm which is usually used to ensure the protection of conversations on Global System for Mobile Communications (GSM) mobile phones. There are two versions of the stream cipher available now. The strongest version is the A5 /1 which is used in most of the countries. On the other hand the weaker version A5/2 is used in such countries where export restrictions apply. By the third quarter of 2002, European Telecommunications Standards Institute (ETSI) has published GSM new security algorithms. The new security algorithms are known as A5/3. A5/3 is completely based on the kasumy algorithm, specified by 3rd Generation Partnership Project (3GPP) for the usage in 3G mobile systems. During this same period, there was a discussion going on about the Rijndael algorithm in the cryptographic community for its use in the field of mobile security. Thus a higher level of security will be provided than A5/1 and original version of A5/3.

The smartcards which makes possible the content encryption for the mobile devices in order to achieve a secure communication is proposed on [3]. In this era, the usage of mobile devices such as personal digital assistance, smart phones etc are used instead of traditional computers as wireless (mobile) communication and computing became popular. Many services and protocols are developed to secure the wireless communication. These protocols include Secure Sockets Layer (SSL)/Transport Layer Security (TLs), Internet Protocol Security (IPSec) etc. It is difficult to generate heavy computations such as the process of generating Rivest-Shamir-Adleman (RSA) keys (large prime numbers) on mobile devices. It is due to the fact the mobile device possesses limited resources. This can be simplified by using the help of smartcards. To secure the communication between the mobile devices the well-known Rijndael cryptographic algorithm is used.

The design of Rijndael algorithm based on"NIOSll + FPGA (Field Programmable Gate Array) " was proposed on [4] which is able to achieve a high data processing speed as it occupies comparatively low resources. The advanced encryption standard (AES) algorithm is optimized through the look-up table based on the analysis of round transformation and the expansion. After that, the optimized Rijndael algorithm based on SOPC (system on a programmable chip) was designed and was implemented through software and hardware. Based on this software design flowchart of the optimized Rijndael algorithm, the program design of the key generated and corresponding B table is completed. These give the test results such that the highest working frequency is 147MHz and the biggest data flow is 2832Mbps. Hence the design of Rijndael algorithm based on "NIOS ll + FPGA" has a big breakthrough when it is compared with the traditional FPGA realization.

The structure and the design of new Advanced Encryption Standard (AES) were analyzed on [5]. The National Institute of Standards and Technology (NIST) choose to adopt the Rijndael algorithm as AES by the U.S Department of commerce. It replaced the Data Encryption Standard (DES). The new structure and design of AES was analyzed based on the three criteria: a) The amount of resistance against all of the known attacks; b) the amount of speed and the code compactness on a wide range of platforms; and c) the simplicity of design. They also evaluated the similarities and dissimilarities with other symmetric ciphers. Other investigations done on it was the measurement of advantages of the new AES with respect to DES and T-DES (Triple-Data Encryption Standard). These made the implementation aspect of Rijndael and its inverse possible. Hence, even though Rijndael was well suited to be implemented efficiently on a wide range of processor and on dedicated hardware, they concentrated their study on 8-bit processor which is used in current smart cards and on 32-bit processor which is used in PCs.

A reconfigurable architecture of the existing Advanced Encryption Standard (AES-Rijndael) cryptosystem was

proposed in [6]. This one is capable to handle all of the possible combinations of standard bit lengths (128,192,256) of data and key. Lesser hardware complexity is ensured by the fully rolled inner-pipelined architecture. This work developed an FSMD (Finite State Machine with Data path) model based controller. This controller is the one which is ideal for many iterative implementations of AES. Here S-boxes are also implemented. The S-Boxes are implemented using the combinational logic over composite filed arithmetic. This composite field arithmetic has a feature to completely eliminate the need of any internal memory. This design was implemented on XilinixVirtex XCV1000 and 0.18 mum CMOS (Complementary-Metal-Oxide-semiconductor) technology.

An FPGA Rijndael encryption design was proposed in [7]. This design utilized the look-up tables to implement the entire Rijndael Round function. A comparison was made between the new design and similar existing implementations. The result of the comparison was that, hardware implementations of encryption algorithm were found to be much faster than equivalent software implementations. Due to their flexibility and the architecture, programmable gate arrays (FPGAs) are well suited for encryption implementations in particular fields. The specialty of the architecture is that, it can be exploited to accommodate typical transformations of encryption. The look-up table based Rijndael design has a speed of 12 Gbits/sec, which is 1.2 times faster than an alternative design in which the look-up tables are utilized to implement only one of the Round function transformations. It is also 6 times faster than all of the other previous implementations.

The system level issues encountered in a high performance implementation of a Rijndael encryption core on a memory – slot based reconfigurable computing platform is discussed in [8]. This platform is called Pilchard. US National Institute of Standards and Technology (NIST) adopted Rijndael algorithm in 2000 as the Advanced Encryption Standard (AES). The implementation of Rijndael was done on such a manner that, the number of unrolled rounds in the encryption core was changed as it can affect the performance of the system. For the proposed design, a higher performance of 755 Mbit/sec was achieved by implementing a core with a single round. The process of implementing a high performance core on an FGPA is easy, even though due to I/O (Input / Output) bottlenecks, achievement of high system level performance was difficult. Hence all these feature enabled the measured throughput of the AES core to reach 445 Mbit/sec which, although slower than the AES core, was double that of an optimized interface.

The security issues connected with the existing ATMs and other electronic fund transfer mechanism was studied in [9]. The fact is that, hackers commit uninterrupted crimes, they had given importance to use Rijndael algorithm in order to obtain matured cryptographic techniques which could combat such unethical attempts. The existing researches made to implement Rijndael hardware was based on conventional CMOS technology. They made a novel approach to improvise the Rijndael using one highly advanced technology called Single Electron Transistor (SET) Technology. They made a comparative study to reveal the merits of SET based Rijndael model. The detailed study revealed that SET based Rijndael circuit possess less propagation delay of about 6ns/gate which was nearly half of CMOS based design. Similarly the power gate using SET was reduced to 10 to 12 times lower than existing CNOS (Change Number of Sessions) architectures. The fastness was doubled for SET made circuits. There is also another feature that the composite structure of SET has an immense size reduction possibility which increases its integrity. In modern era, the electronic fund transfer mechanism to ATM is anticipated to relay on such SET based Rijndael models. Hence they came to a conclusion that SET technology stands much ahead when compared to conventional electronics.

The EM attacks were analyzed in [10]. They demonstrated a real EM-based attack on a PDA (Personal Digital Assistant) which runs Rijndael and elliptic curve cryptography. A new frequency based differential EM analysis which is able to compute the spectrogram was presented. In addition a low energy counter measure for symmetric key cryptography was also presented which is able to avoid large overheads of the regeneration of table or excessive storage. The new differential analysis was not in need of perfect alignment of EM traces. Thus its supports attack on real embedded systems. It is important for future wireless embedded system which will be having a higher demand for levels of security.

3. PROPOSED ARCHITECTURE

The proposed architecture is the design of Globalized medi care and organ transplantation system portal. The design shows how the portal is designed. The portal consists of four options which are admin, health department, hospital and blood donation.

The admin module is used by the admin. To enter into the admins profile first the user has to login. After login the page redirects to that admin page. Inside he admin page there are several options they are, Add global medi centre, Add organ

transplantation, View organ transplantation, View global medi centres and View feedbacks. Each of these sub options have their own functions.

After the admin, next option is the module of hospitals. For each hospital there will be an admin to manage the portal .Each admin will be provided with a user name and password in order to login to the portal. The admin is allowed to provide true and correct information's to the website. Inside the hospital option there are several sub options which are, Doctor Registration to allow the doctor to register. Patient registration which allows the registration of the patient, Donor registration which makes the donor to register and to make others know about their willingness to donate, Recipient registration which allows the recipient to register and seek the help of donors, Search patient which allows to search whether any patients who are registered with this site are in emergency need for organ in order to survive their lives, View doctors which allows to display the list of efficient doctors present on a particular hospital, Change password which helps the hospital administrator to change the password in order to provide efficient security to the website.

The next module is the health department module which is managed by the administrator of health department. Inside the health department module there are many sub options, they are, Approve hospital which are used for approving the hospital to use the portal, View hospital which are used to know the list of hospitals requested to use this portal, Send feedback which is used to send feedback to the hospitals if any, Change password which is used to change the password by the administrator of health department.

The next options is for blood donation where log in is not required. Any persons who are ready to donate their blood can register to the site. They have to provide some of their personal details during registration. In blood donation the two sub modules are donor search and blood donor registration. The search donor helps to know if there is any emergency

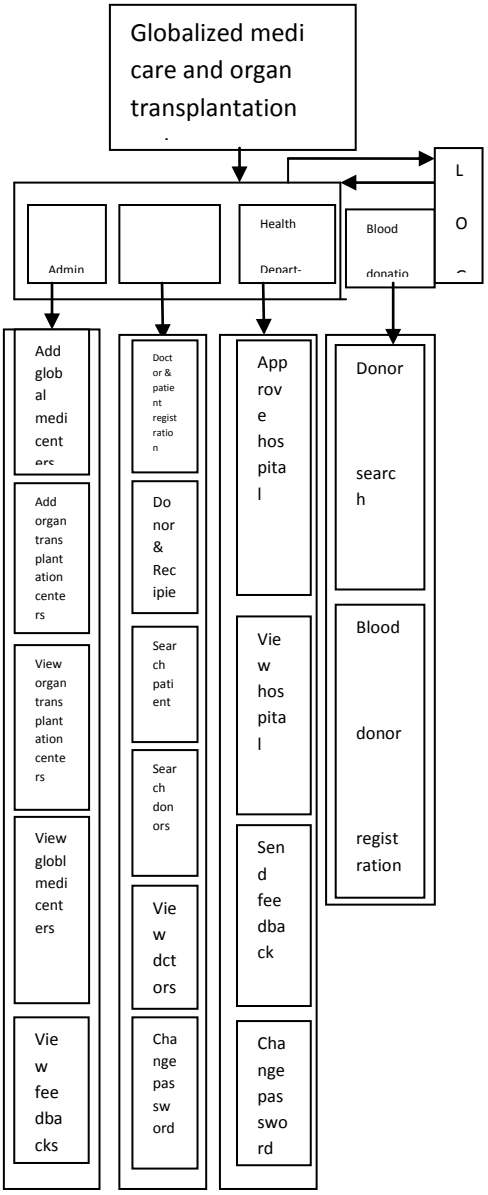

Fig-1: System Design

The proposed design consist of different modules for its implementations. The different modules required for the implementation of the portal are:-

3.1 Database design

The data design transforms the information domain model created during analysis into the data structures that will be required to implement the software.

The data objects and relationships defined in the entity relationship diagram and the detailed data content depicted in the data dictionary provide the basis for the data design activity.

The overall objective in the development of database technology has been to treat data as an organizational resource and as an integrated whole. Database Management System allows data to be protected and organized separately from other resources. Database is an integrated collection of data. This is the difference between logical and physical data. Databases are implemented using a DBMS package. Each particular DBMS has unique characteristics and general techniques for database design. There are 6 major steps in design process. The first five steps are usually done on paper and finally the design is implemented.

- Identify the table and relationships
- Identify the data that is needed for each table and relationship
- Resolve the relationship
- Verify the design
- Implement the design.

The proposed system 'Globalized Medicare and Organ Transplantation System' stores the information relevant for processing in the Microsoft SQL Server Management Studio Express (Microsoft SQL Server2008). The database uses tables for storage. A table also contains records, which is a set of fields. All records, in a table have the same set of fields with different information. Uses 10 tables.

The design of the database measures the efficiency of the system. The background used in this application is Microsoft SQL Server2008, which provides databases and tables for storage and queries for retrieving data from the database.

3.2 System Architecture Design

The most powerful C#.Net is used to design system architecture of the proposed project. System architecture is designed with a concept of 3 tier architecture.

A three-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms. Three-tier architecture is a software design pattern and well-established software architecture. Three-tier architecture allows any one of the three tiers to be upgraded or replaced independently. The user interface is implemented on a desktop PC and uses a standard graphical user interface with different modules running on the application server. The relational database management system on the database server contains the computer data storage logic. The middle tiers are usually multitiered.

The three tiers in three-tier architecture are:

1. Presentation Tier: Occupies the top level and displays information related to services available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.

2.Application Tier: Also called the middle tier, logic tier, business logic or logic tier, this tier is pulled from the presentation tier. It controls application functionality by performing detailed processing.

3.Data Tier: Houses database servers where information is stored and retrieved. Data in this tier is kept independent of application servers or business logic.

3.3 Security Architecture Design

Rijndael algorithm is used for the advanced encryption standard (AES). The two researchers who developed and submitted Rijndael for the AES are both cryptographers from Belgium: Dr Joan Daemon and Dr Vincent Rijmen. Rijndael was designed to have the following characteristics.

- Speed and code compactness on a wide range of platforms
- Design simplicity
- Rijndael is very well suited for the restricted-space environments. It has very low RAM and ROM requirements.
- Rijndael performs encryption and decryption very well across a variety of platforms, including 8 bit and 64 bit platforms.

The bits of the key are numbered from 1 through 64; every eighth bit is ignored and is subjected to a permutation. The resulting 56-bit key is then treated as two 28–bit quantities, labeled C_0 and D_0 .At each round C_{i-1} and D_{i-1} are separately subjected to left shift or rotation of 1 or 2 bit. These shifted values serve as input to the next round. They also serve as input to permuted choice 2 which produces a 48-bit output that serves as input to the function $F(R_{i-1}, K_i)$.

Incrementing key size is a good idea to improve the security of Rijdael algorithm. Adding an extra bit after every eighth bit, will resulting actual key size from 56 to 64. After including bits for permutation will outcome total 72 bit key size. At the time of decryption, we need to fetch and skip these extra added bits from the cipher text. Implementing this modification inside the existing algorithm is not a simple and easiest task. And it is a little bit tricky and logically more complex.

3.4 Website Design

The proposed website is designed with the latest web technology named as Active Server Pages (ASP) and HTML5 as a User interface Design Language. Website design is mainly divided in to two they are input design and output design. The input is the set of values that is provided by the user to the system. The input design must enable the user to provide the error free input to the system for efficient processing.

The input design is the process of converting the user-oriented inputs into computer based formats. The data's fed into the system using simple interactive forms. The forms have been supplied with messages so that user can enter data without facing any difficulty. The data is validated wherever it requires in the project. This ensures that only the correct data have been incorporated into the system. The input data have to be validated, edited, organized, and accepted by the system before being proposed to produce the outputs.

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any systems results of processing are communicated to the user and to the other systems through outputs. In the output design it is determined how the information is to be displayed for immediate need. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship with the user and helps in decision making. The objective of the output design is to convey the information of all the past activities, current status and to emphasize important events.

The output generally refers to the results and information that is generated from the system. Outputs from computers are required primarily to communicate the results of processing to the users. The result for each query option that is submitted by the user, the system displays the output. The output that is obtained for each query submitted should be tested before confirming the result.

4. RESULT AND ANALYSIS

A comparison between the existing Rijndael algorithm and the modified Rijndael algorithm was made. In the existing one the security provided is less as provided with the extended version. The time consumed by both while running is compared and analyzed that the existing one used less time as compared with the new one. The key length of the existing one is less as compared with the key length of the new one. As a result the security is greater for the new modified Rijndael algorithm. The comparison chart is given in Fig. 2.

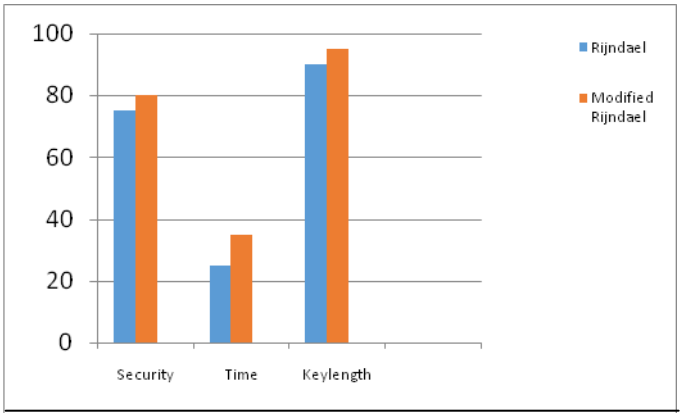

Chart -1: Comparison chart

5. CONCLUSION

The Globalized medi-care and organ transplantation system is an efficient portal which helps to treat patients globally. The security issue which may arise in the portal is solved by implementing the modified version of Rijndael algorithm. Thus the efficiency of the portal is increased.

REFERENCES

[1] Jamil T, "The Rijndael Agorithm,Potentials,2004," pp .36-38

[2] Soyjaudah,K.M.S, "A, Design and Implementation of Rijndael Algorithm for GSM Encryption," Mobile Future, 2004, pp. 106-109

[3] Bin Nafey, F, "A Study on Rijndeal Algorithm for Providing Confidentiality to Mobile Devices," TENCON 2008, 2008, pp.1-6

[4] Shunwen xiao, "The Optimized Design of Rijndael Algorithm Based on SOPC, Information and Multimedia Technology," 2009, pp. 384-387

[5] Sanchez-Avila, C and Sanchez-Reillo, R, "The Rijndael Block Cipher (AES proposal): A Comparison with DES," Security Technology, 2001 ,pp. 229-234

[6] Alam, " An Area Optimized Reconfigurable Encryptor for AES-Rijndael," Design, Automation & Test in Europe Conference & Exhibition, 2007, pp. 1-6

[7] McLoone,M and McCanny, J.V, "Rijndael FPGA Implementation Utilizing Look-up Tables," Signal Processing Systems, 2001, pp. 349-360

[8] Tong, D.K.Y, "A System Level Implementation of Rijndael on a Memory-Slot based FPGA card," Field-Programmable Technology, 2002, pp. 102-109

[9] Jayanta Gope and Prakash Kumar Shah, "Advanced and Secured Rijndael Hardware Realization Using Single Electron Transistor Technogy," International Journal of Emerging Research in Management & Technology, 2014, vol.3, pp .182-18

[10] Catherine H, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," CHES, 2005, pp. 250-264