Pocket Certificate for Government Portal using combined Cryptography

Shamal Chavan, Priti Gaikwad, Prathamesh Koyande
Guided by Prof. Martina Rodgrigues

Abstract— The Pocket Certificates System is software, which tries to alter the originality of the Government Related Documents such as Aadhaar Card, PAN Card, etc. into encrypted form. We are making use of Combined Cryptography Techniques (Ex. AES, DES, RSA) in order to provide a Security to our software. The major task of Pocket Certificates is to provide the user the flexibility of passing the information implementing the encryption standards as per the specification and Algorithms proposed and store the information in an encrypted form that is unreadable and also availability of documents on their private accounts. Whenever user want to download file the system will decrypt the document which is store on server. The Entire application will have a user friendly Graphical User Interface, which will be in a self-learning mode for the end user. The System will provide all the functional standards of proper navigation.

Index Terms — Cryptography, Encryption, Decryption, AES, 3DES.

1 INTRODUCTION

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered.

This paper is about a System that helps citizen to get their original document whenever they want. Citizen shouldn't carry their original document all the time. Citizen only needs to login into that system and download the desired document. This system provides high level of security to those documents. This system mainly implements for security purpose. In this system the documents of citizen are encrypted using combined cryptography as AES and 3DES technologies. When user or citizen want to download the document the server decrypt the document.

2 PROBLEM STATEMENT

Each time we make an application for job or admission for any course or any other purpose to the university or company, we have to submit all the documents of all the previously appeared exams as well as the identity proofs. Also the documents have to be attached with the form along with true copy done. All this requires lot of verification and also the form becomes complicated with so many documents attached. Sometimes the staff due to his negligence can make error in verification and can lead to errors.

Also there is a huge loss if these documents get misplaced. Thus to avoid such situations we have come up with this project idea wherein all the documents will be created and issued as soft copy to the citizens. This will reduce the paper-work and workload of the verification team as all the documents will be available at a single place and that too secured.

DigiLocker, national Digital Locker System launched by Govt. of India which provides 1GB of free space in the locker to securely store resident documents, is somewhat similar to our idea of project. But it has certain drawbacks like, citizen cannot login unless he has Aadhar card. Other issue is that DigiLocker does not allow storing all the documents; it has options only for certain type of documents.Also citizens themselves upload the documents which may or may not be genuine.But our project not only allows storing the documents online, but also we guarantee their authenticity and security.

3 Relevance of the Project

- The "Pocket Certificate for Government Portal using Combined Cryptography" will make a complete information detail about each individual citizen.
- Once a citizen is born, a request from the respective hospital is made to government for Birth Certificate. Thus every citizen's account is created.
- Every citizen will be provided with a card(we can use Aadhar Card to avoid creation of more documents) which will contain UID(Unique Identity) number and further more all the documents will be uploaded in this account.
- It will contain all the examination results from his S.S.C. till date, which will include all government given examinations results as well as government given identity proofs.
- These results will be in the form of "E-Certificates" and the format will be very compressed one which won't

require more storage space, also they will be encrypted using various security algorithms.

- The existing citizen can apply for the same and get their respective card, long with other identity proofs.
- The admin will get a list wise view of all the citizens with their UIN (Unique Identification Number), which is unique for all the citizen and he can view it also state wise and also city wise.
- At government side, once they get a request from hospital authority for creation of account, government verifies the newborn citizen and creates an account for it. Further it issues birth certificate.
- As time passes by, and more documents are needed, citizens can apply for new documents like domicile certificate, passport, PAN card, etc.
- Upon successful creation and uploading of documents citizens will be sent an e-mail and an SMS notifying about the document upload.
- Citizens can view their documents, download them and share them(via email) with other people/companies/institutions.
- These documents will be encrypted with algorithms like AES and DES from government/server side. And they can be decrypted only by Citizen's Private Key.
- This will prevent unauthorized access to documents, maintaining their security.

4 SCOPE

Load Balancing:
Since the system will be available only the admin logs in the amount of load on server will be limited to time period of admin access.

Easy Accessibility:
Records can be easily accessed and store and other information respectively.

User Friendly:
The system will be giving a very user friendly approach for all user.

Efficient and reliable:
Maintaining the all secured and database on the server which will be accessible according the user requirement without any maintenance cost will be a very efficient as compared to storing all the citizen data on the spreadsheet or in physically in the record books.

Easy maintenance:
Pocket Certificate Data Card System is design as easy way. So maintenance is also easy.

5 ALGORITHMS USED

1. AES:

Advanced Encryption Standard (AES)
Steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

The order of operation in decryption is:

1. Perform initial decryption round:
   XorRoundKey
   InvShiftRows
   InvSubBytes
2. Perform nine full decryption rounds:
   XorRoundKey
   InvMixColumns
   InvShiftRows
   InvSubBytes
3. Perform final XorRoundKey

2. 3DES:

This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.

Algorithm:

```
For j = 1 to 3
{
Cj,0= IVj
For i = 1 to nj
{
Cji = EKEY3(DKEY2 (EKEY1 (Pj, iCj, i-1)))
Output Cj, i
}
}
```

6 System Design

6.1 System Block Diagram

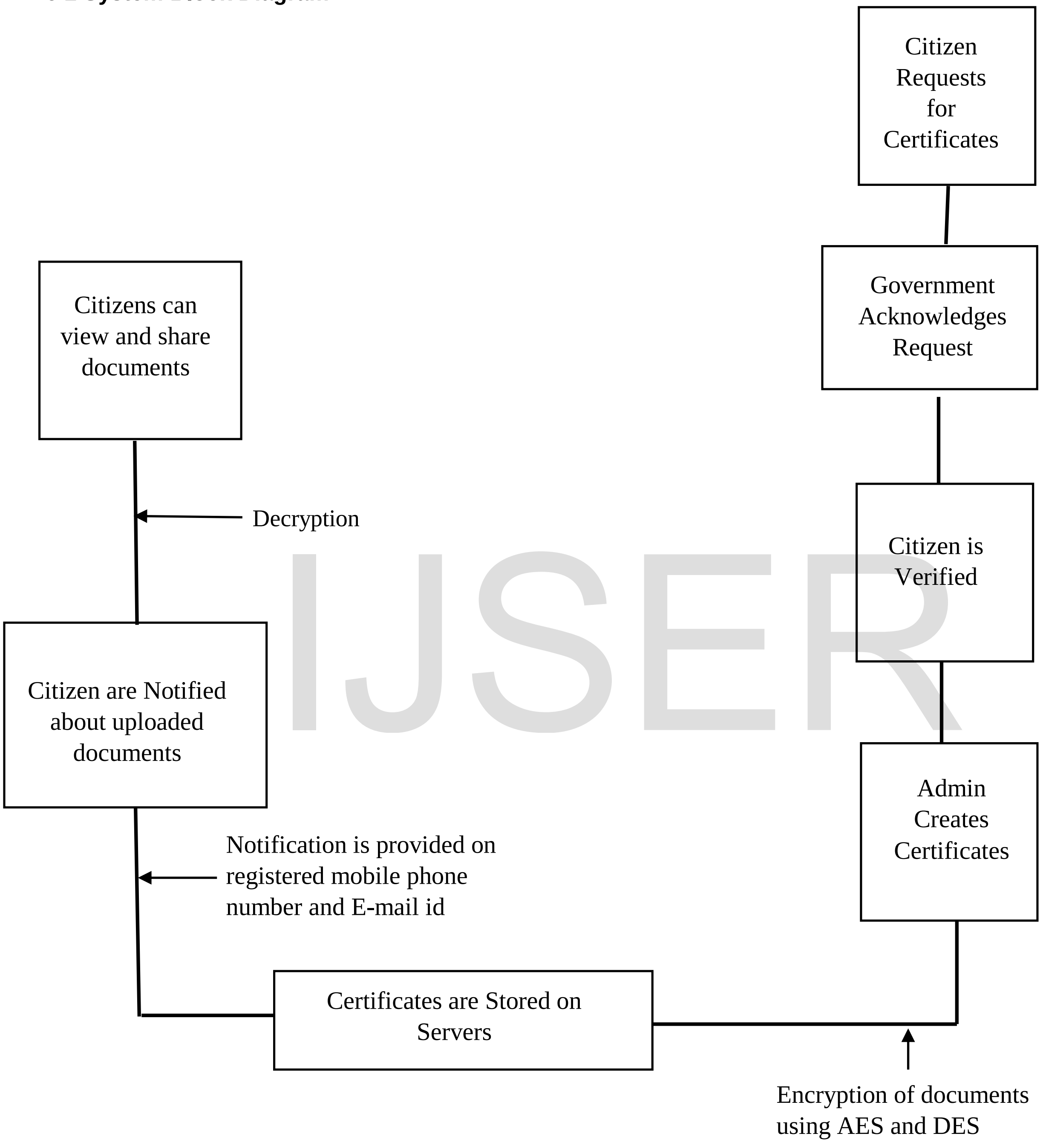
Citizen Requests for Certificates
Government Acknowledges Request
Citizen is Verified
Admin Creates Certificates
Encryption of documents using AES and DES
Certificates are Stored on Servers
Notification is provided on registered mobile phone number and E-mail id
Citizen are Notified about uploaded documents
Decryption
Citizens can view and share documents

Fig. 6.1: System Block Diagram

This is a diagram of a system in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks.

6.2 Use case Diagram

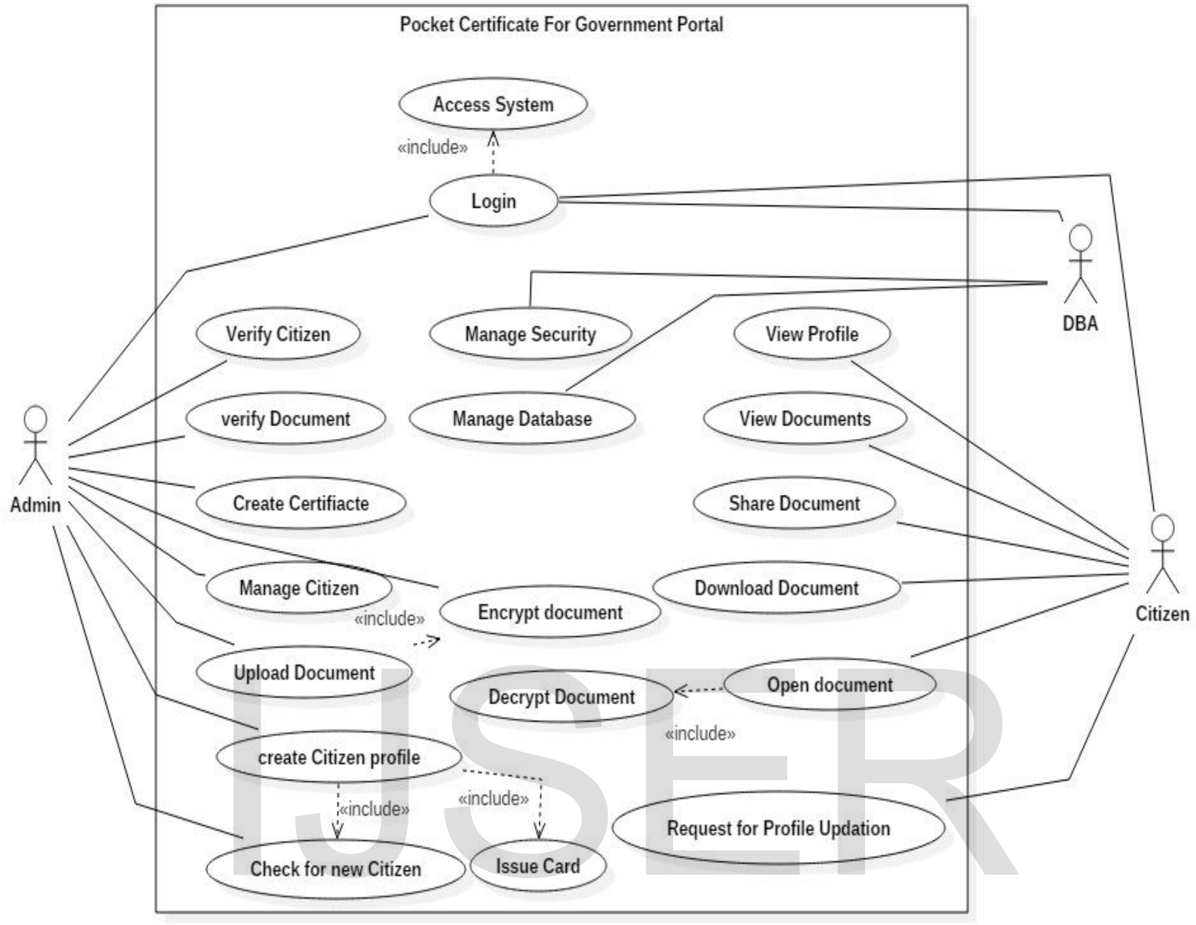

Fig. 6.2: Use Case Diagram

This use case diagram is a graphic depiction of the interactions among the users and the application of the system. The boundary defines the scope of the system.

6.3 System Requirements

6.3.1. Hardware:

Processor	: Intel Processor i3 and above
RAM	: 4 GB
Hard disk	: 40 GB
Monitor	: Any Monitor having resolution of 1024*768

6.3.2. Software:

- Microsoft Visual Studio

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.

- Microsoft SQL Server

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet).

Microsoft markets at least a dozen different editions of Microsoft SQL Server, aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users.

6.4 Modules

6.4.1. Home Page:

Home page basically gives a brief idea about the system and it uses. It has an Introduction part and the aim of the system. The portal has basically four tabs : Home, Login, Contact Us and Credits.

6.4.2. Login Page:

Login page provides login facilities for admin and citizen. Citizen can use their smart/aadhar card number as their username and mobile number as their password.

Admin gets a pre-defined username and password to log-in to the system and perform his desired functions. Citizen can click on citizen login to access his/her account

6.4.3. Citizen login page:

When you click on Citizen Login option from Login page, you are redirected to Citizen Login page. Here, one needs to type incorrect Login ID and Password.

Login ID in this case will be smart card/ aadhar card number and password can be mobile number or self-generated password by each citizen.

6.4.4. Contact Us page:

This is Contact Us page which will provide all the information regarding the help for citizens. Various social media links, email address and contact number for seeking any kind of help, suggestion, grievances are provided. Citizen can use this information for any kind of difficulty.

7 Conclusion

The Project gives us a solution of carrying our Sensitive Documents freely without the harm of being tampered. Also we can produce these documents securely at any government related for organizations as a part of proof of our identity. The main feature of our system is that it makes use of Combined Cryptography which makes it almost impossible for the hackers to break into the system. In future we try to secure the login details of the Citizens by using Biometrics Encryption Techniques.

References

1. Harshal Pandit, Shailendra Nipane,Suraj Jadhav, Sunita Naik "Secured E-Documents and Sharing using Encrypted QR-Code ", International Journal of Computer Applications (0975 – 8887), The National Conference on Role of Engineers in National Building.

2. Shiv Shakti, "ENCRYPTION USING DIFFERENT TECHNIQUES", International Journal in Multidisciplinary and Academic Research, ISSN: 2278-5973, 1 Jan-Feb 2013, vol. 2, Issue no. 1.

3. AbhinandanAggrawal, Gagandeep Singh, Prof. (Dr.) Neelam Sharma, "Implementation of AES algorithm", International Journal ,Of Engineering Research & Science (IJOER), ISSN: 2395-6992, 4 April 2016, vol. 2, Issue no. 4.

4. Shraddha Kalbhor, Anita Gaikwad, Kajal Bhise, Prof. Dipmala Salunke, Varsha Bangar, "A Survey on Digital Signature", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, January 2015 , vol. 5, Issue no.1.

5. Binal Shah, Zahir Aalam, "Implementation and Performance Evaluation of the AES Algorithm for Data Transmission using Various Programming Languages", Foundation of Computer Science FCS, New York, USA, ISSN: 2394-4714, November 2015, vol. 3, Issue no.4.

6. Nimmi Gupta, "Implementation of Optimized DES Encryption Algorithm upto 4 Round on Spartan 3", International Journal of Computer Technology and Electronics Engineering (IJCTEE), ISSN 2249-6343, 19 Jan 2012, vol. 2, Issue no.1.

7. Shabnam Kumari, Reema, Princy and Sunita Kumari, "Security in Cloud Computing using AES and DES", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, IJRITCC April 2007, vol. 5, Issue no.4.

8. Ms. E. Kalaikavitha, Mrs. Juliana gnanaselvi, "Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology", International Journal Of Engineering And Science, April 2013, Pp 14-17, Vol.2, Issue no.10.

9. Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques", International

Journal Of Engineering And Computer Science, ISSN:2319-7242, April 2017, vol. 6, Issue no. 4.

10. Tutorials Point, ASP.Net TUTORIALS, [Online], Available from: https://www.tutorialspoint.com/asp.net/ [Accessed 12th Sep 2017]

11. w3schools.com, ASP Tutorial - W3Schools, [Online], Available from: https://www.w3schools.com/asp/ [Accessed 12th Sep 2017]

12. Microsoft, ASP.NET Core tutorials, [Online], Available from: https://docs.microsoft.com/en-us/aspnet/core/tutorials/ [Accessed 24th Sep 2017]

13. ProgrammingKnowledge, ASP.NET Tutorial 1- Introduction and Creating Your First ASP.NET Web Site, [Video], Dec 8, 2013, Available from: https://www.youtube.com/watch?v=KVlXccl-XBA&list=PLS1QulWo1RIaM8-S7kTHgWd_pGNu-CyQS [Accessed 20th Sep 2017].

14. Michiel Wouters, Create a website with ASP.Net - Part 1, [Video], Dec 8, 2013, Available from: https://www.youtube.com/watch?v=aUx2Bdx68f4 [Accessed 28th Sep 2017].