iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40888

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Pocket Certificates using Double Encryption

Ajay Kumar[1], Dr. Umarani Chellapandy[2]
[1]*Student,* [2]*Professor, Department of MCA, Jain (Deemed-to-be University), Bengaluru, Karnataka, India*

Abstract: ***The Pocket Certificates System is software that attempts to encrypt the authenticity of government-issued documents like as Unique identification cards Addhaar and PAN cards. To secure our programme, we employ a combination of cryptography techniques (for example, AES, DES, and RSA). The main purpose of Pocket Certificates is to give users the flexibility of sending data while trying to implement encryption standards according to the specification and algorithms suggested, storing information in an encrypted form that is unintelligible, and making documents available on their private accounts. When a client asks a document to be downloaded, the system decrypts the document on the server. The entire programme will have a user-friendly Graphical User Interface that the end user will be able to learn on their own. All functional standards for effective navigation will be provided by the System.***
Keywords: Cryptography, Encryption, Decryption, AES, DES.

I. INTRODUCTION

Almost all government-issued papers in India are currently available in tangible form across the country. This implies that if a resident has to share a document with an agency in order to obtain a service, an attested photocopy is supplied, either in physical or digitised form.

Physical copies of documents suffer significant overhead in terms of human verification, paper storage, manual audits, and other tasks, all of which are costly and inconvenient. This makes it difficult for multiple organisations to check the validity of these papers, opening up opportunities for the use of forged documents and certifications. Due to the lack of a clear identification tied to these documents, anyone with the same name might definitely misuse someone else's document.

DigiLocker, the government of India's national digital locker system, which gives 1GB of free storage capacity in the vault to safely keep resident papers, is comparable to our project concept. However, it has several downsides, such as the fact that citizens cannot log in unless they have an Aadhar card. Another concern is that DigiLocker does not allow for the storage of all documents; it only permits for the storage of specific types of documents. Citizens can also upload papers that may or may not be authentic. However, our product not only provides for the online storage of documents, but it also ensures their legitimacy and security.[1], [2]

II. PROBLEM STATEMENT

Every time we apply for a job, admission to a course, or any other reason at a university or corporation, we must provide all of the documentation from all prior tests, as well as evidence of identification. The papers must also be attached to the form, with a correct copy made. All of this necessitates a great deal of verification, and the form gets difficult as a result of the numerous papers attached. Due to his neglect, the employees might sometimes make errors in verification, which can lead to errors. There is also a significant financial loss if these documents are missing. To avoid such circumstances, we have devised a project concept in which all papers would be prepared and delivered as soft copies to the Indian peoples. [1]

They'll take up more storage space, and they'll be encrypted with a variety of security techniques.

Existing citizens can apply for it and receive their card, as well as other identity evidence.

1) The administrator will see a list of all citizens with their UIN (Unique Identification Number), which is unique to each citizen, and he will be able to see it by state and city.
2) Once the government receives a request for account formation from the hospital, the government validates the newborn citizen and opens an account for them. It also provides birth certificates.
3) As additional documents are required, citizens can apply for new documents such as a domicile certificate, passport, PAN card, and so on.
4) Citizens will get an e-mail and a text message alerting them of the document upload when it has been successfully created and uploaded.
5) Citizens will be able to read, download, and share their papers (through email) with other people/companies/institutions. • These documents will be encrypted by the government/server using techniques such as AES and DES. They can only be decrypted using Citizen's Private Key. This will keep papers secure by preventing unwanted access to them.

III. RELEVANCE OF THE PROJECT

A. The "Pocket Certificate for Government Portal Using Combined Cryptography" will compile a detailed profile of each citizen.
B. When a citizen is born, the hospital transmits a message to the government for a birth certificate. As a result, each citizen's account is established.
C. Every person will be given a card (we may utilise the Aadhar Card to avoid creating extra papers) that has a UID (Unique Identity) number, and all documents will be uploaded to this account.
D. That will include all of his examination results from his S.S.C. to the present, as well as all government-issued examination results and identity papers.
E. These findings will be in the form of "E-Certificates," with a compressed format that won't take up as much storage space. They will also be encrypted utilising a variety of security techniques.
F. Existing citizens can apply for it and receive their card, as well as other identity evidence.
G. The administrator will see a list of all citizens with their UIN (Unique Identification Number), which is unique to each citizen, and he will be able to see it by state and city.
H. Once the government receives a request for account formation from the hospital, the government validates the newborn citizen and opens an account for them. It also provides birth certificates.[3]
I. As additional documents are required, people can apply for new documents such as a domicile certificate, passport, PAN card, and so on.
J. People will get an e-mail and a text message alerting them of the document upload when it has been successfully created and uploaded.
K. People are able to read, download, and share their papers (through email) with other people/companies/institutions.
L. Those documents will be encrypted by the government/server using techniques such as AES and DES. They can only be decrypted using Citizen's Private Key. This will keep papers secure by preventing unwanted access to them.

IV. SCOPE AND OBJECTIVE

A. Empower residents' digital independence by presenting them with a Digital Locker called Pocket Certificates.
B. Use tangible papers as little as possible.
C. includes Ensuring the integrity of e-documents, preventing the use of forged papers.
D. People have secure access to government-issued papers via a mobile application.
E. Lower administrative costs for government departments and agencies, making it easier for citizens to get services.
F. Documents may be accessed at any time and from any location.
G. Enabling secure access to documents by creating a PIN for login and making them accessible electronically whenever needed.

V. ALGORITHM USED

A. AES

The AES cypher is a block cypher.
key can be 128/192/256 bits in length.
Data is encrypted in 128-bit chunks.
AES uses bytes rather than bits to conduct operations. The cypher handles 128 bits (or 16 bytes) of incoming data at a time since the block size is 128 bits.
The number of rounds is determined by the length of the key as follows:
10 rounds using a 128-bit key
12 cycles using a 192-bit key
14 rounds using a 256-bit key

B. DES

DES is a Feistel Cipher algorithm. It has a Convolution with 16 rounds. The blocks are 64 bits in size. DES has an adequate and effective length of 56 bits, despite the fact that the key length is 64 bits. This is because 8 of the 64 bits of the key are not utilised by the encryption algorithm (function as check bits only).[4], [5]

VI. SYSTEM DESIGN

A. *System Architecture*

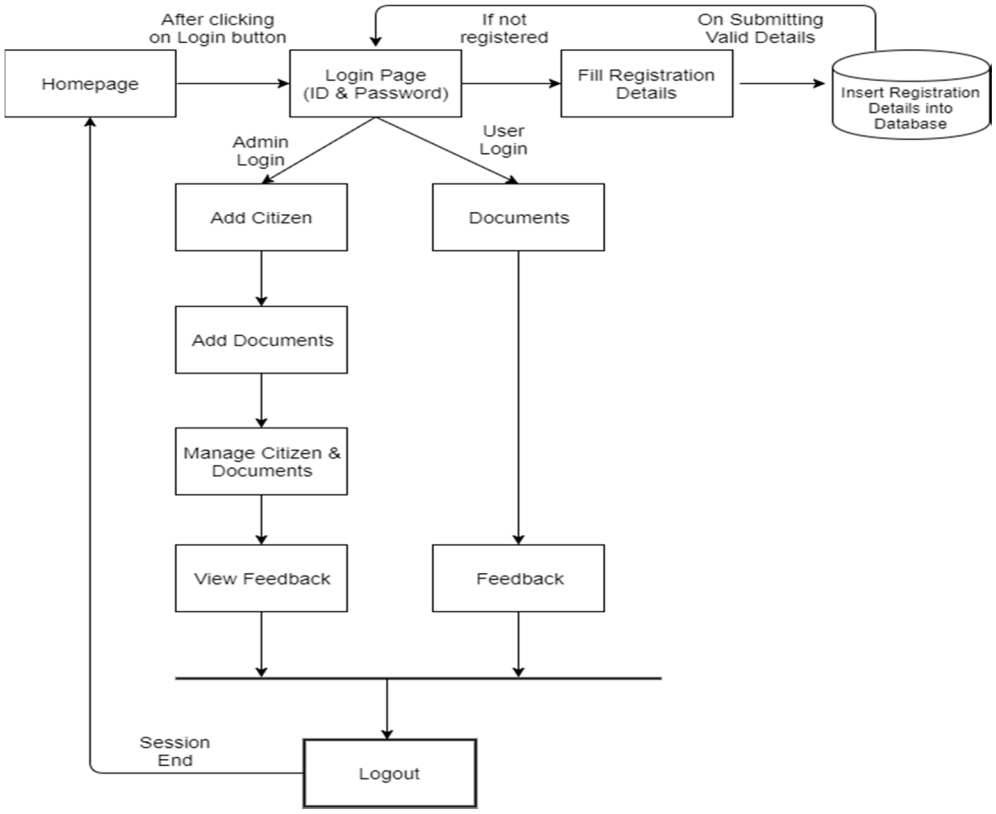


Fig. 6.1: Pocket Certificates using Double Encryption

B. *Use Case Diagram*

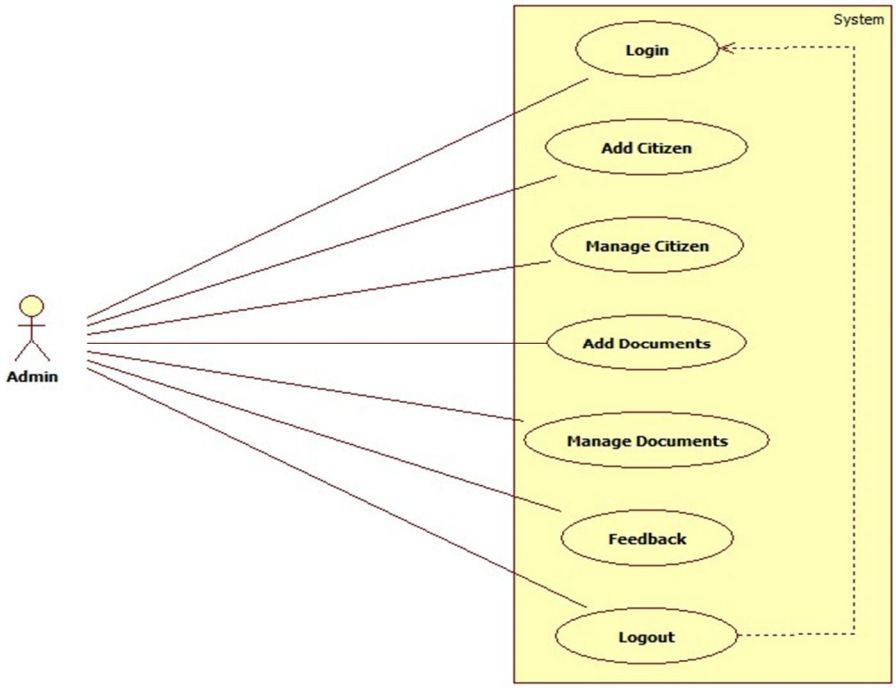


Fig. 6.2.1 : Use Case Diagram of Admin

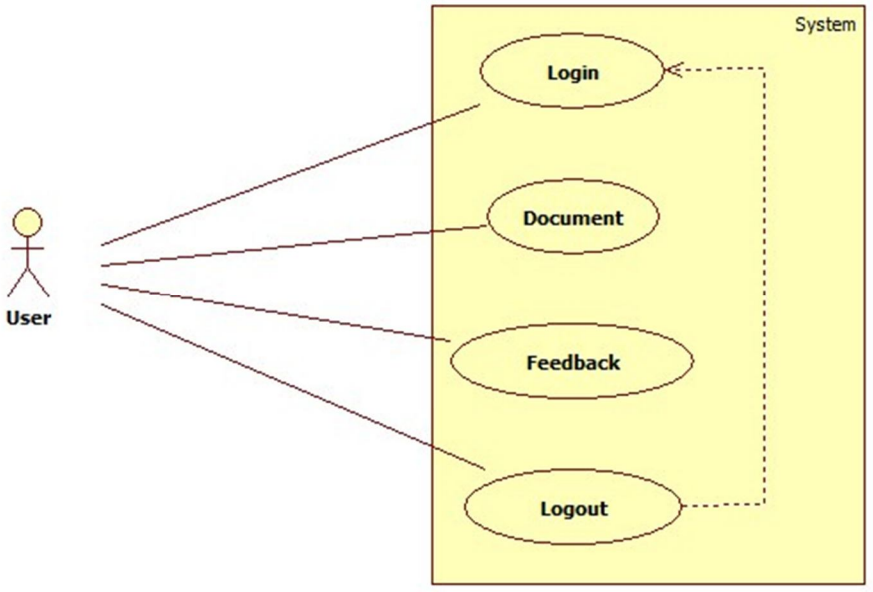


Fig. 6.2.2 : Use Case Diagram of User

C. System Requirements

Visual Studio 2010 has the project loaded. Visual Studio was used to design and code the project. We created and maintained all databases in SQL Server 2008, in which we created tables and wrote queries to hold project data and records.

1) Hardware Requirement

i3 Processor Based Computer or higher
Memory: 1 GB RAM
Hard Drive: 50 GB
Monitor
Internet Connection

2) Software Requirement

Windows 7 or higher
Visual studio 2010.
SQL Server 2008.

D. Front End Technology

1) Microsoft .NET Framework

a) The.NET Framework is a new computing platform that makes it easier to construct applications in the Internet's widely dispersed environment. The.NET Framework was created with the following goals in mind:

b) To offer a consistent object-oriented programming environment regardless of whether object code is saved and run locally, locally but disseminated via the Internet, or remotely.

c) To create an environment for code execution that reduces software deployment and versioning conflicts.

d) To provide a code-execution environment that assures the safe execution of programmes written by untrusted or partially trustworthy third parties.

e) To offer a code-execution environment that does not suffer from the performance issues that scripted or interpreted environments suffer from. Why To ensure that the developer experience is uniform across a wide range of apps, including Windows and Web-based applications.

f) All interaction should be based on industry standards to guarantee that code written with the.NET Framework can function with any other code.

2) *Microsoft Visual Studio:* Microsoft Visual Studio is an integrated development environment (IDE) developed by Microsoft for several forms of software development, including computer programmes, websites, web applications, online services, and mobile apps. To make the software development process easier, completion tools, compilers, and other features are incorporated.
3) *Microsoft SQL Server:* Microsoft SQL Server is a relational database management system (RDBMS) used in corporate IT settings to handle a wide range of transaction processing, business intelligence, and analytics applications.

E. Modules

The system is made up of the following two primary modules and their sub-modules:

1) Admin

a) Login: Admins must use their valid login credentials to log in.
b) Add Citizen: The administrator can add a new citizen by providing basic information such as Aadhaar ID and DOB.
c) Citizen Management: The admin may handle all of the citizen information that has been added.
d) Add Documents: The system allows administrators to search for citizens using their Aadhaar numbers and enter document types and documents. Encrypt with Triple DES and AES, then send an email to the citizen.
e) Document Management: Search Citizen with a List of Uploaded Documents and Upload Option.
f) Feedback: The administrator has access to the feedback messages sent by registered users.[1], [6]

2) User

a) Login: The user must log in using their credentials, including their Aadhaar ID and OTP.
b) Documents: The user can view a list of all encrypted files in his or her document. On download, the file undergoes a reversal procedure and is converted to its original format. After a user logs into the system, he or she can choose Document Decrypt. The user can browse any of the documents and download them as needed.
c) Feedback: A user can provide a message of feedback, which will be forwarded to the administrator.[2], [7]

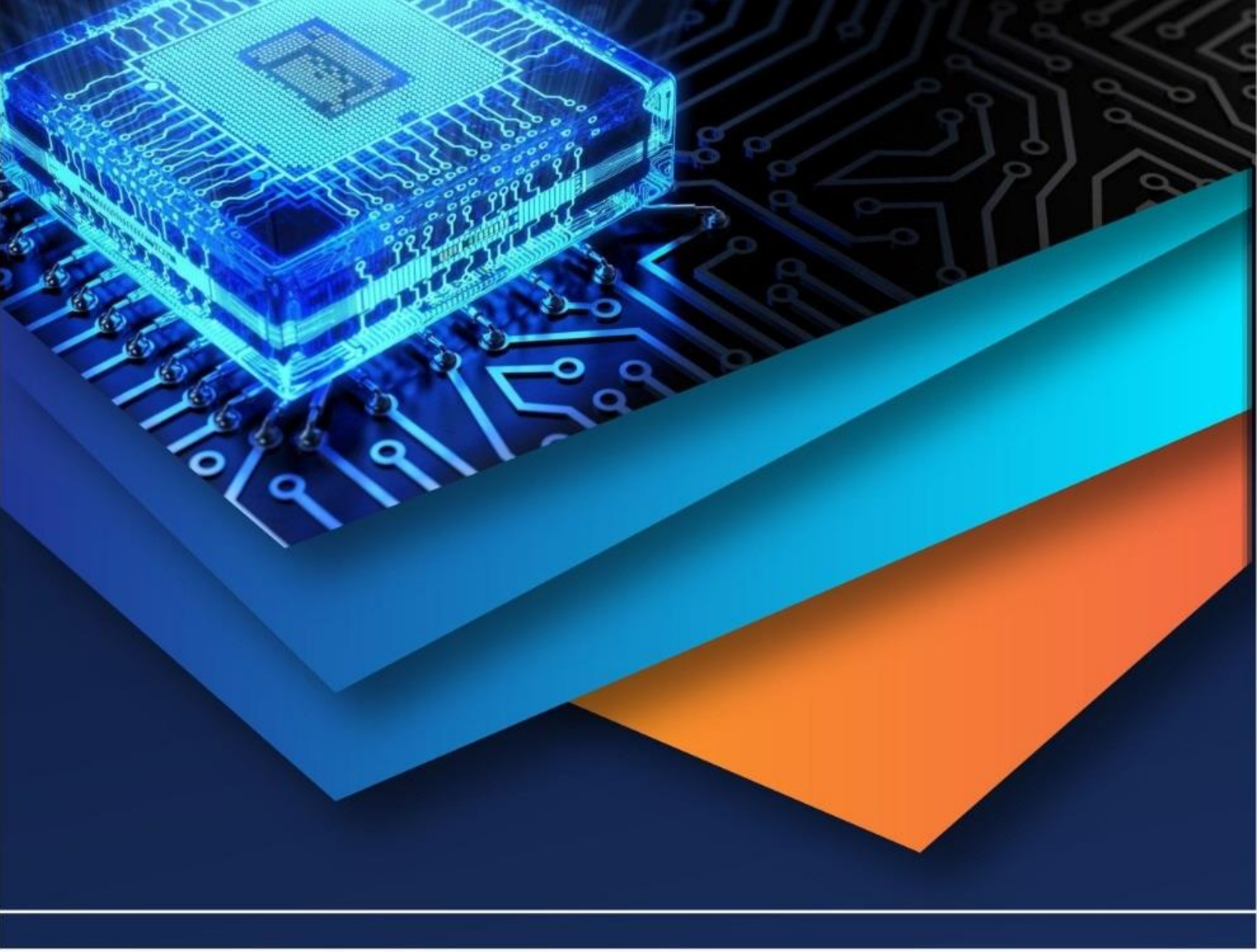
VII. CONCLUSION

This was our System Design project for "Pocket Certificates with Double Encryption," which is a web application written in the.NET programming language. We have put a lot of effort into developing this system. We believe that this system provided us with a great deal of satisfaction.

Even if no work is ever stated to be ideal in the development area, there may be room for improvement in this application. We studied a lot and got a lot of expertise in the field of development. We are hoping that this will be fruitful for us.

REFERENCES

[1] S. Chavan, P. Gaikwad, K. Guided, and P. M. Rodgrigues, “Pocket Certificate for Government Portal using combined Cryptography,” International Journal of Scientific & Engineering Research, 2018, [Online]. Available: http://www.ijser.org
[2] Kongunadu College of Engineering & Technology and Institute of Electrical and Electronics Engineers, Proceedings, International Conference on Smart Electronics and Communication (ICOSEC 2020) : 10-12, September 2020.
[3] J. Kaur, S. Lamba, and P. Saini, “Advanced Encryption Standard: Attacks and Current Research Trends,” in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021, Mar. 2021, pp. 112–116. doi: 10.1109/ICACITE51222.2021.9404716.
[4] “Design and Implementation of Pipelined AES Encryption System using FPGA,” International Journal of Recent Technology and Engineering, vol. 8, no. 5, pp. 2565–2571, Jan. 2020, doi: 10.35940/ijrte.e6475.018520.
[5] A. Hamza and B. Kumar, “A Review Paper on DES, AES, RSA Encryption Standards,” in Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020, Dec. 2020, pp. 333–338. doi: 10.1109/SMART50582.2020.9336800.
[6] Sri Venkateshwara College of Engineering. Department of Electronics and Communication Engineering, Institute of Electrical and Electronics Engineers. Bangalore Section, IEEE Computer Society, and Institute of Electrical and Electronics Engineers, RTEICT 2018 : 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology : 2018 proceedings : Bengaluru, Karnataka, India, May 18-19, 2018.
[7] “A Review Paper on Cryptography.”



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY