IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Pocket Certificate Using Double Encryption by Combined Cryptography

Dr. K. Velmurugan[1], G. Rishi Kumar[2], G. Sivasurya[3], S. Syed Muhammed Ashmueel[4]
Professor and Head, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *The Pocket Certificates System is software that attempts to encrypt the authenticity of government-issued documents like as Aadhaar cards and PAN cards. In order 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 passing information while implementing encryption standards according to the specification and algorithms proposed, storing information in an encrypted form that is unreadable, and making documents available on their private accounts. Whenever a user requests a file, the system decrypts the document stored on the server. The entire programme will feature a user-friendly Graphical User Interface that will allow the end user to learn on their own. The system will meet all functional requirements for proper navigation.*

Keywords: Pocket Certificates System.

I. INTRODUCTION

Almost every document issued by the Indian government is physically available throughout 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 shared, either physically or electronically. The use of physical copies of documents adds a lot of overhead in terms of human verification, paper storage, manual audits, and other things, all of which add up to a lot of money and time. This makes it difficult for numerous organisations to check the validity of these documents, resulting in loopholes for the use of forged documents. Because no solid identify is tied to these documents, anyone can utilise them with the document. This system is a digital locker that gives inhabitants digital empowerment. It reduces the consumption of paper documents. The system ensures the validity of e-documents and prevents the use of forged papers. Documents are more secure using this method. It lowers the administrative burden on government departments and organisations while making it easier for citizens to access services. Multiple users can access documents at any time and from any location.

Data encryption is critical in the real-time context because it keeps data out of the hands of unauthorised persons and prevents it from being manipulated or tampered with. This article discusses a system that allows citizens to obtain their original documents at any time. Citizens should not have their original documents with them at all times. All that is required of the citizen is to log into the system and download the appropriate document. This technology protects the papers with a high level of security. This system is mostly used for security purposes. Citizens' documents are encrypted in this system utilising AES-based combination cryptography. When a user or citizen requests a copy of a document, the server decrypts it. This will decrease the verification team's paper work and effort because all of the papers will be stored in a single, safe location.

II. METHODOLOGY

2.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric block cypher that the United States government has chosen to safeguard confidential information. To encrypt sensitive data, ES is used in software and devices all around the world. It's critical for government computer security, cyber security, and data security.

2.2 How AES Encryption Works

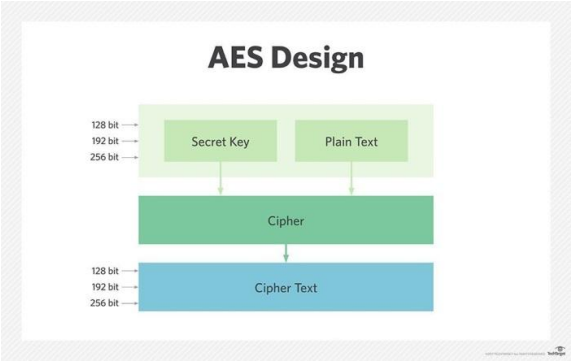
Three block cyphers are included in AES:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

1. AES-128 encrypts and decrypts a block of messages with a 128-bit key length.
2. AES-192 encrypts and decrypts a block of messages with a 192-bit key length.
3. AES-256 encrypts and decrypts a block of messages using a 256-bit key length.

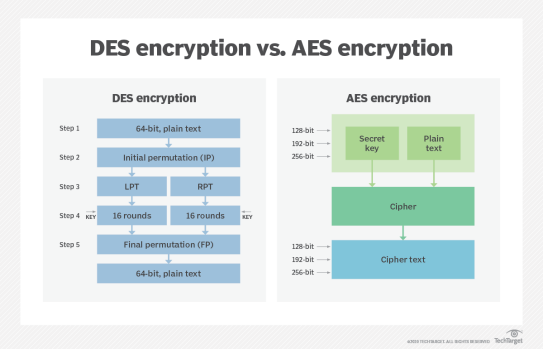
Each cypher encrypts and decrypts data in 128-bit blocks using 128, 192, and 256-bit cryptographic keys, respectively. Symmetric cyphers, often known as secret key cyphers, encrypt and decode using the same key. Both the sender and the recipient must have access to the same secret key. Information is classified by the government into three categories: confidential, secret, and top secret. The Confidential and Secret levels can be protected with any key length. Key lengths of 192 or 256 bits are required for top-secret information.

For 128-bit keys, there are 10 rounds, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round is made up of numerous processing phases, including The input plaintext is substituted, transposed, and mixed to create the final output of cypher text.



The AES encryption technique specifies a number of changes to be applied to data in an array. The cipher's initial step is to organise the data into an array, following which the cypher modifications are done over and over again.

The replacement of data using a substitution table is the first transformation in the AES encryption algorithm. The data rows are shifted in the second transformation. The third is a column mix. Each column undergoes the final transformation, which employs a different component of the encryption key. Longer keys need more rounds.



III. SYSTEM ANALYSIS

3.1 Existing System

Almost every document issued by the Indian government is available in tangible form throughout 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. Existing citizens can apply for it and receive their card, as well as other forms of identification. 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. also city wise. At When 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. Citizens can apply for new documents such as a domicile certificate, passport, PAN card, and so on as time goes on and more documents are required. Citizens will receive an e-mail and an SMS notification after the papers have been successfully created and uploaded. Citizens can read, download, and share their

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

papers (through email) with other people, corporations, and institutions. These documents will be used for the government's/perspective, server's data should be

Disadvantage

Using physical copies of documents incurs significant overhead in terms of human verification, paper storage, manual audits, and other costs and inconveniences. This makes it difficult for multiple authorities to check the validity of these documents, opening up opportunities for the use of forged documents and certifications.

As a physical copy, all of this necessitates a great deal of verification, and the form gets cumbersome as a result of the numerous papers 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.

3.2 Proposed System

This system is a digital locker that gives inhabitants digital empowerment. It reduces the consumption of paper documents. The system ensures the validity of e-documents and prevents the use of forged papers. Documents are more secure using this method. Multiple users can access documents at any time and from any location. Users will receive an e-mail and an SMS notification when their papers have been successfully created and uploaded. The main purpose of Pocket Certificates is to give users the flexibility of passing information while implementing encryption standards according to the specification and algorithms proposed, storing information in an encrypted form that is unreadable, and making documents available on their private accounts.

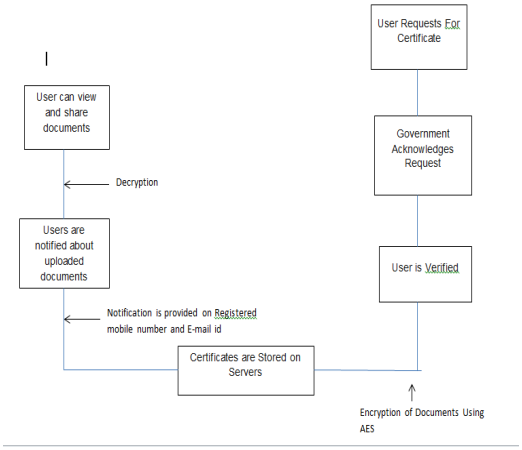
Advantage

The use of hard copies of documents incurs significant overhead in terms of human verification, paper storage, manual audits, and so on, while providing low cost and convenience.

This makes it difficult for multiple authorities to check the legitimacy of these documents, resulting in gaps that allow legitimate documents and certifications to be used.

IV. SYSTEM ARCHITECTURE

A system architecture is a conceptual model that specifies a system's structure, behaviour, and other perspectives. A formal description and representation of a system arranged in a way that facilitates reasoning about the system's structures and behaviours is known as an architectural description.



4.1 Algorithm

Advanced Encryption Standard (AES)

Encryption steps for a 128-bit block:

1. From the cypher key, create a series of round keys.
2. Load the block data into the state array (plaintext).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

3. In the beginning state array, add the initial round key.
4. Manipulate the state for nine rounds.
5. Complete the tenth and final state manipulation round.
6. Copy the final state array out as the encrypted data (cipher text).

The order of operation in decryption is:

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

4.2 Module Implementation

Module List

- User Registration
- Document Digitization
- Encryption & Decryption
- Document Retrieval

4.3 Module Description

A. User Registration

The first and most important stage in the Certificate Encryption Process is User Registration.This registration includes the following information: name, email address, phone the number of children, their gender, and their birthdate. Create Password and Confirm Password are two steps that must be completed by a person.

Once these procedures are completed, the user may log in with his credentials and execute the functions he or she desires.

B. Document Digitization

The process of transforming paper documents into a digital (i.e. computer-readable) format that computer systems may employ to automate processes or workflows is known as document digitization.Rather information sitting on paper and being stored in a physical file cabinet, it must be transferred to digital format in order to gain meaningful insights.

Aadhaar, PAN card, driving licence, and other documents may be uploaded using this method.

C. Encryption & Decryption

Encryption is a security mechanism for converting plaintext data into cypher text that can only be decoded by the user with the encryption key. The certificates can be encrypted after uploading and a secret key produced using encryption. Encrypted documents are kept in a secure database, and decryption is the process of converting encrypted material back to its original form. It's essentially a reversal of the encryption process.

It decodes the encrypted document so that an authorized user can only decrypt the data because decryption requires a secret key.

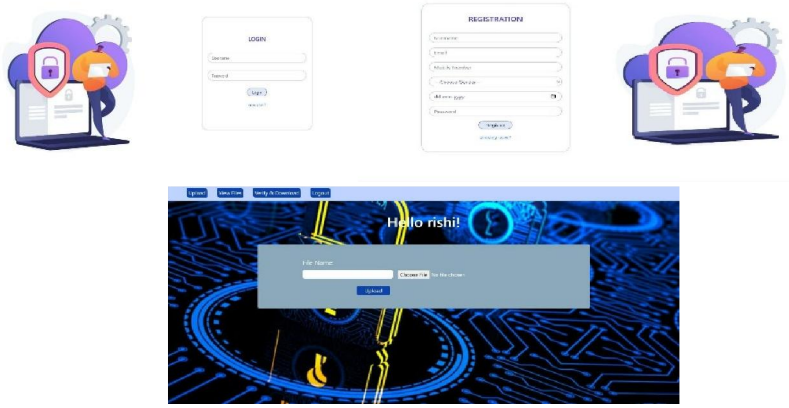
D. Document Retrieval

Document retrieval is a computerised procedure that includes the registered user decrypting encrypted documents in order to produce a relevant document in response to an inquirer's request.

Using the secret key, the user can download the desired document from the server at any time and from any location.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

V. IMPLEMENTATION AND OUTPUT



VI. CONCLUSION

The project provides us with a way to carry our sensitive papers freely without fear of them being tampered with, as well as the ability to produce them securely at any government-related body as confirmation of our identification. The key aspect of our system is that it employs Combined Cryptography, making it nearly hard for hackers to get access to it.

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] Abhinandan Aggrawal, 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,
[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].