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.2022.41090

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: A Survey

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

Abstract: ***Documents are items that convey information, can be used to certify someone, or can constitute a legal report. Theft of such crucial documents/certificates can obstruct or hinder an individual's or organization's ability to execute their work effectively, as well as result in the loss of personal belongings. "Pocket Certificates" - a traditional document archive with the possibility of securely preserving such papers - is provided in this text. The answer is to utilise a Double Encryption system that combines the AES and 3DES encryption standards. The use of improved security can be considered of as a tradeoff in a system's stability and smooth operation, however there are specific limitations that must be imposed so that the Encryption/Decryption process does not obstruct usability. This work considers such characteristics and strikes a balance between them all. Other Hashing methods are also used, such as bycrypt for securely storing user login data and passport middleware for each application stage's specific user authentication needs. The paper comprises of a comprehensive online application for the safe archiving of essential documents or data.***

Keywords: 3DES, AES, Cryptography, Decryption, Encryption.

I. INTRODUCTION

Physical documents are currently used by more than 70% of people. Physical copies of documents suffer significant overhead in terms of security, paper storage, manual audits, and other areas, resulting in significant expense and annoyance. The modern workplace necessitates the implementation of suitable security measures for all types of paperwork, digital and otherwise. While stealing papers from a traditional cabinet locker is simple, digital theft, replication, and deletion can be more difficult. The use of encryption technologies in conjunction with proper document structure will ensure that sensitive material remains safe.

The Pocket Certificates System is designed to employ both AES and 3DES algorithms in tandem for secure and irreversible document storage. It also seeks to verify that the user's identity is genuine and unharmed, which is accomplished by using the passport function to verify the user's authenticity and the crypt function to store the password in a safe hashed/encrypted format.

The system is built to be as dependable, useful, and smooth as possible while maintaining the security of the documents saved in the database.

II. LITERATURE REVIEW

Almost all govt documents in India are presently available in tangible form across the country. This implies that if a resident has to share a document with an agency in order to acquire a service, an attested photocopy is given, either in physical or digitised form.

Utilization of actual duplicates of archive makes gigantic upward with regards to manual confirmation, paper capacity, manual reviews, and so forth bringing about significant expense and bother. This makes issue for different offices to check the legitimacy of these reports, accordingly, making provisos for utilization of phony records/testaments. Because of the idea of these archives not having a solid character appended to it, anybody with same name can for sure abuse another person's report.[1]–[3]

III. AES AND DES ENCRIPTION TECHNOLOGY

Typical symmetric block cyphers are DES (Data Encryption Standard) and AES (Advanced Encryption Standard). To alleviate the disadvantages of DES, AES was devised. Due to the decreased key size of DES, which makes it less safe, triple DES was created, but it proved to be slower. As a result, the National Institute of Standards and Technology later introduced AES.

A. DES (Data Encryption Standard)

The Feistel structure divides plaintext into two halves, which is the basis for DES. DES generates 64-bit Ciphertext from 64-bit plain text and a 56-bit key.[4]–[6]

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

The following functions are included in each round:
Expansion Permutation: The 32-bit right component is enlarged to a 48-bit right portion in this example.

1) *XOR (Whitener):* DES performs an XOR operation on the enlarged right section and the round key after the expansion permutation. This action necessitates the usage of the round key. The 48-bit right part is Xored with the 48-bit subkey extracted from the 56-bit key, yielding a 48-bit output.
2) *Substitution Boxes (S-boxes):* The S-boxes are in charge of the actual mixing (confusion). Eight S-boxes, each with a 6-bit input and 4-bit output, are used in the DES algorithm. The 48-bit output from the Xor stage is reduced to 32 bits once more.
3) *P-box:* The 32-bit result from S-box is permuted once again, resulting in 32-bit permuted output.

B. AES (Advanced Encryption Standard)

Because DES utilises a relatively short encryption key and the technique is rather sluggish, AES was created to replace it.
The AES method uses a 128-bit plaintext and a 128-bit secret key to create a 128-bit block that can be represented as a 4 X 4 square matrix. An initial transformation is performed on this 4 X 4 square matrix. The 10 rounds come after this phase.

The following stages are included in the nine rounds:

1) *Sub Bytes (Byte Substitution):* It use S-box to execute byte-by-byte substitution of the entire block (matrix). The 16 input bytes are substituted by looking up a fixed table (S-box) supplied in design. A four-row, four-column matrix is the ultimate product.
2) *Shift Rows:* The matrix's rows are shifted. The four rows of the matrix are all shifted to the left. Any 'falling off' entries are re-inserted on the right side of the row.

The following is the procedure for carrying out the shift:

a) The first row has not been moved.
b) The second row is moved one (byte) to the left.
c) The third row has been moved two spaces to the left.
d) The fourth row is moved three spaces to the left.
e) The outcome is a new matrix made up of the same 16 bytes that have been moved in relation to each other.

3) *Mix Columns:* The matrix's columns are shuffled from right to left. Each four-byte column is now altered using a specific mathematical function. This method takes four bytes from one column as input and returns four entirely new bytes that replace the original column. As a consequence, a new matrix with 16 additional bytes is created. It's worth mentioning that in the final round, this step is bypassed.
4) *Add Round Keys:* This does a Xor of the current block and the expanded key. The final tenth round uses just Subbytes, Shift Rows, and Add round keys phases, yielding a ciphertext of 16 bytes (128 bits).

IV. PROPOSED SYSTEM

Pocket Certificates is a sophisticated programme in which file storage makes it highly efficient and trustworthy because we don't have to carry all of our documents with us all of the time. Legal documents, such as passports and birth certificates, are extremely valuable and can be exploited. Putting information on any server is a risky move since it may be hacked, and keeping it on our phone is more worse.
To avoid any type of internal or external hacking, we designed a mechanism that saves the submitted document in an encrypted form and keeps it in the Internal Memory.
The key benefit of this approach is that it requires a Secure Pin to access the file that we input when we register. If our phone is in someone's hands, they won't be able to access the data because of the secure pin.
The files are protected in a variety of ways to ensure that no unauthorised individuals have access to them. To support the application, we use SQL as the backend.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

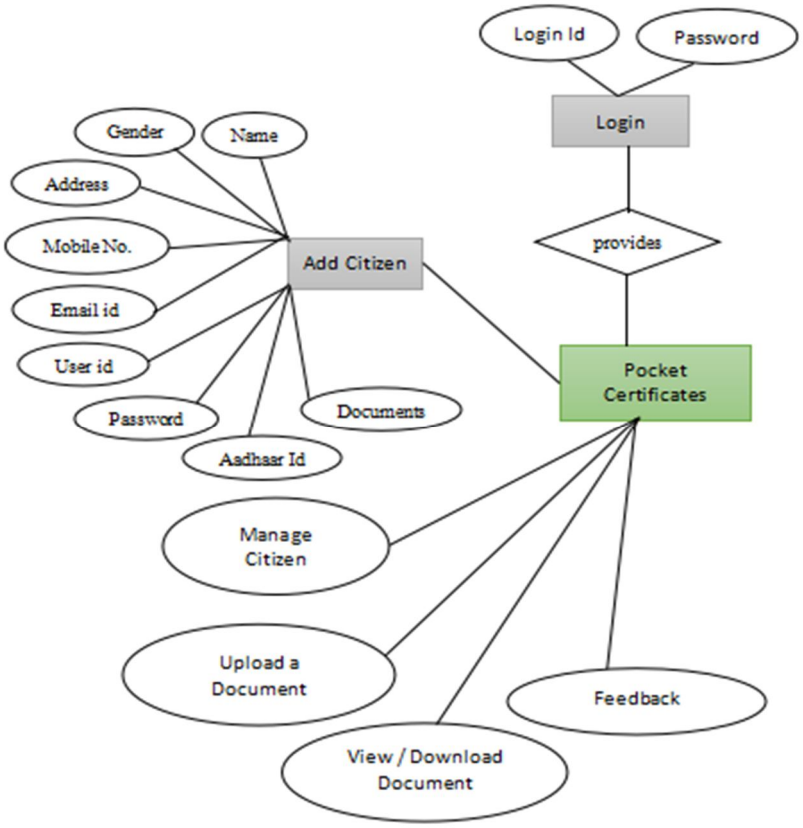


Fig. 1: E-R Diagram

V. ENCRYPTION AND DECRYPTION PHASE

We all function on the internet, interact on the internet, and want our data and information to be safe, which cryptography allows us to achieve. Cryptography protects our personal data and information from other users and attackers. Encryption and decryption are the two most important functions of cryptography.[7], [8]

A. Encryption Techniques

Encryption is the process of converting a sender's original communication into an unreadable format that no one on the network can read or understand. It turns a regular communication, such as plain text, into ciphertext, which is nonsensical or worthless. The unintelligible version of the message is completely different from the original message. As a result, attackers and many other agents are unable to read the data since senders use an encryption technique to convey the data. It occurs at the sender's end. Using the secret key or public key, the communication may be readily encrypted.

The process of applying the encryption technique and converting the original message and data to ciphertext is depicted in the diagram below.

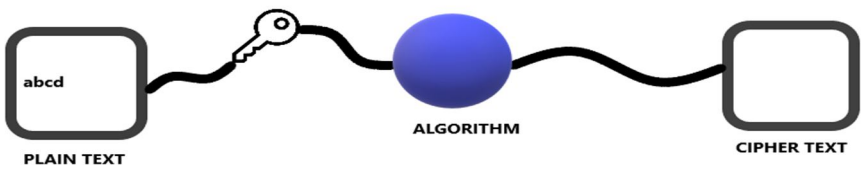


Fig. 2: Encryption work

©IJRASET: All Rights are Reserved

B. Decryption Techniques

Decryption is the process of converting an encrypted code or data into a form that can be understood and read by a person or computer. This is referred to as decrypting encrypted data. It occurs at the receiving end. The secret key or the private key can be used to decode the communication.

The decryption procedure is shown in the picture below, as well as the encrypted text (i.e., the ciphertext is transformed back to the original message).

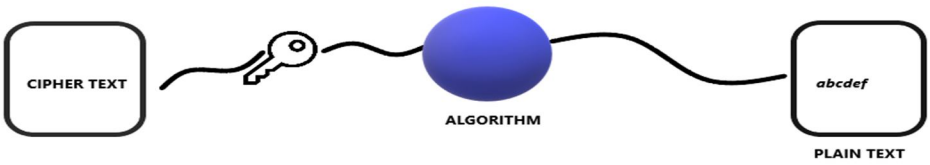


Fig. 3: Decryption work

C. Keys are available in a variety of shapes and sizes.

There are a few important presents that assist in the encryption and decryption process. Let's take a closer look at the keys that are available.

D. Key That Is Symmetric

This key is used in the Symmetric Encryption algorithm, which is also known as the Symmetric-key encryption algorithm. The encryption of plaintext on the sender's side and the decryption of ciphertext on the receiver's side are both done with the same cryptographic keys.

E. Key That Is Asymmetric

The asymmetric key encryption algorithm employs two sets of keys for encryption. These two distinct keys are used to encrypt and decrypt data, respectively. The public key is accessible to everybody, but the secret key is only accessible to the message's recipient. When compared to symmetric key encryption, this gives higher security.

F. Key that is Made Public

The keys that are used to encrypt the message for the receiver are known as public keys. This cryptography is a key-based encryption scheme using two pairs of keys.

G. Secret Key

Because the private key may be used to encrypt and decrypt data, it is commonly employed with asymmetric encryption algorithms. It might also be a component of an asymmetric public/private key pair.

H. Key That Has Been Pre-Shared

PSK is a shared secret key that was previously shared between two distinct organisations or persons through a secure channel before being utilised.

VI. CRYPTOGRAPHY TECHNIQUES PHASE

Here are some simple codes and more advanced contemporary encryption methods that are now utilised on the Internet.

A. Simple Codes

This category encompasses any method of writing a message side by side that makes it difficult for others to read. This entails writing in a different alphabet. We can see Icelandic runes and IPA, as well as other niche-built alphabets like the Deseret Alphabet, here.

We can utilise language to code in this. We investigated the origins of invented languages like Elvish and Esperanto.
The book Code Talker by Chester Naz and Judith Schiess Avila discusses how the Navajo language was utilised as a code during WWII and how it was never cracked under harsh situations.
If the Navajo language lacked words for a concept, the code speakers came up with a phrase. For example, the Navajo term for "hummingbird" had become a fighter jet, while "iron cap" had been Germany.

B. Symmetric Encryption

Symmetrical encryption is a kind of encryption that uses just one key to encode and decode electronic data (a secret key). Symmetrical encryption techniques like substitution cyphers exist, but current symmetric encryption may be far more sophisticated.
Using symmetrical encryption techniques, data is turned into a format that no one can decipher without a secret key.
Symmetric encryption is an older algorithm than asymmetric encryption, yet it is quicker and more efficient. Because of symmetric encryption's superior performance and quickness as compared to asymmetric encryption.
Symmetric key cryptography, on the other hand, uses the same key for both encryption and decryption. Asymmetric key cryptography uses one key for encryption and a separate key for decryption at the same time.
Symmetric encryption is common for large amounts of data, such as database encryption and bulk encryption. The secret key can only be encrypted or decrypted by the database itself in the event of a database.

C. Asymmetric Encryption

Public-key cryptography is another name for asymmetric encryption. Asymmetric key encryption aids in the resolution of the symmetric key cryptography key exchange problem. In asymmetrical encryption, two keys are utilised to encrypt plain text. The secret keys are shared across the internet or a large network. Because anybody with a secret key may decrypt the message, asymmetric encryption employs two matching keys to boost security.
A public key will be publicly accessible to everyone who chooses to send you a message, while the second private key will be kept hidden for you to comprehend alone. A private key can decode a message encrypted using a public key. With a public key, a communication encrypted with a private key may be deciphered.

D. Steganography

Steganography is a technology that allows a message to be hidden inside another message. People employed invisible ink, minute changes, and other means to hide messages in the past.
However, in today's technological world, Steganography is a technique for hiding data, which can be a file, message, picture, or other type of data, among other files, messages, or images.

E. Hashing

Hashing is a cryptographic technique for converting any type of data into a single string. Any data may be hashed using a hashing algorithm, regardless of its size or nature. It turns data of arbitrary length into a fixed hashed value.
Hashing differs from other encryption methods in that it does not allow for reverse encryption; that is, it cannot be decoded using keys. The most extensively used hashing algorithms are MD5, SHA1, and SHA 256.

VII. FUTURE SCOPE

1) *Demand Balancing:* Because the system will only be accessible to administrators, the amount of load placed on the server will be restricted to the duration of admin access.
2) *Easy Accessibility:* Records and other information may be retrieved and stored with ease.
3) *User-Friendly:* The website will cater to all users in a highly user-friendly manner.
4) *Efficient and Dependable:* Keeping everything secure and database on the server, which will be available according to user requirements without any maintenance costs, will be a lot more efficient than storing all client data on spreadsheets or in physical record books.
5) *Simple to Maintain:* Pocket Certificates with Double Encryption are designed to be simple to maintain. As a result, upkeep is also simple.[9]

©IJRASET: All Rights are Reserved

VIII. CONCLUSION

In this work, a dual encrypted method for storing users' private papers is presented. The fundamental goal of using many encryption layers was to maintain the CIA trinity of secrecy, authenticity, and integrity of the user's data as well as the system's validity. Most assaults, such as brute force and the use of other tools to compromise the system's security, are prevented by using many levels of encryption. Multiple encryptions may slow down the system's speed, but it may slow down assailants, who would need a lot more storage if they used comparison lists on more than one encryption level.

IX. ACKNOWLEDGMENT

I want to specially thank Dr. Umarani .C for guiding me throughout this research paper, which has expanded my knowledge on data security and cyber security. Without her support I do not think this research paper will be been a success, I am very thankful.

REFERENCES

[1] 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.

[2] 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.

[3] “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.

[4] 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.

[5] “A Review Paper on Cryptography.”

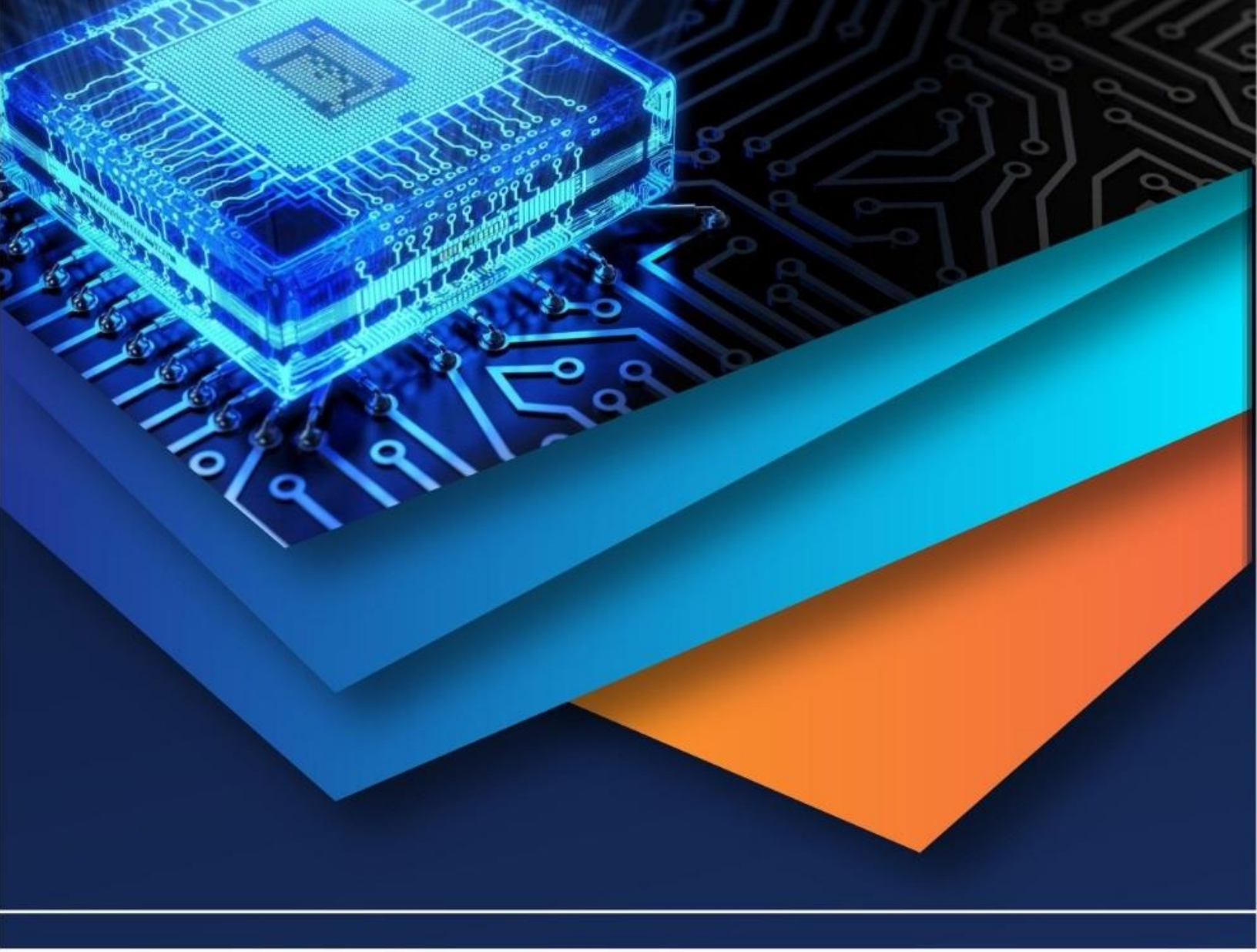
[6] J. Kaur, S. Lamba, and P. Saini, “Advanced Encryption Standard: Attacks and Current Research Trends,” in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021, Mar. 2021, pp. 112–116. doi: 10.1109/ICACITE51222.2021.9404716.

[7] “Difference Between DES and AES (with Comparison Chart) - Tech Differences.” https://techdifferences.com/difference-between-des-and-aes.html (accessed Mar. 28, 2022).

[8] “Difference between AES and DES ciphers - GeeksforGeeks.” https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/ (accessed Mar. 28, 2022).

[9] 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

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)