iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35404

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: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Document Organizing using Multiple Encryptions

Shivani V. Dhoke[1], Sunil R.Gupta[2]
[1, 2]*Department of Computer Science and Engineering, PRMIT&R Badnera*

Abstract: In this manuscript, "Pocket Certificates'' - a conventional document organizing with the capability of securely storing those documents is presented. Documents are something that provides information or can be a certification for someone or also can be a legal report. The theft of such important documents/certificates can interfere/hamper an individual or organization from performing their work efficiently and can also lead to loss of possessions. The solution is the use of a Double Encryption system based on an amalgamation of RSA, AES and MD5 standards. Use of enhanced security can be thought of as a compromise in reliability and smooth function of a system but to the process, there are some constraints to be set so that the Encryption/Decryption process does not hamper the usability. This paper takes account of such attributes and keeps a balance between all of them. There is also the use of other Hashing techniques like bycrypt securely storing user login details and use of passport middleware for unique user authentication requirements at each application stage. The paper consists of an overall web application for the secure archive to documents or important data.
Keywords: RSA, AES, MD5, Cryptography, Decryption, Encryption

I. INTRODUCTION

A. Overview

Multiple encryption is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. It is also known as cascade encryption, cascade ciphering, multiple encryption, and super encipherment. Super encryption refers to the outer-level encryption of a multiple encryption. Presently there are so many organization use the physical document. The use of physical document creates a huge overhead in terms of security. The Documents are something that provides information or can be a certification for someone or also can be a legal report. The theft of such important documents/certificates can interfere/hamper an individual or organization from performing their work efficiently and can also lead to loss of possessions. "Pocket Certificates[1]" - a conventional document archive with the capability of securely storing those documents is presented.

The solution is the use of a Double Encryption system. Use of enhanced security can be thought of as a compromise in reliability and smooth function of a system but to the process, there are some constraints to be set so that the Encryption/Decryption process does not hamper the usability. This dissertation takes account of such attributes and keeps a balance between all of them. There is also the use of other Hashing techniques like bycrypt securely storing user login details and use of passport middleware for unique user authentication requirements at each application stage. The dissertation consists of an overall web application for the secure archive to documents or important data.

Some cryptographers, like Matthew Green of Johns Hopkins University, say multiple encryption addresses a problem that mostly doesn't exist: Modern ciphers rarely get broken. You're far more likely to get hit by malware or an implementation bug than you are to suffer a catastrophic attack on AES. and in that quote lies the reason for multiple encryption, namely poor implementation. Using two different cryptomodules and keying processes from two different vendors requires both vendors' wares to be compromised for security to fail.

B. Motivation

Documents can be a official paper that gives information about something or that is used as proof of something or can be a certification for someone or also can be a legal report. The theft of such important documents can hamper an individual or organization from performing their work efficiently and can also lead to loss of possessions. So the basic motivation behind this dissertation is

1) To secure our data from hackers/attackers and understand different techniques to secure document.
2) It may allow banks to utilize resources in a highly flexible and efficient manner with the help of data analytics, data storage, and batch processing.
3) It serves as a transformative digital solution which offers unparalleled levels of security, agility, and scalability to the banking sector while boosting its capability to handle consumer data.

C. Problem Definition

In this manuscript, “Pocket Certificates" - a conventional document archive with the capability of securely storing those documents is presented. Documents are something that provides information or can be a certification for someone or also can be a legal report. The theft of such important documents/certificates can interfere/hamper an individual or organization from performing their work efficiently and can also lead to loss of possessions. To overcome this problem the solution is that the use of a Double Encryption system. Use of enhanced security can be thought of as a compromise in reliability and smooth function of a system but to the process, there are some constraints to be set so that the Encryption/Decryption process does not hamper the usability. This dissertation takes account of such attributes and keeps a balance between all of them.

D. Objectives

To solve the challenging problem of document security such as theft of documents following objectives are listed:

1) To prevent data loss from possible cyber-attack on sensitive documents
2) Explore multiple ways to achieve document encryption and decryption
3) Study different Compression and Encryption technique to achieve Data Safety
4) Understanding different techniques to achieve faster and secure ways of document archiving.

In section 1 introduces about Secure Document Archival and multiple Encryption Technique. Section 2 presents detailed literature review work in the field of Secure Document Archival and Multiple Encryption Technique. Section 3 describes Existing Systems and Architecture for Secure Document Archival. Section 4 Explore and Discusses detailed design for Secure Document Archival using different Encryption techniques. Finally the result is concluding in section 5.

II. LITERATURE REVIEW

A. Background

Document security is a highly sophisticated service for document storage that requires a secure, safe facility and provides individuals who have the expertise of handling, retrieving, and storing documents on behalf of other businesses/companies. Document security, defined in literal terms, is the maintenance of all of the essential documents stored, filed, backed up, processed, delivered, and eventually disposed of when no longer needed. As documents face major security threats, one must realize the importance of developing a backup and storage plan for documents. It is a much more complicated process than just choosing a storage platform that will provide you ample space. It involves profoundly understanding the security features, capacity, and ability to maintain a backup if the documents are lost. If the documents are lost, then document storage platform should have the ability to retrieve them quickly.

Many businesses hire companies that provide storage facilities instead of spending cash on renting/leasing more storage space. This storage space is a cost-effective method and provides sufficient document safety because the storage facility companies guarantee adequate security.

A cost-effective method used by many businesses for document storage is hiring companies that offer document storage services in the form of document storage and management platforms, instead of paying a lease for more space. Another primary reason that document storage should be a top priority for any business is document security.

Document security is a highly sophisticated service for document storage that requires a secure, safe facility and provides individuals who have the expertise of handling, retrieving, and storing documents on behalf of other businesses/companies. Although there are some mistakes related to document storage and management that should be avoided at all costs:

1) Documents that are not labeled or packaged in an organized manner are often tough to locate. Most facilities complete the task for businesses as they mostly provide their packaging, retrieval, and storage system.
2) One major factor that many businesses are concerned about is the security of document storage. Most documents stored online are not as safe as they are likely to fall prey to malicious attacks on the internet. Documents are easily accessible to third parties and can be hacked despite having security. Therefore, the lack of an effective encryption method can prove to be fatal for a business.
3) If not appropriately managed daily, document storage can get jumbled up, resulting in a troublesome and time-consuming retrieval process.

B. Secure Document Archiving

Document organizing [34] means putting information you no longer use regularly into secure storage for extended periods of time. It's a complex process to get right, and doing it wrong risks leaving yourself open to security breaches. Document archiving companies can manage your documents for you, reducing risks of mistakes and helping to improve your data protection. Document archiving is securely storing information you no longer use regularly.

The two options for how to archive documents are as follows:

1) Organizing documents on your own premises—this will take up valuable storage space and mean that you'll need to implement a proper archiving system so you can easily locate documents when you need them

2) Organizing documents with a document archiving company—a specialist company will collect your documents and store them in dedicated off-site premises. Depending on the service you choose, they will:

a) Organizing your documents and scan them and send them to you when requested

b) Organizing your documents and deliver individual hard copy documents to you when requested

c) Scan your paper documents before either archiving or destroying them

Organizing documents off-site can save valuable space on your premises and make retrieving documents much easier

C. Encryption and Encryption Techniques

1) *Encryption:* In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

2) *Encryption Techniques:* Cryptography is protecting the confidentiality and integrity of the information without being vulnerable to the attackers or threat. It is an encryption technique when ensure the data is only visible to the sender and recipient and no middle man can steal the data and snoop for information.

There are three most common types of cryptographic techniques in general. They are –

a) Symmetric key cryptography – Here the sender and receiver share a similar key and it can be used for both encryption and decryption.

b) Hash functions – There is no key used, rather a hash value is used to encrypt text, contents and passwords.

c) Public key cryptography – In this two different keys such as public key for encryption and private key for decryption is used. Only the private key is kept as secret.

3) *Encryption Tools and Techniques*

There are few tools available for encryption technique[33]. They include –

a) Triple DES – Replaces Data encryption standard(DES) algorithm, uses 3 individual keys with 56 bit.

b) RSA – Public encryption algorithm to protect the data over internet. It is an asymmetric key encryption algorithm which uses public and private key.

c) Blowfish – It splits the message into 64 bits and encrypts them, is used in certain payment gateways. It is fast, effective and flexible.

d) Twofish – Keys in this algorithm are 256 bits in length and it is a symmetric key encryption technique.

e) AES – Advanced encryption standard, trusted by many standard organizations. It can encrypt is 128 bit, 192 bit as well as 256-bit.

D. Methods

3DES is used to boost up the security aspect of the Project. The DES encryption process is run three times in 3DES, with three different keys:

a) The key one is used for the plaintext encryption.

b) This step uses decryption upon the encrypted data of step one, using key two.

c) To further encrypt the data, key three is used

How can the use of decryption in the second step boost security? This uses a separate key, the decryption process will not simply decrypt the data, it would be logically ironic, but decryption with a different key would only confuse the data more.

1) *DES:* The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). The algorithm takes the plain text in 64-bit blocks and converts them into cipher text using 48-bit keys. Since it's a symmetric-key algorithm, it employs the same key in both encrypting and decrypting the data. If it were an asymmetrical algorithm, it would use different keys for encryption and decryption. DES is based on the Feistel block cipher, called LUCIFER, developed in 1971 by IBM cryptography researcher Horst Feistel. DES uses 16 rounds of the Feistel structure, using a different key for each round. DES became the approved federal encryption standard in November 1976 and subsequently reaffirmed as the standard in 1983, 1988, and 1999. For the longest time, DES was the data encryption standard in information security. DES's dominance came to an end in 2002, when the Advanced Encryption Standard (AES) replaced the DES encryption algorthm as the accepted standard, following a public competition to find a replacement. The NIST officially withdrew FIPS 46-3 (the 1999 reaffirmation) in May 2005, although Triple DES (3DES), remains approved for sensitive government information through 2030. Triple DES is a symmetric key-block cipher which applies the DES cipher in triplicate. It encrypts with the first key (k1), decrypts using the second key (k2), then encrypts with the third key (k3). There is also a two-key variant, where k1 and k3 are the same keys. The NIST had to replace the DES algorithm because its 56-bit key lengths were too small, considering the increased processing power of newer computers. Encryption strength is related to the key size, and DES found itself a victim of the ongoing technological advances in computing. It reached a point where 56-bit was no longer good enough to handle the new challenges to encryption.

The algorithm process breaks down into the following steps:

a) The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
b) The initial permutation (IP) is then performed on the plain text.
c) Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
d) Each LPT and RPT goes through 16 rounds of the encryption process.
e) Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
f) The result of this process produces the desired 64-bit ciphertext.

The encryption process step (step 4, above) is further broken down into five stages:

a) Key transformation
b) Expansion permutation
c) S-Box permutation
d) P-Box permutation
e) XOR and swap

For decryption, we use the same algorithm, and we reverse the order of the 16 round keys.

➢ *DES Modes of Operation*

Data encryption experts using DES have five different modes of operation to choose from.

- Electronic Codebook (ECB). Each 64-bit block is encrypted and decrypted independently
- Cipher Block Chaining (CBC). Each 64-bit block depends on the previous one and uses an Initialization Vector (IV)
- Cipher Feedback (CFB). The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit
- Output Feedback (OFB). Much like CFB, except that the encryption algorithm input is the output from the preceding DES
- Counter (CTR). Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each subsequent block

2) *AES:* The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard.

a) How does AES work?: The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 258-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

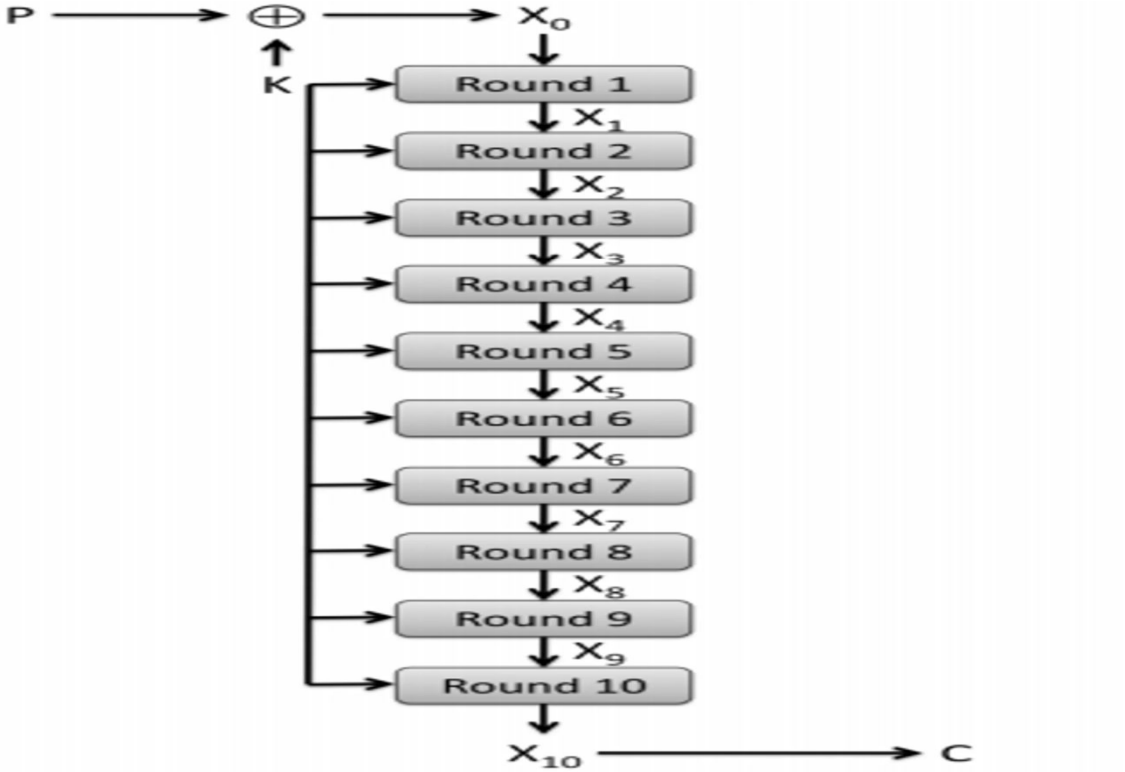


Fig 1 : Rounds to produce cipher text

b) Steps in each round

Each round in the algorithm consists of four steps.

- *Substitution of the Bytes:* In the first step, the bytes of the block text are substituted based on rules dictated by predefined S-boxes (short for substitution boxes).

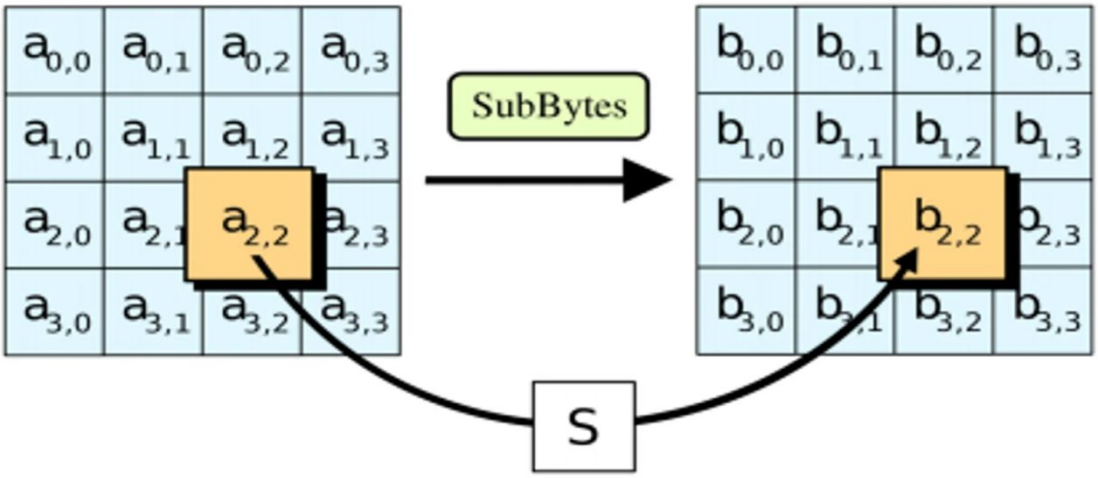


Fig 2 : first step of each round

- *Shifting the Rows:* Next comes the permutation step. In this step, all rows except the first are shifted by one, as shown below.

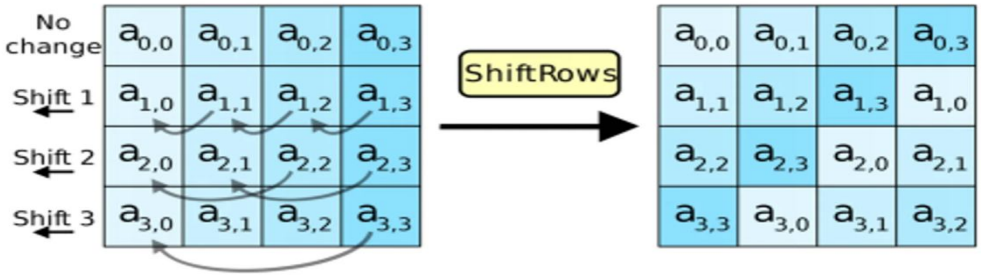


Fig.3 : second step of each round

- *Mixing the Columns:* In the third step, the Hill cipher is used to jumble up the message more by mixing the block's columns.

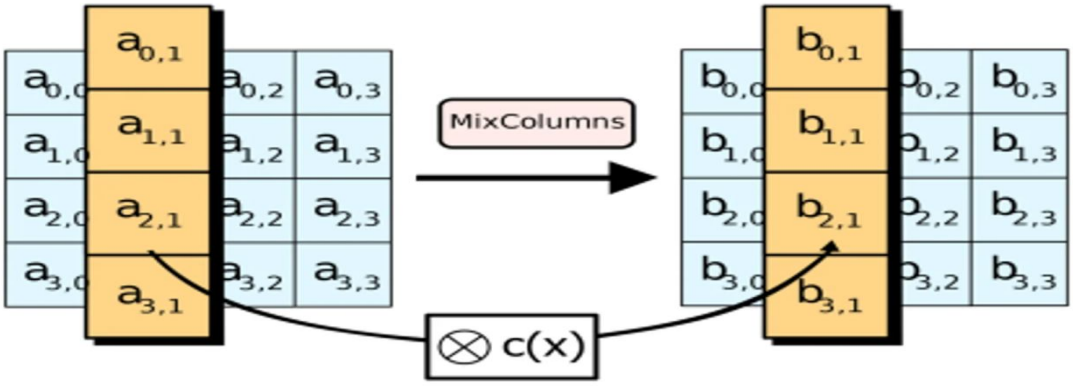


Fig 4 : Third step of each round

- Adding the Round Key: In the final step, the message is XORed with the respective round key.

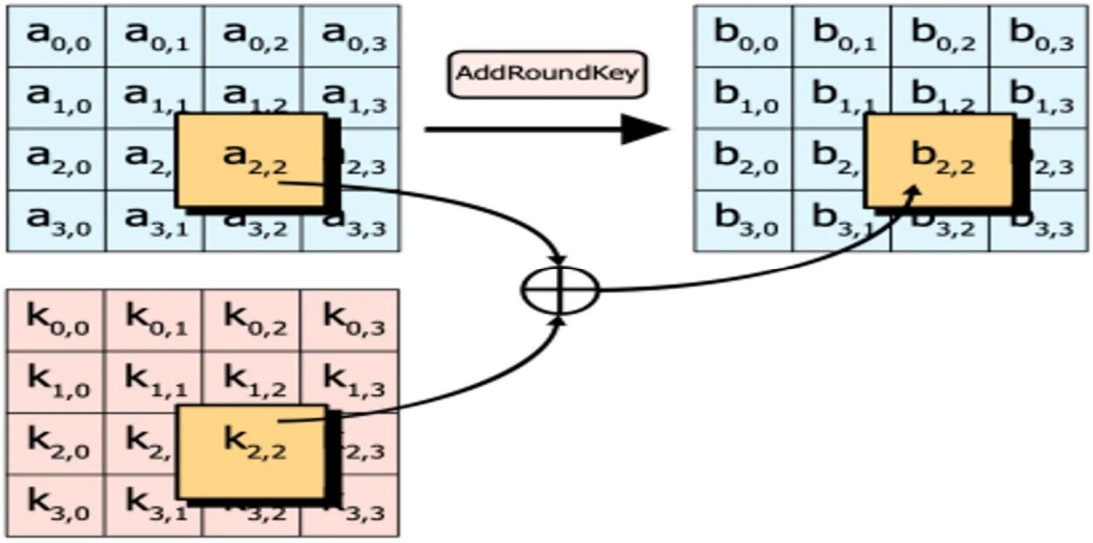


Fig 5 : Fourth step of each round

When done repeatedly, these steps ensure that the final ciphertext is secure.

3) *RSA:* RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997. In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers. The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used. RSA is a relatively slow algorithm. Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric key cryptography, which are then used for bulk encryption-decryption.
4) *Blowfish:* Blowfish is another algorithm that was designed to replace DES. This symmetric tool breaks messages into 64-bit blocks and encrypts them individually. Blowfish has established a reputation for speed, flexibility, and is unbreakable. It's in the public domain, so that makes it free, adding even more to its appeal. Blowfish is commonly found on e-commerce platforms, securing payments, and in password management tools.
5) *Twofish:* Twofish is Blowfish's successor. It's license-free, symmetric encryption that deciphers 128-bit data blocks. Additionally, Twofish always encrypts data in 16 rounds, no matter what the key size. Twofish is perfect for both software and hardware environments and is considered one of the fastest of its type. Many of today's file and folder encryption software solutions use this method.

E. Recent Research Trends

Design and implementation of encrypted and decrypted file system based on USBKey and hardware code [2] is based on the usage of USBKey for user authentication, use of the 3DES algorithm to encrypt files and an MD5 Hash to verify the integrity of that file. USBKey suggests the use of external hardware. Hu, G [3] shows a similar study of USBKey for user authentication, data encryption and digital signature. Their method addresses the approach of combining software and hardware, the hardware dedicated to the management of secret keys and the encryption of session keys and the software conducting the process of file encryption. Yandji, G.A., Hao, L.L., Youssouf, A.E. and Ehoussou, J [4] Aimed to bring the multifunction of MD5 and AES together. AES was used for encryption of files and MD5 to hash out the encrypted data and password. The authors aim to generate a hashed result that can circumvent the tricks of malicious operations carried out by eavesdroppers, by interfering in the encryption process with those components. [5] The author's main motive is to provide secure cloud storage. Use of a double layer encryption method to guarantee security in the cloud is being suggested via this paper. It is based on a popular cryptography algorithm RSA which is a relatively novel technique. In this proposed double layer of encryption schemes, the data will be extremely secure while protecting and sharing in cloud environments. This scheme not only makes full use of the great processing skill of cloud computing but also can efficiently ensure cloud data privacy and security.

The proposed system of Mary, J.S. and Usha, S. [6] is a web-based document management system to provide mobile access to authorized users on any device. To encrypt passwords in the database, MD5 is used in the system. Also, when any document is stored, a checksum is set. If any unknown user changes the contents of the document the checksum value is changed and the user will be able to tell if the document has tampered or not. In this system, the whole document is encrypted and then stored so there is less to none chance that the data will tamper.

[7] The encryption technique used here for data security is Multi-phase Data Encryption. Multi-phase encryption produces a complex number of steps for data encryption by performing the same procedure several times with different encryption keys in an established way. The ever-increasing sophistication of the data improves data transmission protection, which would be very difficult to decrypt. The proposed AES algorithm with hybrid approach will be an effective technique for providing strong security in message transmission by adding more complexity in AES to increase Confusion and Diffusion in Cipher text. It will protect message from Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack. Proposed system[8] will be an effective technique for the applications which are based on internet such as e-commerce online shopping, Stock Trading, Net Banking and Electronic bill payment and so on.

The research of Dr. AbulBashar[13] provides a secure and a cost effective way of off-loading for the mobile computing by integrating them advanced encryption standard and the whale optimization algorithm for the encryption and the decryption of the

information's offloaded respectively. This ensure the authentication for the information transmission to the appropriate person avoiding the circumstances of information misuse by the intruders and the attackers. The performance analysis of the proposed method evinces the competence of the AES-WOA in terms of security, cost and delay in the offloading against the existing methods
The research of Pondi Jyothirmai1 • Jennifer. S. Raj1 • S. Smys2[14] Wormhole and Black hole attack are main security threats that degrades the performance of routing protocol in Mobile Ad hoc Network. Its detection and isolation is the main factor of concern to improve network quality. Performance metrics such as packet delivery ratio, throughput, end–end delay, good put and routing overhead are analysed by varying the number of nodes and black hole nodes in the network. The throughput value of a network is reduced to 1030 kbps and below when black hole nodes are increasing and increased the throughput performance to 1810 kbps by isolating the black hole attack. End–end delay is increased by 16 s with black hole attack from 0.782 s without attack, after isolation of attack delay is reduced to 4.01 s. Packet delivery ratio is 98.392% without attack and decreased to 55.16% when the network is attacked by the attacker node after isolation it is increased to 83.08%. Routing overhead is 198.54kbps without attack in the network, with attack overhead is 252.36 kbps and increased to 302.46kbps after isolation. Therefore, the performance of the network is increased due to decrease in packet drop rate in the network and also multiple attackers can be detected. More than 80% of the performance of the network is increased after recovery and isolation of attacks in the wireless network. Future work implementation in the real time, by considering military fields, relief camps, hostile environments etc.
AES is a popular symmetric block cipher used by different commercialization sectors. But this algorithm is facing a number of cryptanalysis effects as they have seen in the literature review. Therefore, in this research [15] author have tried to solve the problem by incorporating the changes in key expansion module. Te highlight of this work is to apply randomness in the key generation. Moreover, as per their previous work using SRFG as a cryptographic function in AES has been proved beneficial. Te justification for the same has been already shown in the research. Te results show that RK-AES is having three times better confusion property and 53.7% better avalanche effect as compared to the original AES. The limitation of their present work is about the time taken by the modified key expansion module which is actually creating a trade-of between security and time. It is also known that both these two cannot be achieved simultaneously. Therefore, if they ignore the part of the time, their proposed RK-AES is efficient in all respects of cryptographic algorithms. Furthermore, being a symmetric key algorithm AES uses the single key for both encryption and decryption. In their present work, the round keys are stored separately as each round keys are generated randomly and are used for decryption accordingly. In their future work, they shall try to work on the trade-of and also about the storing process of round keys.
The idea of modularity-based community detection is to try to assign each vertex of the given network to a community such that it maximizes the modularity value of the network. Optimizing modularity is an NP-hard problem. [18] Exact algorithms that maximize modularity such as [19], [18], [20] can be used only for small networks.
For large-scale modularity optimization, heuristic algorithms are proposed. We basically focus on three well known algorithms, namely; CNM, Louvain and SLM. The first one is Clauset et al.'s [21] CNM algorithm. It is a greedy modularity maximization algorithm that searches for best community assignment for each node. The second one is referred as Louvain algorithm and proposed by Blondel et al. [22] in 2008. By considering each community as a single node, it further searches for new community merges after the local optimum satisfied using CNM. The last one is called as Smart Local Moving (SLM) algorithm that is proposed by Waltman and Jan van Eck in 2013.
Due to the dynamic features of many social networks [23], the need for detecting communities dynamically in the large networks is emerged in the latest years. There have been many community detection algorithms proposed in the literature to fulfil this need. Xu et al. divides the current research on community evolution into the following categories. Parameter estimation methods and probabilistic models have been proposed in the literature.
[24], [25] A methodology that tries to find an optimal cluster sequence by detecting a cluster structure at each timestamp that optimizes the incremental quality can be classified as evolutionary clustering. [26], [27] Furthermore, tracking algorithms based on similarity comparison have also been studied in order to be able to describe the change of communities on the time axis. [28], [29] Apart from these algorithms that are focused on the evolution procedures of communities, community detection in dynamic social networks aims to detect the optimal community structure at each timestamp.
For this purpose, incremental versions of both CNM and Louvain algorithm are proposed by Dinh et al.[30] and Aynaud et al. [31]. To the best of our knowledge, this is the first work considering the incremental version of Smart Local Moving algorithm in literature. their algorithm can be classified as the last mentioned category which aims to detect optimal community structure at each timestamp with minimum running time.

F. Summary and Discussion

Document Security is a significant issue faced by almost all businesses operating worldwide. When a company uploads its documents onto the internet through cloud storage devices and platforms, they are at an extremely high risk of falling prey to malicious viruses and dangerous hackers. When placed in a physical form, there is an extremely high chance that they can be lost or damaged due to consequences like fire or theft. Many businesses around the world have had to face difficult situations of data theft and security breaches, forcing them to pay a heavy price.

The solution is the use of a Double Encryption system based on an amalgamation of AES and 3DES standards. Use of enhanced security can be thought of as a compromise in reliability and smooth function of a system but to the process, there are some constraints to be set so that the Encryption/Decryption process does not hamper the usability.

III. SYSTEM ANALYSIS

A. Existing System

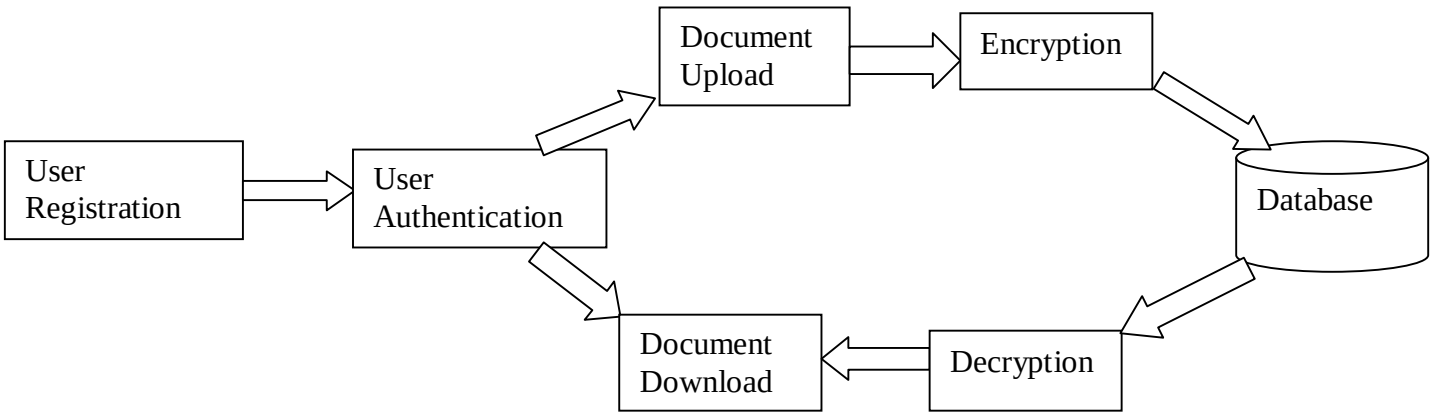


Fig 6. Architecture Diagram of Existing System

Above figure shows the architecture diagram of Existing system. In current situation there are so many organisation/sectors use the physical documents. The use of physical copies of documents creates huge overhead in terms of security, paper storage, manual audits, etc. incurring high cost and inconvenience. The work environment nowadays demands that proper security measures be taken when it comes to all forms of documentation – digital or otherwise. It is easy to heist documents from a conventional cabinet locker and anyone can theft document easily. Proper document organization combined with the use of cryptography tools will make sure that the sensitive data can stay secure.

The Pocket Certificates System is aimed for secure and unalterable storage of important documents. It also aims to check the fact if the user identity is true and not compromised, this achieved by the use of passport function for checking the authenticity of the user, and bycrypt function to store the password in a secure hashed/encrypted format.

The system is designed in such a way that it doesn't compromise on the fact that it must be reliable, usable and smooth while entertaining the security of the documents stored in the database. To implement the concept of document security this dissertation designed E-banking application which is used to stores details of customers like customer details, transaction details etc, and must be able to retrieve those documents whenever necessary. The main purpose to use multiple encryption layers was to hold the confidentiality, authenticity, and integrity of the user's data maintaining the CIA triad along with the authenticity of the system. Using multiple layers of encryption prevents most of the attacks like brute force and uses of other tools to breach the system's security.

B. Existing Technology

Client side and server side requirements

Client side and server side[9] are web development terms that describe where application code runs. Web developers will also refer to this distinction as the frontend vs. the backend, although client-side/server-side and frontend/backend aren't quite the same. In a server less architecture, the server less vendor hosts and assigns resources to all server-side processes and the processes scale up as application usage increases.

1) *Client-server Model:* Much of the Internet is based on the client-server model. In this model, user devices communicate via a network with centrally located servers to get the data they need, instead of communicating with each other. End user devices such as laptops, smartphones, and desktop computers are considered to be 'clients' of the servers, as if they were customers obtaining services from a company. Client devices send requests to the servers for webpages or applications, and the servers serve up responses. The client-server model is used because servers are typically more powerful and more reliable than user devices. They also are constantly maintained and kept in controlled environments to make sure they're always on and available; although individual servers may go down, there are usually other servers backing them up. Meanwhile, users can turn their devices on and off, or lose or break their devices, and it should not impact Internet service for other users. Servers can serve multiple client devices at once, and each client device sends requests to multiple servers in the course of accessing and browsing the Internet. Multiple clients and servers interact: Suppose a user is browsing the Internet and types 'netflix.com' into their browser bar. These results in a request to DNS servers for the IP address of netflix.com, and the DNS servers respond to this request by serving the IP address to the browser. Next, the user's browser makes a request to Netflix servers (using the IP address) for the content that appears on the page, such as the movie thumbnail images, the Netflix logo, and the search bar. Netflix servers deliver this to the browser, and the browser loads the page on the client device
2) Client side of Application: In web development, 'client side' refers to everything in a web application that is displayed or takes place on the client (end user device). This includes what the user sees, such as text, images, and the rest of the UI, along with any actions that an application performs within the user's browser. Markup languages like HTML and CSS are interpreted by the browser on the client side. In addition, many contemporary developers are including client-side processes in their application architecture and moving away from doing everything on the server side; business logic for dynamic webpages*, for instance, usually runs client side in a modern web application. Client-side processes are almost always written in JavaScript. In the netflix.com example above, the HTML, CSS, and JavaScript that dictate how the Netflix main page appears to the user are interpreted by the browser on the client side. The page can also respond to 'events': For instance, if the user's mouse hovers over one of the movie thumbnail images, the image expands and adjacent thumbnails move slightly to one side to make room for the larger image. This is an example of a client-side process; the code within the webpage itself responds to the user's mouse and initiates this action without communicating with the server. The client side is also known as the frontend, although these two terms do not mean precisely the same thing. Client-side refers solely to the location where processes run, while frontend refers to the kinds of processes that run client-side. A dynamic webpage is a webpage that does not display the same content for all users and changes based on user input. The Facebook homepage is a dynamic page; the Facebook login page is for the most part static.
3) Server side of Application: Much like with client side, 'server side' means everything that happens on the server, instead of on the client. In the past, nearly all business logic ran on the server side, and this included rendering dynamic webpages, interacting with databases, identity authentication, and push notifications. The problem with hosting all of these processes on the server side is that each request involving one of them has to travel all the way from the client to the server, every time. This introduces a great deal of latency. For this reason, contemporary applications run more code on the client side; one use case is rendering dynamic webpages in real time by running scripts within the browser that make changes to the content a user sees. Like with 'frontend' and 'client-side,' backend is also a term for the processes that take place on the server, although backend only refers to the types of processes and server-side refers to the location where processes run. Difference between Server Side Scripting and Client Side Scripting
4) *Client side Scripting:* Web browsers execute client side scripting. It is use when browsers has all code. Source code used to transfer from web server to user’s computer over internet and run directly on browsers. It is also used for validations and functionality for user events. It allows for more interactivity. It usually performs several actions without going to user. It cannot be basically used to connect to databases on web server. These scripts cannot access file system that resides at web browser. Pages are altered on basis of users choice. It can also used to create “cookies” that store data on user’s computer.

5) *Server Side Scripting:* Web servers are used to execute server side scripting. They are basically used to create dynamic pages. It can also access the file system residing at web server. Server-side environment that runs on a scripting language is a web-server. Scripts can be written in any of a number of server-side scripting language available. It is used to retrieve and generate content for dynamic pages. It is used to require to download plugins. In this load times are generally faster than client-side scripting. When you need to store and retrieve information a database will be used to contain data. It can use huge resources of server. It reduces client-side computation overhead. Server sends pages to request of user/client.

C. Hardware and Software Requirements -

1) Minimum Hardware Requirement

a) System :Core i3 1.80 GHz Processor
b) Hard Disk: 500 GB
c) Ram: 4 GB.

2) Software Requirement

a) Operating System : Windows 7
b) Technology Used: PHP
c) Database Used : MySQL

IV. SYSTEM DESIGN

A. Proposed System Architecture

The proposed system is a web-based document management system to provide mobile access to authorized users on any device. In the system passwords are encrypted in the database,. Also, when any document is stored, a checksum is set. If any unknown user changes the contents of the document the checksum value is changed and the user will be able to tell if the document has tampered or not. In this system, the whole document is encrypted and then stored so there is less to none chance that the data will tamper.
This research developed a system that can securely store user documents and keep those documents out of reach of unauthorized people and must be able to retrieve those documents whenever necessary. The subsequent diagrams shall depict the workflow of the framework that has proposed.

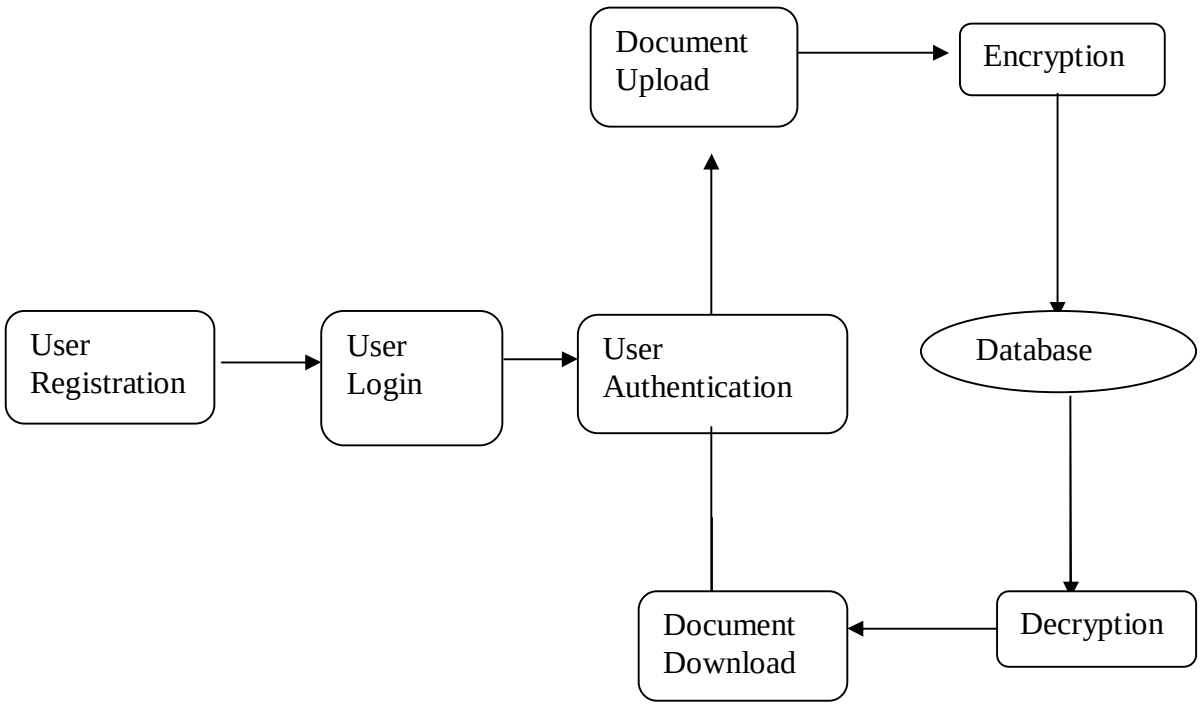


Fig 7: System Flow

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

In this instance, as developers, developed a system that can securely store user documents and keep those documents out of reach of unauthorized people and must be able to retrieve those documents whenever necessary. The subsequent diagrams shall depict the workflow of the framework that has proposed. When a user enters the site, they are greeted with a login page. New users are required to create a new account whereas returning users are required to enter their credentials to proceed. At Login, as soon as the user credentials are verified, the user will be forward authenticated to Dashboard. This is where the user can choose the File Upload action to securely upload the documents. While uploading the documents the user must specify a name for the document, this name shall be referenced later for downloading the specific document. As the user clicks on the submit button the document is passed through the encryption process and stored in MySQL database. At Dashboard the list of documents present in the user database is presented, where the user will have a download option in front of the specific document. When the user opts to download the required document the encrypted binary data of that document is fetched and passed through the decryption process and then retrieved by the user.

B. Proposed System Design

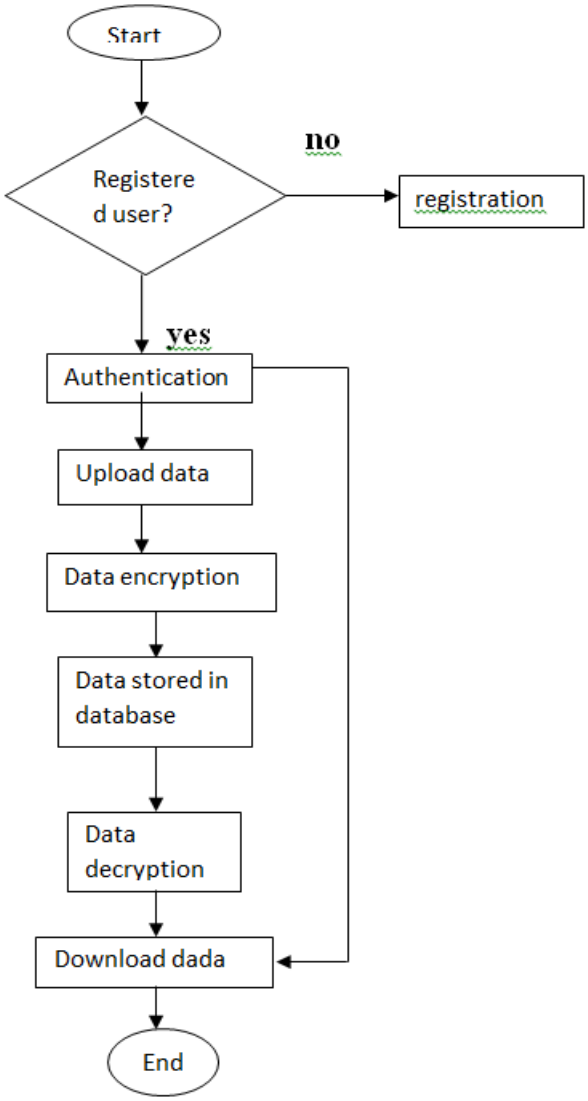


Fig 8: Flowchart of Existing System

The aim of our existing system is to can securely store user documents and keep those documents out of reach of unauthorized people. When user enter a system, they are addressed with home page. If there is a new user to the system, then they have do the registration by creating new account. After that At Authentication, as soon as the user credentials are verified, the user will be forward authenticated to Dashboard. This is where the user can choose the File Upload action to securely upload the documents. While uploading the documents the user must specify a name for the document, this name shall be referenced later for downloading the specific document. After that the document is passed through the encryption process and stored in MySQL database. At Dashboard the list of documents present in the user database is presented, where the user will have a download option in front of the specific document. When the user opts to download the required document the encrypted binary data of that document is fetched and passed through the decryption process and then retrieved by the user.

Use case Diagram

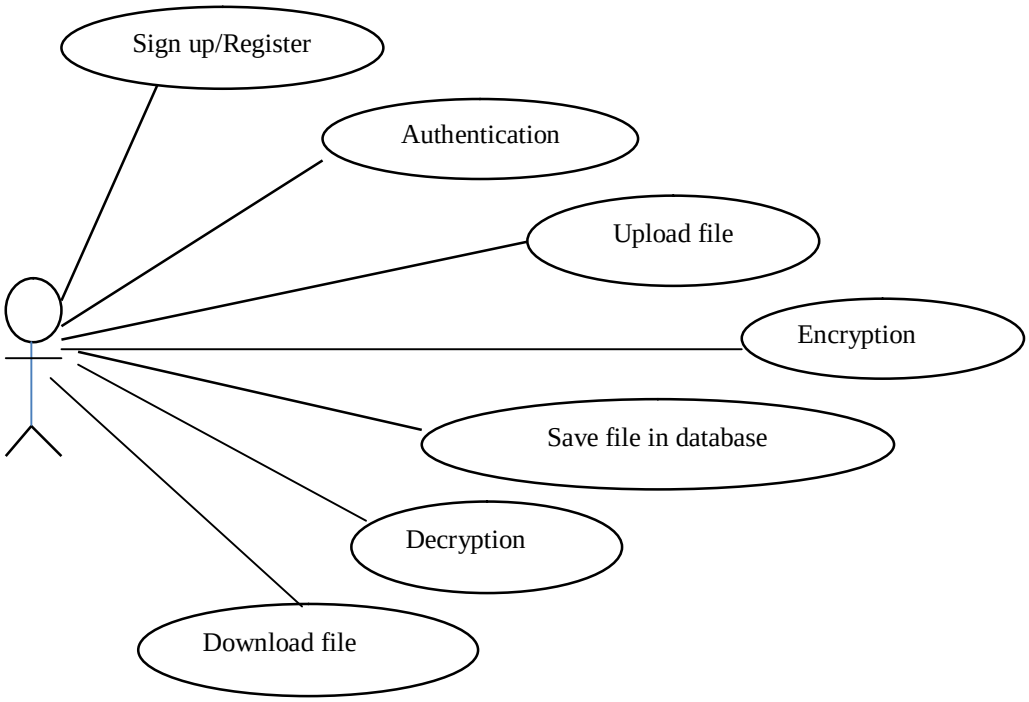


Fig 9: Use Case Diagram of System

C. Proposed Algorithm

1) RSA Algorithm: RSA (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm i.e., public and private key used here. The acronym RSA is made from the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997. As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone. Public key of user A is used for encryption, we have to use the private key of same user for decryption.

The following illustration highlights how asymmetric cryptography works:

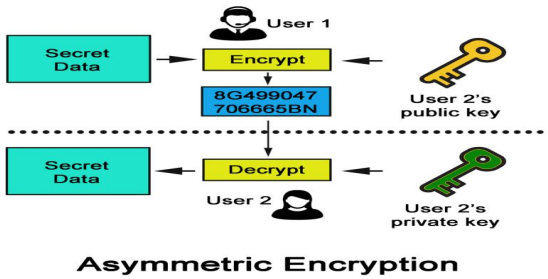


Fig 10: Asymmetric Encryption

2) How it Works

The following steps highlight how it works:

a) Generating the Keys

- Select two large prime numbers, x*x* and y*y*. The prime numbers need to be large so that they will be difficult for someone to figure out.
- Calculate n = x * y*n*=*x*∗*y*.
- Calculate the *totient* function; \phi(n) = (x-1)(y-1)$\phi(n)$=(*x*−1)(*y*−1).
- Select an integer e*e*, such that e*e* is *co-prime* to \phi(n)$\phi(n)$ and 1 < e < \phi(n)1<*e*<$\phi(n)$. The pair of numbers (n,e)(*n*,*e*) makes up the public key.

b) Encryption

Given a plaintext PP, represented as a number, the ciphertext CC is calculated as:
C = P^{e}C=Pemodmodnn.

c) Decryption

Using the private key (n,d)(n,d), the plaintext can be found using:
P = C^{d}P=Cd modmodnn.

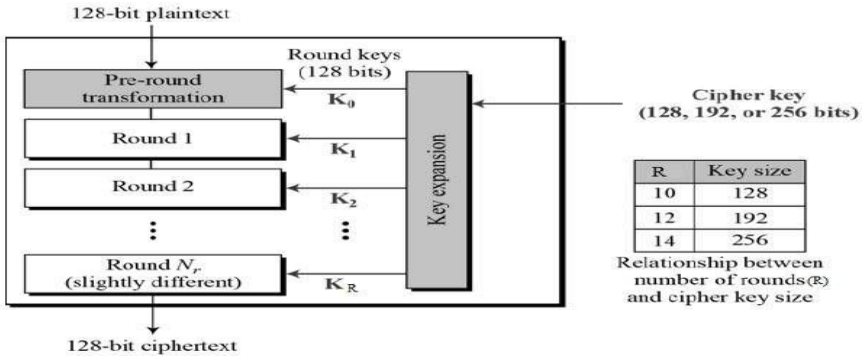
3) AES Algorithm: The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

a) Symmetric key symmetric block cipher
b) 128-bit data, 128/192/256-bit keys
c) Stronger and faster than Triple-DES
d) Provide full specification and design details
e) Software implementable in C and Java

4) Operation of AES: AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −



R	Key size
10	128
12	192
14	256

Fig 11: AES Structure

5) *Encryption Process:* Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –

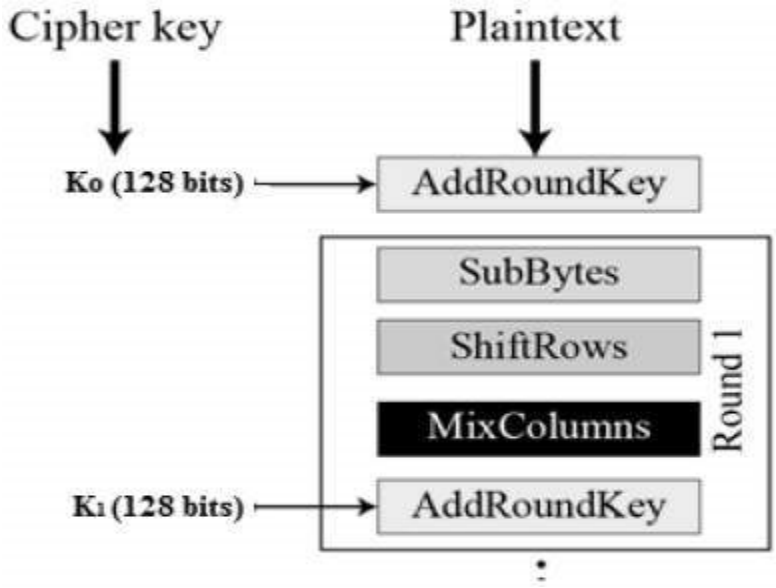


Fig 12 : First Round Process

6) *Byte Substitution (SubBytes):* The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.
7) *Shift Rows:* Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

a) First row is not shifted.
b) Second row is shifted one (byte) position to the left.
c) Third row is shifted two positions to the left.
d) Fourth row is shifted three positions to the left.
e) The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

8) *Mix Columns:* Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.
9) *Add Round Key:* The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.
10) *Decryption Process:* The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

a) Add round key
b) Mix columns
c) Shift rows
d) Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

11) *AES Analysis:* In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

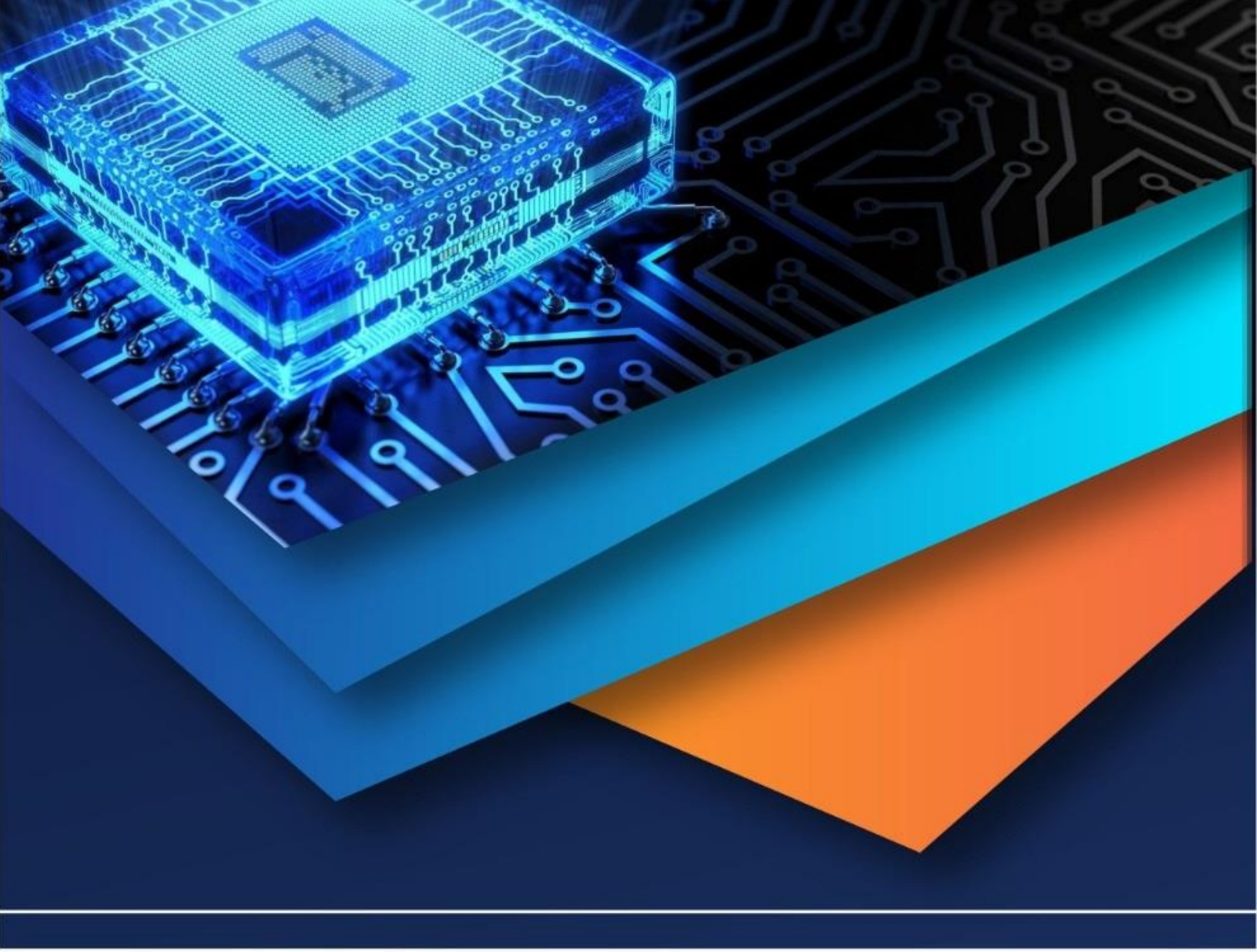
V. CONCLUSION

Document Security is a significant issue faced by almost all businesses operating worldwide. When a company uploads its documents onto the internet through cloud storage devices and platforms, they are at an extremely high risk of falling prey to malicious viruses and dangerous hackers. To overcome this problem, a dual encrypted system for E-banking application is proposed that stores details of customers. The main purpose to use multiple encryption layers was to hold the confidentiality, authenticity, and integrity of the user's data maintaining the CIA triad along with the authenticity of the system. Using multiple layers of encryption prevents most of the attacks like brute force and uses of other tools to breach the system's security. While multiple encryptions may slow down the system's performance but it may decelerate assailants, who at the very least would require substantially more storage to utilize comparative lists on more than one encryption stage.

REFERENCES

[1] DevavratAgnihotri, DevavratAgnihotri, DhanashreeDarekar, ChinmayGadkari, Asst. Prof. SagarJaikar, Asst. Prof. Mohandas Pawar, "A Secure Document Archive Implemented using Multiple Encryption," Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020)
[2] Wu, K., Zhang, Y., Cui, W. and Jiang, T., 2017, May. Design and implementation of encrypted and decrypted file system based on USBKey and hardware code.In AIP Conference Proceedings (Vol. 1839, No. 1, p. 020215).AIP Publishing LLC.
[3] Hu, G., 2010, April. Study of file encryption and decryption system using security key.In 2010 2nd International Conference on Computer Engineering and Technology (Vol. 7, pp. V7-121).IEEE.
[4] Yandji, G.A., Hao, L.L., Youssouf, A.E. and Ehoussou, J., 2011, May. Research on a normal file encryption and decryption.In 2011 International Conference on Computer and Management (CAMAN) (pp. 1-4).IEEE.
[5] Usha, D.D. and Subbbulakshmi, M., 2018. Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud.International Journal of Scientific & Engineering Research, 9(5).
[6] Mary, J.S. and Usha, S., 2015, November. Web based document management systems in life science organization. In 2015 Online International Conference on Green Engineering and Technologies (ICGET) (pp. 1-3).IEEE.
[7] Gupta, H. and Sharma, V.K., 2013. Multiphase encryption: A new concept in modern cryptography. International Journal of Computer Theory and Engineering, 5(4), p.638.
[8] D'souza, F.J. and Panchal, D., 2017, May. Advanced encryption standard (AES) security enhancement using hybrid approach.In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 647-652).IEEE.
[9] Paar, C. and Pelzl, J., 2009. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.
[10] Mardan, A., 2018. Using Express.js to create Node.js web apps. In Practical Node.js (pp. 51-87).Apress, Berkeley, CA.
[11] Gackenheimer, C., 2013. Implementing security and cryptography.In Node.js Recipes (pp. 133-160).Apress, Berkeley, CA.
[12] Mardan, A., 2018. Security and Auth in Node.js.In Practical Node.js (pp. 205-237).Apress, Berkeley, CA.
[13] Bashar, A., 2019. SECURE AND COST EFFICIENT IMPLEMENTATION OF THE MOBILE COMPUTING USING OFFLOADING TECHNIQUE. Journal of Information Technology, 1(01), pp.48-57.
[14] Jyothirmai, P., Raj, J.S. and Smys, S., 2017. Secured self organizing network architecture in wireless personal networks.Wireless Personal Communications, 96(4), pp.5603-5620.
[15] Saha, R., Geetha, G., Kumar, G. and Kim, T.H., 2018. RK-AES: an improved version of AES using a new key generation process with random keys. Security and Communication Networks, 2018.
[16] Indrayani, R., Ferdiansyah, P. and Satria, D.A., 2019, July. Effectiveness comparison of the AES and 3DES cryptography methods on email text messages.In 2019 International Conference on Information and Communications Technology (ICOIACT) (pp. 66-69).IEEE.
[17] Aleisa, N., 2015. A Comparison of the 3DES and AES Encryption Standards.International Journal of Security and Its Applications, 9(7), pp.241-246.
[18] U. Brandes, D. Delling, M. Gaertler, R. Goerke, M. Hoefer, Z. Nikoloski, and D. Wagner, "On modularity clustering," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 2, pp. 172– 188, 2008.
[19] D. Aloise, S. Cafieri, G. Caporossi, P. Hansen, L. Liberti, and S. Perron, "Column generation algorithms for exact modularity maximization in networks," Physical Review E, vol. 82, no. 4, article, pp. –, jan 2010
[20] G. Xu, S. Tsoka, and L. G. Papageorgiou, "Finding community structures in complex networks using mixed integer optimisation," The European Physical Journal B, vol. 60, no. 2, pp. 231–239, 2007. [Online]. Available: http://dx.doi.org/10.1140/epjb/e2007-00331-0
[21] A. Clauset, M. E. J. Newman, and C. Moore, "Finding community structure in very large networks," Phys. Rev. E, vol. 70, p. 066111, Dec 2004. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevE.70.066111
[22] V. Blondel, J. Guillaume, R. Lambiotte, and E. Mech, "Fast unfolding of communities in large networks," J. Stat. Mech, p. P10008, 2008.
[23] P. Holme and J. Saramaki, "Temporal networks," ¨ Physics Reports, vol. 519, no. 3, pp. 97–125, 2012.
[24] T. Yang, Y. Chi, S. Zhu, Y. Gong, and R. Jin, "Detecting communities and their evolutions in dynamic social networks - a bayesianapproach."Machine Learning, vol. 82, no. 2, pp. 157–189, 2011
[25] X. Tang and C. C. Yang, "Dynamic community detection with temporal dirichlet process." in SocialCom/PASSAT. IEEE, 2011, pp. 603–608.
[26] D. Chakrabarti, R. Kumar, and A. Tomkins, "Evolutionary clustering," in Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, ser. KDD '06. New York, NY, USA: ACM, 2006, pp. 554–560. [Online]. Available: http://doi.acm.org/10.1145/1150402.1150467
[27] M.-S. Kim and J. Han, "A particle-and-density based evolutionary clustering method for dynamic networks."PVLDB, vol. 2, no. 1, pp. 622–633, 2009.
[28] D. Greene, D. Doyle, and P. Cunningham, "Tracking the evolution of communities in dynamic social networks." in ASONAM, N. Memon and R. Alhajj, Eds. IEEE Computer Society, 2010, pp. 176–183.

[29] P. Brodka, S. Saganowski, and P. Kazienko, "Group evolution discovery in social networks," in Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on, 2011, pp. 247– 253.
[30] T. Dinh, Y. Xuan, and M. Thai, "Towards social-aware routing in dynamic communication networks," in Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International, Dec 2009, pp. 161–168.
[31] T. Aynaud and J.-L. Guillaume, "Static community detection algorithms for evolving networks," in Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on, May 2010, pp. 513–519.
[32] DevavratAgnihotri, Saad Ahmed, DhanashreeDarekar, ChinmayGadkari, Asst. Prof. SagarJaikar, Asst. Prof. Mohandas Pawar, "A Secure Document Archive Implemented using Multiple Encryption," Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020), November-2020,IEEE, pp. 765-770.
[33] https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/encryption-techniques/
[34] https://www.russellrichardson.co.uk/advice/3/complete-guide-document-archiving-services



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY