*International Journal of Research in Advent Technology, Vol.7, No.6S, June 2019*
*E-ISSN: 2321-9637*
*Available online at www.ijrat.org*

# CODOC: A Future of Documentation

**Ayush Sharma, Abhinav Raj, Deepti Singh, Swati Kumari, Dr. T N Anitha**

**Abstract—**Advancement of technology caters men comfort and convenience. New technologies are changing the world but there are few things which are still used as the way they were being used since the day they were invented. Paper is the most important medium to store data is still used in the same way. New technologies comes with new responsibilities, and now a days everyone is concerned about security of their data. Cryptography is the necessity now a days, advanced encryption standard (AES) being the most feasible algorithm for encryption and decryption, and it's best to use for securing data over open network or on a standalone device. Cipher and inverse cipher are the two components generated from advanced encryption standard. Crypted Organization of Document (CODOC) is the solution for all of these problems.

**IndexTerms**— AES, Encryption, Decryption, CODOC.

## I. INTRODUCTION

The most important thing which we do in our life is the documentation and it is generally done by using paper. Now documentation is the process should be digitalized for more security and the ease of the individual.The simplicity ofdocument storage for every society is very important. In traditional methods, documentation isdone by exchanging physical paper.Conventionally paper has some drawbacks like there are chances of wear and tear, with time quality of paper starts degrading or some time we can't find it when it is required and some more problems. creating an independent method important. That way, the documents of the customer should be kept virtually. A solution would be to replace the physical collection of paper with a digital wallet integrated into an existing mobile device like a smartphone. Crypted Organization of Document (CODOC) is the solution for all our paper problems. CODOC is the digital wallet for all digital form of our paper. A digital document wallet allows users to make electronic commercial storage swiftly and securely. Its functions are similar to a physical wallet. A digital document wallet has both a software and information component. The software provides security and encryption for personal information and for the actual storage.Typically, digital documents wallets are stored on the client-side and are easily compatible with most e-commerce storage. A server-side digital wallet, known as thin wallet, is the one that an organization creates for you and maintains on its servers. When the customer needs to perform any kind of work on their documents, the value of virtual storage should be updated. Digital storage can be placed on hardware chip or stored as software data.Each of these methods has its own advantages and disadvantages.

Cryptography is the most popular technique for securing data from attackers by encryption and decryption [8]. Encryption is the process of converting data into a from which can be accessed by only authorized parties but not by those who are not authorized. This converted form is known as cipher text and original data is known as plain text. Similarly, decryption is the process of getting plain text from cipher text. Integrity, authentication, nonrepudiation and confidentiality is the key features provided by modern cryptography techniques [9].

**Manuscript revised May 13, 2019 and published on June 5, 2019**
***Ayush Sharma**, Dept. Computer Science and Engineering, SJC Institute of Technology, Chickballapur, Karnataka, India*
***Abhinav Raj**, , Dept. Computer Science and Engineering, SJC Institute of Technology, Chickballapur, Karnataka, India*
***Deepti Singh**, , Dept. Computer Science and Engineering, SJC Institute of Technology, Chickballapur, Karnataka, India*
***Swati Kumari**, , Dept. Computer Science and Engineering, SJC Institute of Technology, Chickballapur, Karnataka, India*
***Dr. T N Anitha**, Professor and HOD , Dept. Computer Science and Engineering, SJC Institute of Technology, Chickballapur, Karnataka, India*

## II. RELATED WORK

**Problem Statement**

Solution for some of the main key research related issues is mentioned in this paper:

- How the actors will change their roles and responsibilities from physical world to digital world?
- How these actors are involved in creating new ecosystem?
- What are the challenges these actors are going to faced in the involvement of mobile digital services?

This paper will describe the architecture based on which mobile wallet service will be build on and will draw the conclusion based on some factors but they are not limited to only current smartphone technology or encryption standards.

**Digital wallet and its uses**

The motive behind creating this paper is to give an idea of how document can be digitalized. As we all know that every year more than 5 billion pages are printed only for magazines [5]. And now you just imagine how many trees are killed. Just to have a clear idea, as per research shows around 2 million trees are killed every year to make papers. And if you want to make paper whiter then you need to use bleach. The more bleach you use the whiter paper is [5]

As the word wallet says, it is nothing but the small item which can be used for storing small items like money, key, card etc. Similarly, digital wallet is a software which is used for storing the items in their digital form. A digital wallet can have a soft copy of a license which will be acting as a pass, it



doi: 10.32622/ijrat.76S201927

can also store information such as health information which can be helpful in case of emergency[6]

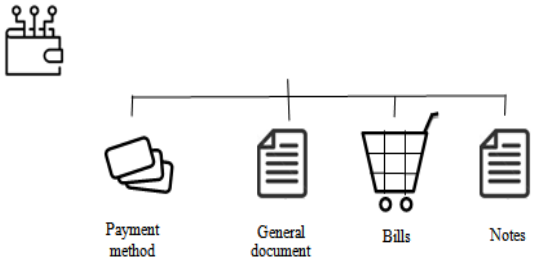


Fig 1: Digital Wallet and its uses

**Significance and relevance of work**

Studies shows that Advanced Encryption Standard (AES) is the most suitable algorithm for getting best performing encrypted and decrypted data when compared with all other secret key algorithm [4]. Digital India campaign is one of the inspiration among all inspirations behind this paper

## III. METHODLOGY

**CODOC** is the best alternative for physical documentation. Mobile wallets are essentially digital form of old school style of lockers used for storing important documents with safety. While we generally require different wallets for different kinds of items. Digital wallet systems and digital wallet devices are key requirements of digital wallet. The Advanced Encryption Standard (AES) algorithm is most preferable algorithm to use instead of Data Encryption Standard (DES). Its best to use a block cipher of size 256 bits, whereas 128 bits and 192 bits are two more size of block cipher. Data AES can be transferred and received in a very secure way. Data in AES 256 is so secure that, it cannot be attacked by any clone attacker [2].

**Proposed Architecture**

The proposed architecture for CODOC consists of actors and they are referred as user_1, user_2, authorization server, connecting server. The authorization server, connecting server and user_2 are having the following private and public key: ( $PK_{au}$, $SK_{au}$), ( $PK_{ps}$, $SK_{ps}$), ( $PK_{u2}$, $SK_{u2}$ ) respectively.

All the steps are described below and its diagrammatic representation is also given for better understanding.

- The user_1 send { [AC, PW, IMEI, TS], LO, LA, SN } to the authorization server: the authorization application provides an interface that allows user_2 to input the account username and password and then sends a request containing this information to the authorization server.
- The authorization server sends { [AC, SN, TS], [AC, SN, TS]} to the connecting-service server: the server provides the service of verifying if users have authorization to use the 2D barcode certificate service.
- The connecting-service server sends { [AN], [AC, AN, Limit], Limit} to the authorization server and the user: after access permission is granted, the server executes the service of generating a connection certificate and responds by providing the user_2's identification data to the user.
- The one user sends {2D_Barcode_Gen, [AN], [AC, AN, Limit], Limit)} to other user: theauthorization application calls a 2D barcode encoder to generate a 2D barcode that acts as a ownership certificate.
- The other user sends {[AN]} to the connection server: the other user decrypts and verifies the data stored in the 2D barcode, and then the checkout system sends this authorization number to the connection-service server to indicate that the authorization number was used.

Where,

- AC: user_1's account username,
- PW: user_2's account password,
- IMEI: International Mobile Equipment Identity,
- TS: time stamp,
- LO: longitude of the position of the mobile device,
- LA: latitude of the position of the mobile device,
- SN: service name,
- AN: authorization number,
- Limit: amount limit of a single transaction
- $E_{PK\_au}$ : encrypt using public key of authorization server.
- $E_{PK\_cs}$ :encrypt using the public key of the connecting server.
- $SigN_{SK\_au}$ :sign using the private key of the authorization server.
- $SigN_{SK\_cs}$ :sign using the private key of the connecting server.
- $SigN_{SK\_u2}$ :sign using the private key of the user_2.

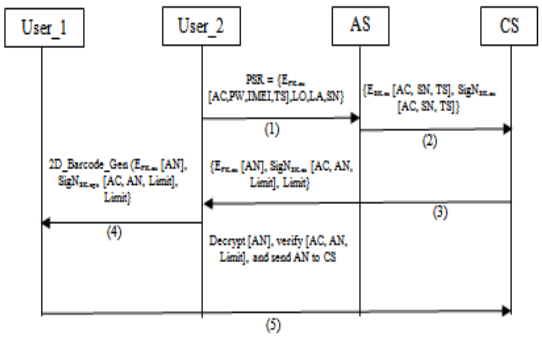


Fig 2: Architectural design

**User Authentication**

Now a days for every application need users signing and verification and this is important also. With the increase in number of user and increase in numerous types of



doi: 10.32622/ijrat.76S201927

application, the possibilities of hacking are also increasing simultaneously. AES [4] is the best algorithm for encryption of data. User signing process consist of 4 steps. And these 4 steps are shown in figure 3. Where in first step users data is converted into their hash function and it is further encrypted using signers private key (which is unique for each user) forming a digital signature of a user. Then this digital signature is combined with digital certificate, and then combination of data with digital certificate forms a digital form of data

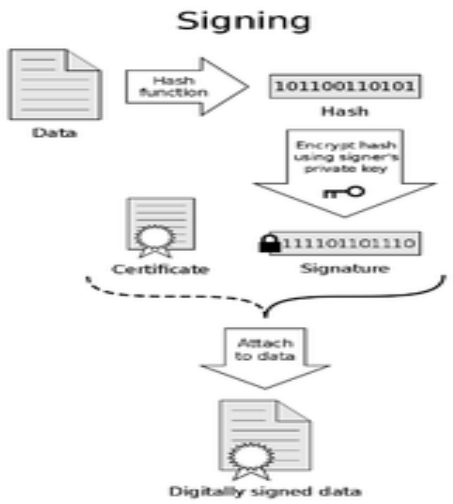


Fig 3: User Signing

As we know that user signing is important similarly user verification is also important. Figure 4 shown below show how this user verification happens, and this process consist of 3 steps. Initially after getting digitally signed data from another user or server, system seperates data and digital signature key. Then data is converteed into its hask function, similarly digital signature key is decrypted using signer's public key. And then its value is compared with has function, if both the values are same, then that digital document will be accepted by the reciever and if both values are different then this digital document will be rejected.

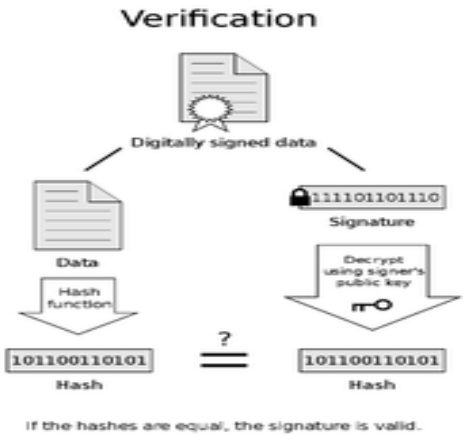


Fig 4: User Verification

**Digital Wallet Ecosystem**

Understanding the requirements of user to make the digital wallet, loyalty and digital wallet universal realities leads to better development of application.

Initially, we need to know what are the different kinds of paper in market like newspaper, magazines, different types of bills, normal papers, receipt and many more. And then we need to know which kind of papers are compatible with this paper. Some time we don't need internet connection and some time we may need for using digital wallets [1]. It is better to test this digital wallet in its development phase with agile methodology by using open source test cases and automation framework. Pragmatic test management is the key in adopting dynamic and agile nature, which indeed help in improving the efficiency of digital wallet

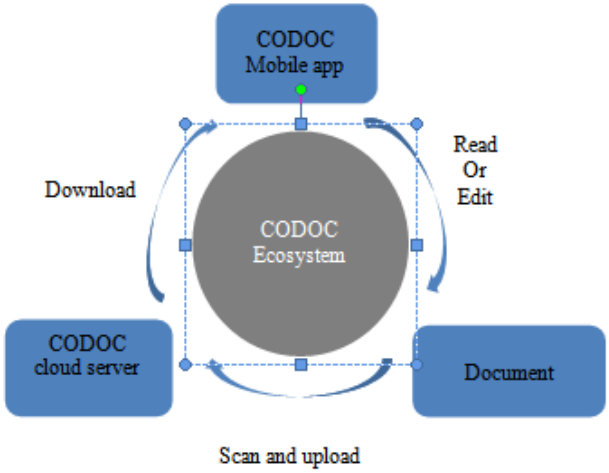


Fig 5: Digital Wallet Ecosystem

CODOC majorly consist of three main components that is mobile application, physical document, a cloud server. Figure 5 shows the ecosystem of digital wallet. Mobile application is the device with the help of which user can access their documents. Physical documents could be any kind of documents which are compatible with digital wallet. And a separate cloud dedicated cloud server is used to store users documents so that digital wallet application will be light in its architecture

**Encryption Technology**

Digital wallet has some constraints, which we need to keep in our mind while developing it, and they are like:

- Its application should be enough secure.
- As per studies, the approaches should meet the confidentiality, authentication, simplicity of security issue. Therefore, the proposed approaches is effective and practical for safe data transmission among users.

There are few techniques which we can use to encrypt our document so that we can keep it secure as shown in figure 6 to Figure 8. As the methods shown below are methods encryption and they are not easy for any third to decrypt. It's better to create a QR code [3] of document file if user want reduce the memory size consumed by document store in digital wallet. AES is the best encrypting algorithm to use all encrypt document [4], The major fear which every user have



doi: 10.32622/ijrat.76S201927

is I can lose our data in case if I forgot my password, then how will I get back my data. For solving this problem, general methods can be used like:

- Creating different patterns of passwords by scanning iris of a user.
- 2-way authentication, email verification and date of creation are some of the ways to recover users account.
- Suggesting at least 3 people as a nominee, on whom user can trust

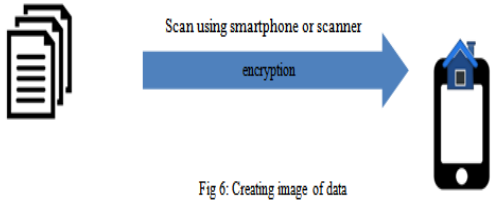


Fig 6: Creating image of data

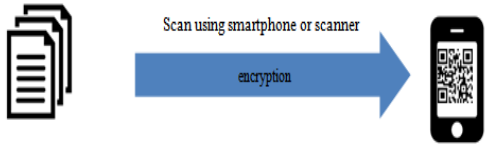


Fig 7: Creating QR code or bar code from data

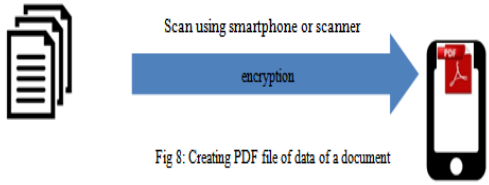


Fig 8: Creating PDF file of data of a document

## IV. Conclusion

This paper was successfully completed with the implementation of it. The data before encryption and data after decryption is analyzed and found to be same in each and every parameter starting from font size of dimensions of page to color of a paper. The digital signature is now mandatory in digital market. Adding digital signature to our document increases the percentage of safety of data. A digitally signed document can be shared by any means like e-mail or anything else also.

## Acknowledgment

This research was done under the guidance of Dr. T N Anitha, who is the HOD of Computer Science and Engineering department of SJCIT. And the motivation of working is from Digital India campaign, global warming. A special thanks to A. Illiev and Stalling for dedicating their life for advancement of encrypting technology. A special thanks to S J C Institute of Technology for providing us an opportunity for showcasing our talent

## References

[1]. Harshal R. Kanhekar, Mrs. Sayalis N. Mane, "Digital Wallet", I.J. Wireless and Microwave Technologies, 2015, 4, 62-68 Published Online July 2015 in MECS (http://www.mecspress.net) DOI: 10.5815/ijwmt.2015.04.06.
[2]. A. Illiev and S. Smith, "Private information storage with logarithmic-space secure hardware", in proceedings of IEEE international conference on Information Security, Management, Education and Privacy, pp. 156, 2004
[3]. P. Sutheebajard, "QR-code generator", in proceeding Eight International Conference on ICT and Knowledge Egineering, Article: November 2010.
[4]. Stallings, W. (2006). "Cryptography and network security: principles and practices". Pearson Education India.
[5]. Christina Nunez, "Deforestaion explained", National Geaograhpic Channel, Published:3 Feburary 7 2019.
[6]. K.cMayes and K. Markantonakis, "Smart Cards, Tokens, Security and Applications", in proceedings of IEEE international conference on Information Security, Management, Education and Privacy, pp. 256, 2008.
[7]. M. Pitchaiah, Phileemin Daniel and Pravenn, "Implementaion of advanced encryption standard algorithm", International Journal of Scientific & Engineering Research, Volume 3, Isssue3, Publish 3 March 2012.
[8]. Ako Muhammad Abdullah, " Advanced Encryption Standard (AES) algorithm to encrypt and decrypt data", ResearchGate, publication number: 317615794, Issue: 16 June 2017.
[9]. Abdullah, A. M., & Aziz, R. H. H. "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm.", International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17), Issue: June 2006



doi: 10.32622/ijrat.76S201927