IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

DIGI-SIGN

[1]Appannagowda D, [2] Harshitha G R, [3]Hithaishini C, [4]Hrishikesh C V, [5]Roopesh kumar B N

[1,2,3,4]Undergraduates, Computer Science and Engineering, K S Institute of Technology,
Bengaluru, Karnataka, India-560109, Affiliated to VTU, Belagavi
[5]Associate professor, Department of Computer Science and Engineering, K S Institute of Technology

Abstract: Paperless Operation has become a very big matter of fact and demand of the society in this fast growing world around us. With increasing population and proportionally increasing services day by day it is ethically very hard to accommodate every single transaction with a piece of paper because that costs a number of trees to the environment. As this rapid cutting of trees have adverse effect on environment and the ecological balance. To solve such problem we need paperless technologies. Digi-Sign is a digital signature system that facilitates creation of digital signatures for documents online, and also facilitates users to communicate online with the help of AES methodology. It also allows status tracking of the document and empowers the owner to maintain the same. Digi-Sign has built in features which allows feasibility of operation with digital signatures and also allows faster creation of signature keys alongside provide instant verification of document online. It binds every single signatory and addressee together into a same network for faster communication that has never been possible before. Digi-Sign do not encrypt the entire document, it creates signatures using basic information of any document. It hosts a public database to index the all the documents created by various owner in one place. That helps easy accessibility for validation of information about any document.

Index Terms - **AES, Encryption, Digi-Sign (digital signature), centralized Database.**

I. INTRODUCTION

During the immergence of Digital signature systems, throughout the time various models have been introduced and most of them were intended to eliminate the use of physical signatures and stamps[1]. One of them is RSA encryption which is practiced in various parts of the world, in this technique the targeted document is encrypted and hash key is generated with respect to the same. A public key is shared which helps to validate the document's hash[2]. The owner holds a private key, to verify the encryption is a combination of public key and signature is required. This technique is also used for point to point encryption of messages[3].This system achieved wide application in message encryption but in case of document signature it has faced various limitations like this service is provided by government organizations under various schemes which is on one hand is provided after submission and validation of applicant's legal documents for every individual signature and is a lengthy process and equally costly and when it involves sharing of keys, it is sometime vulnerable to misuse threats[4]. Digi-Sign introduces a much feasible model which overcomes the existing ethical and technical challenges and provides access to features like:A much cheaper digital signature system, as conventional techniques are costly and are as per owner specification. A much faster hashing and validation procedure, especially for validation purpose by eliminating the requirement of any software (to regenerate the hash for the entire document every time to validate it). A centralized database where a reference to every single digitally signed document exists. So, that the identity of any digitally signed document never gets lost in case the proprietor cannot be identified or is out of reach. A system that can provide instant authentication of any document and also holds the information about the validity of the same and can be maintained at any point of time by the signatory. A digital signature system that provides enough ease of access to be inhibited within the daily lifestyle of our society. Replace encrypted files with files of common document format for easier operation. Digi-Sign succeeded to exhibit the above explained features in it and alongside it also overcome weaknesses in the existing models of digital signature techniques. Digi-Sign exhibited centralized open database which gives basic information about every document signed through it and act as one stop digital preservation solution to every query regarding documents/articles. Digi-Sign maintains similar level of ownership over every signature record by their signatories. So, no discrimination can be done regarding disclosure of information. Due to being open in nature it does not require the authorized person to hold any private key and completely eliminated the factor of private key misuse. Due to being a SaaS (Software as a Service) model and being maintained online, services ofDigi-Sign can be accessed by various public and government service applications programmatically which provides improvement in the expansion of utilization of digital signature technology. Right to Information can be implemented in a more efficient way with faster access to information. The status of any record can be instantly updated and maintained by the signatory, it brings control over document theft and fraud. Digi-Sign incorporated the use of Qr-Code as a representation of the digital signature on the document which eliminated the use of encrypted files. The organization of the paper is listed as below. Section II explains about the literature. Section III describes the methodology. Section IV describes the results. Section V concludes the paper and Section VI gives the references.

II. LITERATURE SURVEY

Digi-Sign is built to b ridge the gap between everyday life activities and their access to paperless operation with the help of digital signature system. Every digital signature system is firstly built to eliminate the use of physical stamp and signature on documents and they have their own techniques to solve it. The concept of Digi-Sign is based on building a centralized database which people and organizations can use to create digital signatures there after Digi-Sign provides a digital preservation platform where the information are stored for viewing and anyone with a genuine signature can look up for information regarding the same in Digi-Sign database. Every single entity (single user or organization) is allowed to join the service by creating an account by providing legal information about them which gives everyone the ability to practice digital signature instead of using paper document. This system also brings a solution to a major challenges held on the existing digital signature models, which is protection of private keys. In their research in 2008 Francesco Buccafurri, Gianluca Caminiti, and Gianluca Lax, DIMET Dept, University of Reggio Calabria. Loc. Feo di Vito, I-89122 Reggio Calabria, Italy have shown how digital signatures can be successfully. Now in case of Digi-Sign, a new technique has been figured out replace the signature and the stamp using hash key. Now this is a modified version of existing RSA encryption techniques, Digi-Sign signature creation technique has been discussed in Section III – B. The hashes built in conventional systems were for the entire document but in case of Digi-Sign, it going to pick up only few important parts from a document i.e., header, subject and Name of the addressee. Now in one hand Digi-Sign will store them in a single public database for indexing along with all the relevant information about the signatory and the owner, on the other hand it will use a standard hashing algorithm to produce the unique digital signature key. Now because hash keys are quite long and are difficult to note and remember. For ease of access Digi-Sign provide two complimentary options to replace the Stamp and Signature, they are Qr-Code. Both are embedded with the Web URL used to validate the authenticity of the document online from the Digi-Sign public database just by scanning the Qr-Code using a hand held scanner or mobile phone scanner application. Now instead of creating the entire hash the operator can register all the required information on Digi-Sign database and simply paste either of the two code images on the document and forward the document for further use. As there is no use of any key sharing, Digi-Sign maintains a very clear policy for maintaining the records i.e., it neither index all the stored information anywhere nor it prohibits anyone with a valid signature key to check the records. Over all Digi-sign provide a strong support to Right to Information. With features like instant document validation and authenticity control, it will help every sector of the society to work more efficiently.

III. DESIGN AND METHODLOGY

3.1 System Architecture:

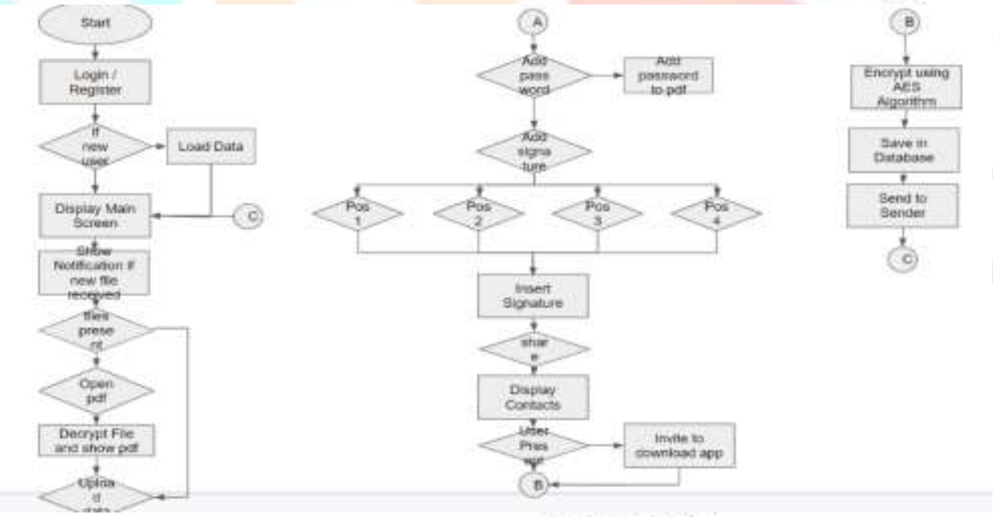


Figure 1: Architecture of the Proposed System

Digi-Sign represents itself as a SaaS (Software as a Service). On breaking the entire Digi-Sign service we can separates various objectives on which Digi-Sign operates. A. Creating User base Digi-sign first of all keeps record about every single entity using it, through accounts. The most important part is it allows both individual users and also organizations to create account using some legitimate documentations that validates that person’s or organization’s identity.

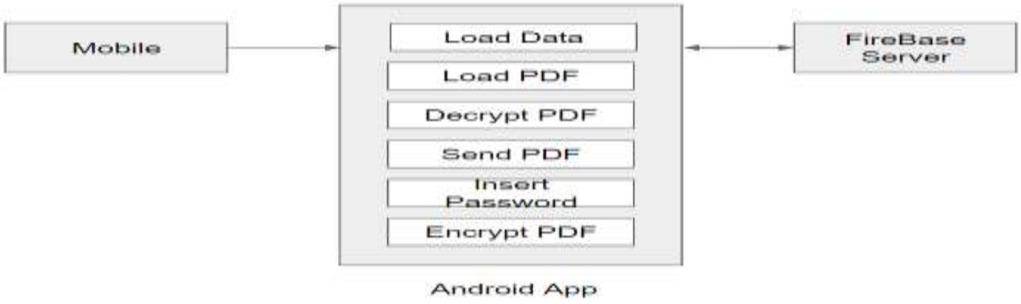


Figure 2: Implementation of Signature on PDF

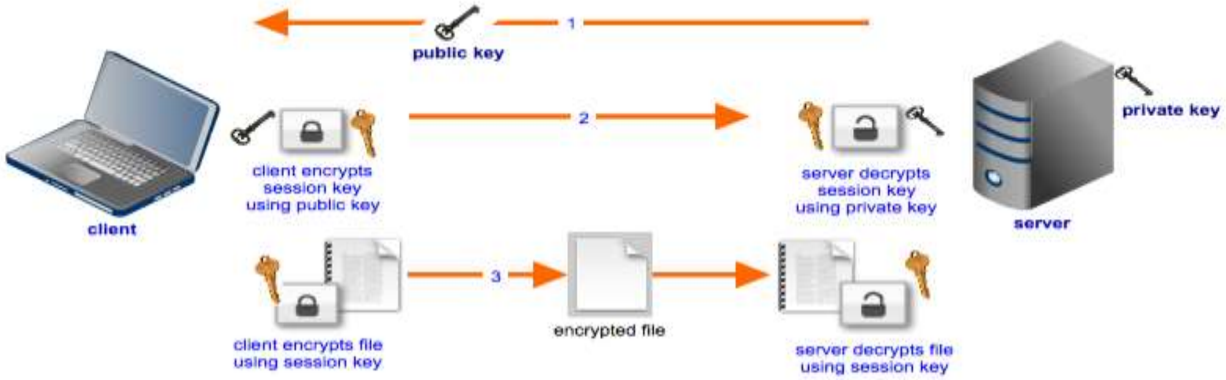

1
public key
client
2
client encrypts session key using public key
server decrypts session key using private key
server
private key
3
client encrypts file using session key
encrypted file
server decrypts file using session key

Figure 3: Implementation of Encryption AES 16 Bit

1. PDF Sign
2. Convert PDF to Bitmap
3. Collect Sign Details from DB
4. Convert Sign Details to Bitmap
5. Insert Sign Bitmap on PDF Bitmap
6. Convert signed bitmap to PDF

AES belongs to a family of ciphers known as block ciphers. A block cipher is an algorithm that encrypts data on a per-block basis. The size of each block is usually measured in bits. AES, for example, is 128 bits long. Meaning, AES will operate on 128 bits of plaintext to produce 128 bits of ciphertext. Like almost all modern encryption algorithms, AES requires the use of keys during the encryption and decryption processes. AES supports three keys with different lengths: 128-bit, 192-bit, and 256-bit keys. The longer the key, the stronger the encryption. So, AES 128 encryption is the least strong, while AES 256 encryption is the strongest.In terms of performance though, shorter keys result in faster encryption times compared to longer keys. So 128 bit AES encryption is faster than AES 256 bit encryption. The keys used in AES encryption are the same keys used in AES decryption. When the same keys are used during both encryption and decryption, the algorithm is said to be symmetric. AES is implemented in secure file transfer protocols like FTPS, HTTPS, SFTP, AS2, WebDAVS, and OFTP. But what exactly is its role? Because symmetric and asymmetric encryption algorithms each have their own strengths, modern secure file transfer protocols normally use a combination of the two. Asymmetric key ciphers a.k.a. public key encryption algorithms are great for key distribution and hence are used to encrypt the session key used for symmetric encryption. Symmetric key ciphers like AES, on the other hand, are more suitable for encrypting the actual data (and commands) because they require less resources and are also much faster than asymmetric ciphers. The article Symmetric vs Asymmetric Encryption has a more thorough discussion regarding these two groups of ciphers. Here's a simplified diagram illustrating the encryption process during a typical secure file transfer secured by SSL/TLS (e.g. HTTPS, FTPS, WebDAVS) or SSH (e.g. SFTP). AES encryption operates in step 3.

IV. RESULTS

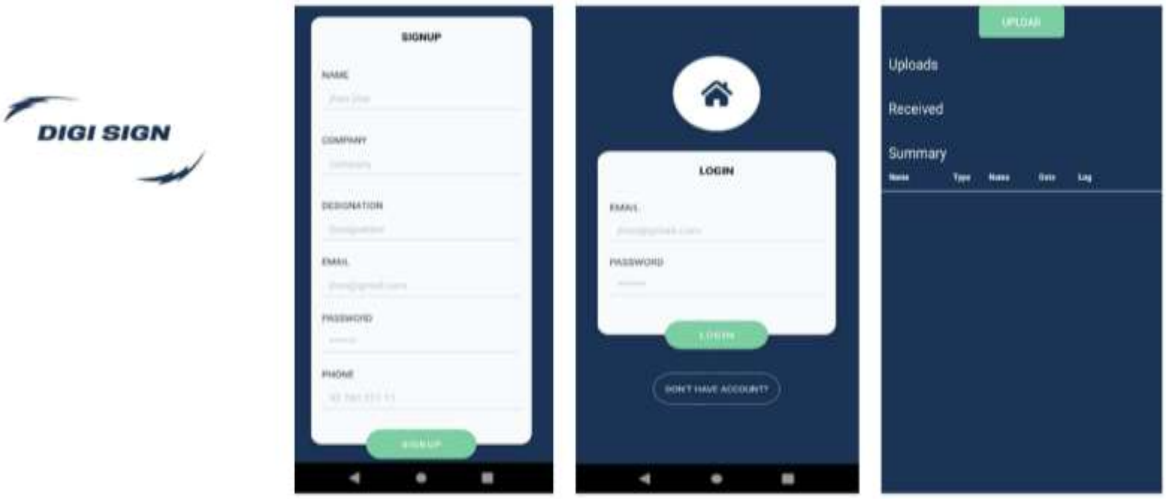
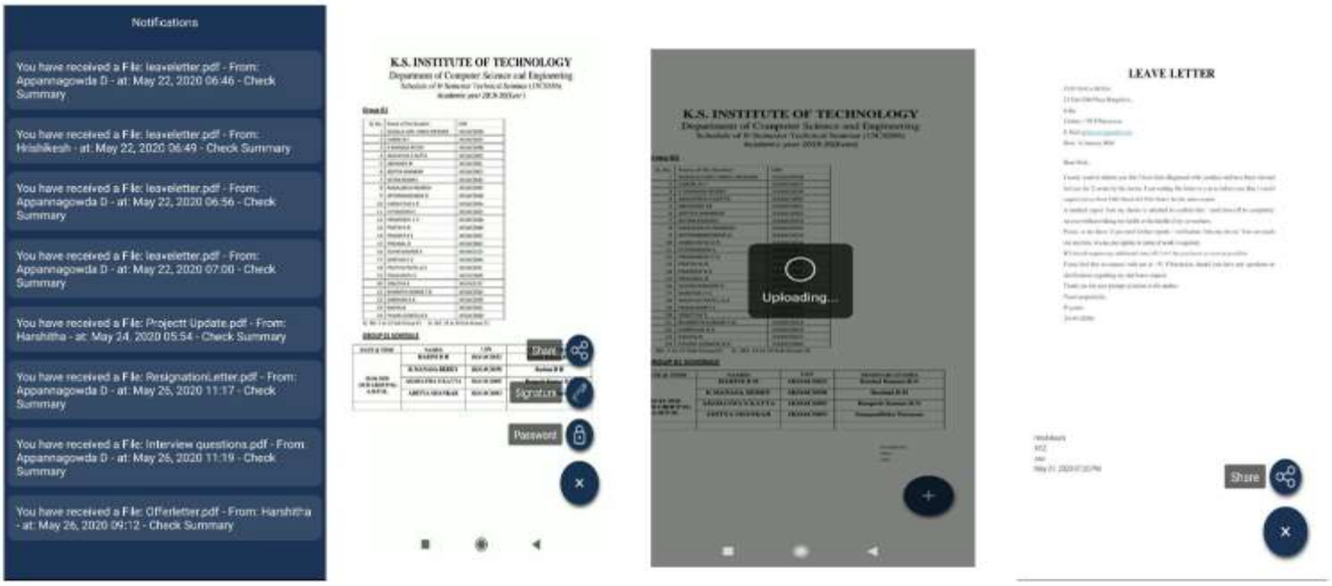


Figure 4. Login to the account.



Notifications

You have received a File: leaveletter.pdf - From: Appannagowda D - at: May 22, 2020 06:46 - Check Summary

You have received a File: leaveletter.pdf - From: Hrishikesh - at: May 22, 2020 06:49 - Check Summary

You have received a File: leaveletter.pdf - From: Appannagowda D - at: May 22, 2020 06:56 - Check Summary

You have received a File: leaveletter.pdf - From: Appannagowda D - at: May 22, 2020 07:00 - Check Summary

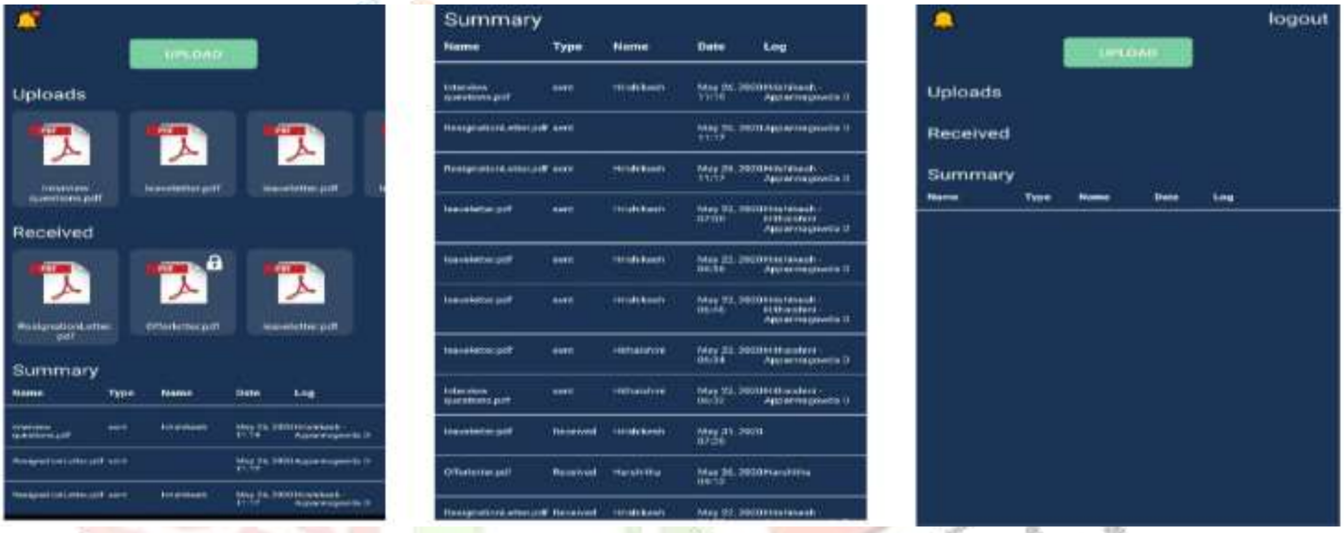
You have received a File: Projectt Update.pdf - From: Harshitha - at: May 24, 2020 05:54 - Check Summary

You have received a File: ResignationLetter.pdf - From: Appannagowda D - at: May 25, 2020 11:17 - Check Summary

You have received a File: Interview questions.pdf - From: Appannagowda D - at: May 26, 2020 11:19 - Check Summary

You have received a File: Offerletter.pdf - From: Harshitha - at: May 26, 2020 09:12 - Check Summary

Figure 5. Signature using AES encryption algorithm



Summary

Name	Type	Name	Date	Log
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Figure 6. Sender and the receiver end log with summary.

V. CONCLUSION

Inventions and discoveries are all the creativity of human mind. It just depends on how we look at the world around us. Even before the discovery of fire someone must have thought about rubbing two rocks together that caused the bright spark of light that is guiding our knowledge till this date about this world. We can innovate the world just the way we want and solve our day to day life problems and let the mankind inhibit them. We can partially own any part of this nature but we can never impose our ownership on it. The nature will work the same way as it always do but as the most advanced generation of living beings on this planet our demands are also more. But with greater capability come in the greater responsibility to save the resources of this planet as we are the one who is extracting the most out of it. Digi-Sign is just a solution to reduce the unwanted consumption of papers. But there are still various other natural resources which are being exploited over time, we have to take responsibility to save them before they vanish from the environment.

VI. REFERENCES

[1] Franceco Buccafurri; Gianluca Caminiti; Gianluca Lax, "Signing the document content is not enough: A new attack to digital signature", ICADIWT, Pages: 520 – 525, 2008 IEEEXplore.

[2] MaxE. Vizcarra Melgar; Mylène C. Q. Farias; Flávio de Barros idal; Alexandre Zaghetto, "A High Density Colored 2D-Barcode: CQR Code-9", SIBGRAPI, Pages: 329 – 334, 2016 IEEE Conference Publication.

[3] J. Barr ; B. Bradley ; B.T. Hannigan,"Using digital watermarks with image signatures to mitigate the threat of the copy attack",ICASSP, 2000 IEEE.

[4] V.Nagarajan, " Secure Data Transmission using Content Fingerprinting Digital Watermarking Techniques", The 30th International Technical Conference on Circuits/Systems, Computers and Communications (ITCCSCC 2015) June 29-July 2 at Grand Hilton Seoul, Seoul, Korea

[5] V.Nagarajan, " A Secured Data Transmission Using Digital Image Watermarking Scheme ", The 30th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2015) June 29-July 2 at Grand Hilton Seoul, Seoul, Korea.

[6]. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley, 1995.

[7]. J. Feghhi and P. Williams, Digital Certificates: Applied Internet Security, Addison-Wesley Professional, 1998.