



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DIGI-SIGN

Roopesh Kumar B N¹, Appannagowda D², Harshitha G R³, Hithaishini C⁴, Hrishikesh C V⁵

¹ Assistant Professor, ^{2,3,4,5} Student

^{1,2,3,4,5} Department of Computer Science and Engineering,

^{1,2,3,4,5} K.S. Institute of Technology, Bengaluru-560062, Karnataka, India.

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 SHA 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 - SHA, 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.

[5]. 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. DigiSign 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 of Digi-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 concludes the paper. Section V gives the references.

II. LITERATURE SURVEY

Digi-Sign is built to bridge 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. METHODOLOGY

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 e.g., AADHAR CARD. These accounts are used to represent the information about the issuer and also make direct communication with the addressee if he or she or the organization is already enrolled with this service (else just refer red with name in the record). Employees working for any particular organization has to create their own individual account then they can request permission from their organization to create signatures on behalf of it (onetime permission). B. Document Hashing and Record Building If we compare, every official document has few things in common.

- Header
- Subject
- Name of Addressee (with address).

Fig. 1 shows a process diagram of the Digi-Sign signature creation process. In the Digi-Sign signature creation process various steps are involved are mentioned below:

Step 1: User enters the required contents about the document though the user interface.

Step 2: A copy of each of these provided content is passed to a concatenation and SHA-1 hashing function where the total provided information are concatenated into a single string of text and then converted into a SHA-1 hash key.

Step 3: The hence generated key along with the original data contents are then passed to the Digi-Sign controller. DigiSign controller interface checks for duplicate record on the database and reports an error if any duplicate record is found.

Step 4: If the query in Step 3 returns a false result then a new query is executed to create a new signature record. The database API (Application Programming Interface) returns the result of the query to the Digi-Sign controller.

Step 5: On successful creation of record controller pass the hash key generated in Step 2 to the code image generator function. The code image generator enrol the Web URL of the signature record in the Digi-Sign database into a Qr-Code and output a view with the generated code images.

Step 6: Finally any of the code image can be pasted in the e-document to represent its digital signature and can be further populated. The proprietor on the generated signature is decided under two conditions. If the signatory used his/her Professional Signature Panel then the owner is maintained as the organization, signatory works for. Else while using Personal Signature Panel the owner is maintained as the user himself. The hence generated record contains these content details:

- Header
- Subject
- Addressee
- Signatory
- Date of Signature

- Issuing Organization (professional operation)
- Organization Mail Id (professional operation)
- Organization Contact Number (professional operation)
- Official Website of the Organization (professional operation)
- Signatory's Contact Details (personal operation)
- Status of the Document
- Hash key C. Presentation On a successful generation of signature Digi-Sign.

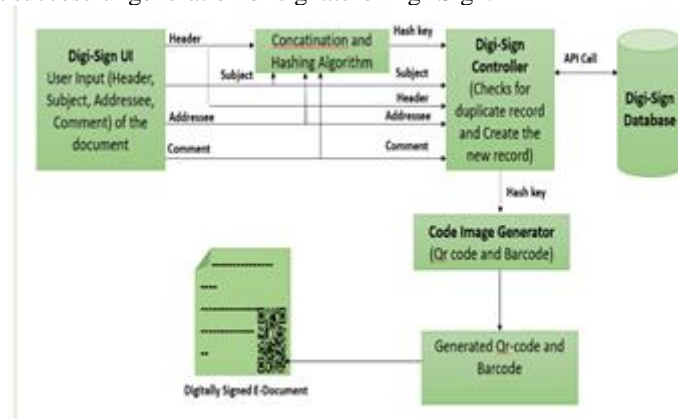


Fig1.Digi-sign creation process

IV. 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.

V. 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 IEEEExplore.
- [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.
- [8] C. Adams and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, AddisonWesley, 2002.