IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Alternative of Applet for Digital Signature Long Term Value in Web Based Signing

Anup Kumar Pandey[1*], Anil Kumar Mahto[2]

[1,2] Jamia Hamdard,New Delhi-110062,India

[*]*Corresponding Author: anupmca007@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i6.1923 | Available online at: www.ijcseonline.org

Accepted: 13/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Today various type of organizations interact with DATA; while sharing / storing / retrieving / communicating such huge data with Public; such as Government organization, Medical, Agricultures(land records) Insurance domain (in term of storing / archiving data/file) and other try to validate the digital document using digital signature . Some document might be used for a short time period, but here I am talking about sharing / store / archive the document for a longer period i.e. long time value (LTV), because if documents are important for future having future prospective need to be preserved for a longer period than expected. The main problem is how to ensure about, the document authenticity, Integrity, non-repudiation, and proof of existence for long-term. Here we put the document (.pdf) sign, which contains the information's like (Certificate, certificate chain, signed message digest, revocation information and time stamp), and here also trying to provide the solution for replacement of applet in web based signing, newer approach will be available both for the Standalone as well as window services i.e. Time and Cost saving for the user.

***Keywords*—** Digital signature Algorithm (DSA), DSC, Alternative of Applet, web based digital signing, Long Term Value (LTV), TSA Certificate

I. INTRODUCTION

Digital Signature is a mathematical schema for verifying the authenticity of a digital document or message.

A "digital signature" is used with the transfer & propagation of Data or any type of document or message; either document or message is encrypted or not, while securing Integrality of Data & Identity of the Sender.

Simply ensuring, that the message so communicated has arrived intact, to its intended recipient; at the same time the Identity of the sender is not compromised

Algorithms used in Digital Signature Algorithms used in a digital signature are mainly of three types, literally known as (G, S, V):

1.Hashing algorithm (G – generates Public Key for corresponding Private key)

2. Signature generation algorithm (S -Signing)

3. A signature verifying algorithm (V –verifying) that tries to verify the Document , public key and signature used , while identifying the authenticity of the Document

Hashing Algorithm (G – generates Public Key for corresponding Private key) : In Digital communication platform, security remains a concern always, which can be solved to a greater extent through Cryptography, by using the Hash functions. Cryptographic hash functions tries to map the input strings of arbitrary length and simultaneously generating a shorter fixed length output strings [13].the seminal paper Published of Diffie and Hellman " New directions in cryptography " on cryptology, 1976 [10].

Signature generation Algorithm (S -Signing): Digital Signing , uses the user defined Algorithm Pattern, which ensures the integrity and authenticity of digital message , privacy of conversation, at the same time the Identity of the sender is not compromised [11] the encrypting techniques used in Digital Signing. The Digitally signed message carries the hash function value [13], the message content and the unique signing information.

Digital Signature Verification (V -verifying): It is the process of verifying the digital signature associated with the original message and a given public key. Verifying also relies on a defined formula. This Verification & Validation Process may be Accepted or Rejected, defending upon the successfully pass of Verification Process. If Verification

process couldn't pass successfully, then Revocation comes into existence, bringing termination of executing process.

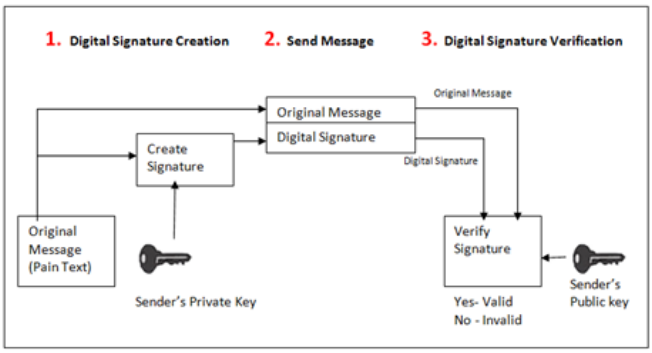

Figure 1. Illustrate the digital signature simple verifying process

A "digital signature" is an authentication process that facilitates the propagator of the message to put a code that behaves as a signature, used for Verification & validation. The Digital Signature Algorithm (DSA) is used as a signing algorithm for authentication. The validation process if not passed successfully, revocation of Authenticity comes into existence, bringing a termination of process execution. Thus validation & Verification is essential & crucial, while transferring Digital contents over Digital Platform, using DSC.

For this two main activities need to be performed:

Firstly, the authenticity of a signature is to be verified by generating a fixed private key from a fixed message and that can only be verified & validated by using the corresponding public key.

Secondly, it should be computationally not possible to generate a valid signature for a party without knowing party's private key.

Long Term Value, In a Globalized World, communication through Digital Platform became more common and gaining importance, which is expanding day-by-day. The use of Digital Platform is gaining appreciation, mainly due to its usefulness in timely delivery of DATA Content & COST-EFFECTIVENESS of the Digital Platform.

The e-Governance initiative is an extended leg to such activity, taken into hand by the Govt., along with uses of Digital Platform in many different facets of life. Just like Banking, DATA BANKING is the banking of "DATA", at the same time preserving & making such valuable DATA available for Future use (to be accessed & used in the future time).

The concerns or issues associated with the Preservation and archiving of digital in-formation, in the future period using long-term value [8] is an important terminology, while maintaining authenticity and integrity of the stored Document or DATA (for the future in terms of DATA BANKING & DATA STORING).

Like huge data used by Govt. Organization i.e. any Government Data or any other important document or data stored electronically, to be used in future, i.e. having future prospective. In some cases, this preservation & archiving may extend beyond 10 years period, during such period a good number of Official Authority may have changed their position, thus transferring the preserved data contents from one Authority to the other or one User to other User, which definitely need to follow a Definite Authenticity Cycle.

Web based digital signing, means signing of the digital document or data, using web based applications. Various web based applications simultaneously support, signing the document, uploading & sending to any other user, keeping the security environment intact.

II. RELATED WORK

Explains based on reputation-based trust system for time-stamping-based archiving called Long-term evaluation of Trust (Lot).This plays an important role to manage the electronic documents, in preserving for the Future, over a long time period [1].

Martin vigil etal, is a survey paper, author tries to summarize the existing issues with securing digital documents, over a long periods of time. Records like Land Records / Medical Records etc., where the origin of the document needs to be verified and the Originator must not be able to Repudiate, that s/he is not the originator [2].

And how to find the document is originated by valid person or not and introduced some result based on the survey.

Focused on long-term validation of digital signature based technology used. It is based on notarization paradigm; propose a mechanism of cumulative DATA NOTARIZATION.A notarization token structure encapsulates an identical data structure containing a previous notarization token, and verify the validity of initial signature [3].

Suggest a methodology that process the digital signing ,based on virtual and interrelated levels of communication and It is argued that structural reliability depends on a quantitative metric, such as the structural in formativeness along with other qualitative characteristics of the syntactic component . The structural reliability of several document representation protocols is evaluated and it is concluded that the higher the in formativeness of the protocol, the less the semantic

distance produced, provided that the communicating parties have the capacity to handle this protocol [4].

III. METHODOLOGY

Here we have proposed the model in two parts-

1. Model for replacement of Applet

2. Model for Long Term Value (LTV)

Model for replacement of Applet For the replacement of applet, presently we have two types of solutions in hand.

•Based on JavaScript / Jquery

•Based on Spring boot application

Based on JavaScript/jquery, we can also able to access the attached information associated with digital signature communication. But it has some inherent issues associated with it, which stand as that of limitations; like, some-times JavaScript/Jquery not working in proper manner and also have the some other associated issues. Sometime user may encounter with Technical Glitch.

Based on Spring Boot application, we create a spring boot application, which is to be installed at client's machine and it provides some predefine restful url , through which we can access / interact the attached digital signature information . Here we are using the spring-boot application, this newer ap-proach will be available both for the Standalone as well as window services i.e. Time & Cost saving for the user.

For Long term value While moving for Digital signing , it is essential to check the validity of the Signer's Certificate, ie. the validity is not revoked- this is where a Validation Authority comes in (it is based on either OCSP/CRL technology or any others).

At the time of signing, it is more important that, the signer's certificate was authentic (not revoked/expired). To do this, proof of the time at which the signature was applied is needed and this is accomplished by using a "Time Stamping Authority" (TSA) to produce authenticity of the time of signing, instead of simply relying upon the signer's time only.

LTV signatures are embedding with timestamps and OCSP/CRL elements at the time of signing.

With the use of long-term signature, the lifetime of the signature can be extended up to the lifetime of the TSA certificate, which stands as an advantage over other tech-nologies, no doubt.

To obtain the LTV and digitally signed document using web based application with-out using applet tools, steps are given below.

Step I- Each of the transaction initiated need to be logged whether it is a successful or failure in case of registration/authentication/signing.

Step II- Keep every XML as Logs for a specific time period like one month or so.

Step III- Keep all details sent from signer app in relevant database structure i.e. enabling & supporting Long term verification. In this, PKCS Object + OCSP Response or CRL File + Chain certificates including user certificate, to be kept in a relevant order as returned from signer app.

Step IV- While making request for revocation in case of authentication and signing, get all chain certificates from database as will be provided to consuming application during response of registration process.

Step V- Do generate relevant DB structure to keep certificates chain pertaining to registered user in DB.

Step VI- Do generate relevant DB structure for LTV for logs purpose, in a separate table, while executing operations like registration, signing and authentication.

Step VII- During all transaction for DSC activities in response of xml, there is status attribute with returning value 0 or 1; further actions will be performed only after checking zero / & one; zero means failure and one means success.

Step VIII- Revocation check will be performed by the consuming application, is to be made mandatory by calling CRL Web service.

Step IX- it's suggested to keep Hash of original noting in DB to track any changes of original content, for the concurrent Audit Trail purpose.

Step X- From now onwards we are signing with PKCS7 standard to enable LTV, and from this, the consuming application not able to get original data, only it can be veri-fied with original content.

Step XI- DSC Signer application returning/consuming certificates list where at 0 level is user certificate and n is root certificate.

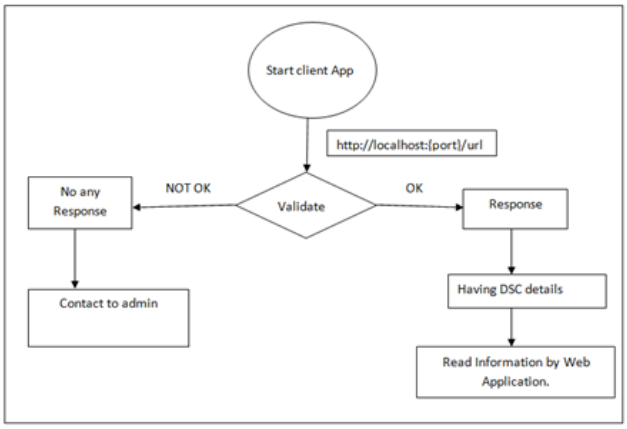

Figure 2. Illustrate the Client application activity

Below Diagram Show the pdf signing and embedded the certificate chain into the pdf.

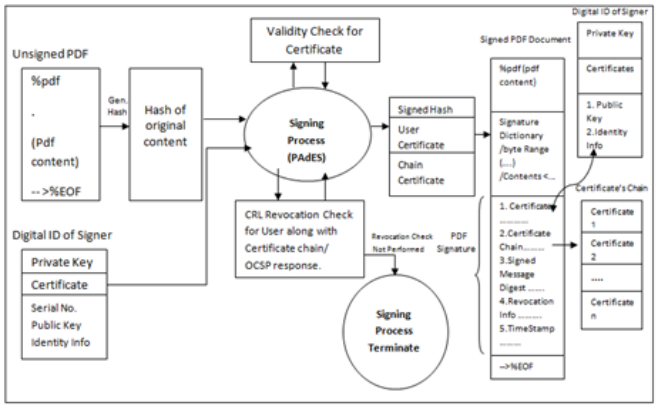

Figure 3. Illustrate the digital signature digital signature LTV process

In above diagram , when we go for signing a pdf document, get the hash value of the pdf content based on the Hash functions and simultaneously by using the digital id of signer applied in the signing process based on the signer's digital id. It checks the validity of the certificate and also it checks the certificate chain or OCSP responses; if response is found to be invalid, than the execution of the signing process terminates predefine. If all executing process passes uninterruptedly and found valid in all respect than it moves to the next step and consolidate the user certificate , pdf hash and certificate chain and together with generates the signed pdf which integrates all consolidated details into the pdf , giving an secured data transmission plat-form as shown in the above diagram.

IV. RESULTS AND DISCUSSION

Based on the some latest published paper we are purposing a new concept / Approach, the first part is how to save the digital signing document / pdf / content for the long time.

Because we know that digital signature issued by the some authority, under some condition, authority can revoke the digital signature rights. So at this condition we cannot justify the document, whether it is valid or not. The LTV approach is to be considered as a right kind of solution where, with a long-term signature, the lifetime of e-Signatures can be extended up to the lifetime of the TSA certificate, which stand as an advantage, no doubt.

Also, LTV signatures are embed with timestamps and OCSP/CRL elements, thus making it more trustful.

In various published paper which were stated below, in all of them, they are trying to provide the solutions for it; we have also tried to provide the solution but in a different manner, by use of different approach. This newer approach will be available both for the Standalone as well as window services i.e. Time & Cost saving for the user.

And here also, our approach tries to provide the solution for signing the digital document using web application along with standalone use, which is no doubt stand as an advantage over other approaches. In older application, where signing of document were carried by using web application, using the most trusted applet ; but as oracle is no longer going to provide the support of applet, so accordingly all the browsers simultaneously going to stop the support of applet. So at this condition, it is really very hard to, Digitally signing the document using web application [14]; currently we are working on it and thinking a new approach / solution to handle such issues in a more easier way, at the same time saving of Time & Cost for the user , which is the core area of discussion through this Publish.

V. CONCLUSION AND FUTURE SCOPE

In this project we are trying to preserve the digital signature document for long time. It means that we have tried to validate the document / pdf for a long period.

The LTV approach is to be considered as a right kind of solution where, with a long-term signature, the lifetime of e-Signatures can be extended up to the lifetime of the TSA certificate, which stands as an advantage, no doubt.

Also, LTV signatures are embed with timestamps and OCSP/CRL info into the signature at the time of signing, making it more trustful.

In above we are describing the functionality, how to achieve the long term value of digitally sign document.

On the other hand we have also tried to fill the gap of applet. In the absence of Applet support, we proposed a more convenient way of approach to handle such issues, in a more effective way, at the same time keeping in mind Time & Cost saving for the user. It means that we put forth a concept, how to digital sign the document using web but without applet. Above I have also provided such type of solution, where such

proposed approaches finds fit & justifiable. This newer approach will be available both for the Standalone as well as window services i.e. Time & Cost saving for the user.

Currently, we are working on it and trying to do it in a more effective way, and also we are trying to implement the above concept in a running phase, so that we can give the exact kind of proof that we are thinking in a right direction, overcoming the arisen issue in a more effective way, addressing almost all the concerns associated with, by applying an appropriate way of Approach.

Based on this concept we are able to fulfil the lack of applet it is the main objective.

REFERENCES

[1] Mart´ın Vigil, Denise Demirel, Sheikh Mahbub Habib, Sascha Hauke,Johannes Buchmann, and Max M¨uhlh¨auser, "*LoT: a Reputation-based Trust System for Long-term Archiving*", SECURWARE: The Tenth International Conference on Emerging Security Information, Systems and Technologies,2016.

[2] Martı´n Vigil ,Johannes Buchmann ,Daniel Cabarcas ,Christian Weinert , Alexander Wiesmaier "*Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey*", elsevier ,computer and security 20,16-32 ,2015.

[3] Dimitris Lekkas, Dimitris Gritzalis, "*Cumulative notarization for long-term preservation of digital signatures*", elsevier , Computers & Security (2004) 23, 413-424,2004.

[4] Argyris Arnellos , Dimitrios Lekkas , Dimitrios Zissis , Thomas Spyrou ,John Darzentas, "*Fair digital signing: The structural reliability of signed documents*", elsevier computers & security 30 (2011) 580-596,2011.

[5] Mart´in A. G. Vigil, Daniel Cabarcas,Alexander Wiesmaier, and Johannes Buch-mann, "*Authenticity, Integrity and Proof of Existence for Long-Term Archiving: a Survey"*.

[6] S. Ries, S. Habib, M. M¨uhlh¨auser, and V. Varadharajan, "*Certainlogic:A logic for mod-eling trust and uncertainty*", in TRUST, vol. 6740, 2011, pp. 254-261.

[7] M. Vigil, J. Buchmann, D. Cabarcas, C. Weinert, and A. Wiesmaier, "*Integrity, authenticity, non-repudiation, and proof of existence for longtermarchiving: A survey*", Computers & Security, vol. 50, no. 0, 2015,pp. 16–32.

[8] H. M. Gladney, "*Preserving digital information*", Springer, 2007.

[9] C. Jee, "*Nhs promises real-time digital health and care records by 2020*",nhs-promises-real-time-digital-health-care-records-by-2020-3585822/ [retrieved: June, 2016].

[10] Diffie, W., Hellman, "*M.E.: New directions in cryptography*", IEEE Trans. on Information Theory IT-22(6), 644–654 (1976).

[11] Ravneet Kaur , Amandeep Kaur, "*Digital Signature*", International Conference on Computing Sciences, (2012).

[12] Saba Mushtaq, A.H.Mir, "*ignature Verification: A Study*", 4th International Conference on Computer and Communication Technology (ICCCT) (2013).

[13] Arvind K. Sharma, Satish.K.Mittal,"*A Comprehensive Study on Digital-Signatures with Hash-Functions*",International Journal of Computer Sciences and Engineering,Vol.-7, Issue-4, April 2019.

[14] A. Ghosh1, S. Karforma,"*Authentication of Study Material in E-Learning using Digital Signature Algorithms*",International Journal of Computer Sciences and Engineering,Vol.7, Special Issue.1, Jan 2019.

Authors Profile

Mr. Anup Kumar Pandey pursed Bachelor of Science from Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur (BPGC), 2007 and Master of Computer Application from UPTU (ITM,Gida Gorakhpur) in year 2010. I am currently pursuing M.Tech. and currently working as Team Lead (Java) payroll of velocis System Pvt Ltd,Nodia (UP) India,I have arroud 7 year work experences as developer as well as team lead.

Mr Anil Kumar Mahto, Currently he working as Assistant Professor Jamia Hamdard ,New Delhi,India and he have 5+ year experience in teaching and acadamic activity,he is pursuing in Phd.

