



Digital Signature for E-Governance – Security & Authentication

Arpitha Martin¹, Sadip Karki², Madhav Baiju³

Assistant Professor, Department of Information Science & Engineering, R.R Institute of Technology, Bengaluru, India¹

UG Student, Department of Information Science & Engineering, R.R Institute of Technology, Bengaluru, India^{2,3}

ABSTRACT: The Digital Signature is the method which is used to validate and authorize the content and users who are going to involve in the E-governance system. E-governance is the latest trend in many countries in which the government system is being online to deliver the governmentservices to the citizens. The services can be from Government to Citizen (G2C) and Government to Business (G2B) or Governmentto Government (G2G) or Government to Employee (G2E) or vice a versa. The vision of National e-Governance Plan (NeGP) of Government of India is to “make all Government services accessible to the common man in his locality, through Common Service Delivery Outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realise the basic needs of the common man”. The key objective of this vision is to provide e-services - G2B and G2C - in a ubiquitous manner. People can access any application or any scheme fromanywhere, anytime. As it comes with the word online, the biggest concern is the security issue. To provide E-authentication to theuser there are many cryptographic techniques available. This paper discusses to increase the security, reliability, and non-repudiation of the user’s data or information using Digital signature. It is highly secured and well-known method to authenticate and verify an electronic transaction.

KEYWORDS: Digital Signature, Security, E-Governance, E-Authentication, MD5 Algorithm

I. INTRODUCTION

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext. Thus Digital Signatures provide the following three features

- Authentication- Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.
- Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions.
- Non Repudiation – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

E-governance is the platform of Information and Communication Technology where all the government services have been delivered online, exchange information electronically, communication is done over the network and electronic transactions take place instead of the traditional system. There are so many entities involved in this E-governance system like a citizen, business, and government. There are many transaction models available involving all these entities. As much secure and confidential information is being passed over the network, it is required to provide security for the same. The Digital Signature is the method which is used to validate and authorize the content and users who are going to involve in the E-governance system, the sender cannot deny that he/she has not sent the particular message of content or document. Using any Hash algorithm, the hash value is generated and sender’s private key is used to make it more secure. Now the signed message is passed by the sender and at the receiver side, the message is decrypted using sender’s public key and again the hashvalue is applied to the message to read the original message.



II. RELATED WORK

In [1], in this research paper the study of DSC, implementation of DSC, Message Digest algorithm, DSC work flow, and DSC risk is presented. The usage of DSC and implementation of Message Digest algorithm must be focused to make the e-Governance applications more successful in a developing country like India. In [2], the proposed technique provides a way to shield the data, check the reliability and certification using best possible industry mechanisms. They have introduced encryption, authentication of user by owner and other by cloud and verification of the digital signature of the owner. In [3], they have proposed asymmetric encryption using a digital signature to maintain data integrity using the customized hash function. They get a better result after implementing dual digital signature mechanism. They have applied very smart concept which is more applicable by ECDSA instead of RSA Digital Signature. In [4], they have concluded that cryptographic system cannot be considered as fully secured from the infringement attempts of the intruders, there will be the scope for further enhancements in the field of certificate generation and database management system. In [5], they implement RSA algorithm with a digital signature in encryption to increase the security of user's data or information. They want to work using safe communication on computers between systems to user. In [6], Digital security is significant in E-Governance initiatives. Privacy of any transaction or information available on the network is essential. The important material or confidential data or information has to be protected from unauthorized users in E-Governance projects. Hence security is critical for successful implementation of such projects.

III. PROPOSED ALGORITHM

Here, n is the modulus, e is the encryption exponent and d is the secret exponent or decryption exponent. The algorithm is divided into 5 steps: Key Generation, Digital Signing, Encryption, Decryption and Signature Verification with their working functions are discussed as under:

Process-1: Key Generation

Randomly generate two large prime numbers: p and q .
 Calculate $n = p * q$
 Calculate the totient: $\Phi(n) = (p-1) * (q-1)$
 Select an integer 'e' such that $1 < e < \Phi(n)$ and $\text{gcd}(e, \Phi(n)) = 1$
 Calculate d , such that $d * e = 1 \text{ mod } \Phi(n)$
 The public key is (n, e) and the private key is (n, d) .

Process-2: Digital Signing

Generate message digest of the document to be sent by using MD5 algorithm.
 The digest is represented as an integer m .
 Digital Signature S is generated using the private key (n, d) , $S = m^d \text{ mod } n$.
 Sender sends this signature S to the recipient.

Process-3: Encryption

Sender represents the plain text message as a positive integer m .
 It converts the message into encrypted form using the receiver's public key (e, n) .
 $C = m^e \text{ mod } n$
 Sender sends this encrypted message to the recipient.

Process-5: Decryption

Recipient does the following operation:
 Using his private key (n, d) ; it converts the cipher text to plain text 'm'.
 $m = C^d \text{ mod } n$

Process-6: Signature Verification

Receiver does the followings to verify the signature:
 An integer V is generated using the sender's public key (n, e) and signature S
 $V = S^e \text{ mod } n$
 It extracts the message digest $M1$, from the integer V using the same MD5 algorithm.
 It then computes the message digest $M2$ from the signature S .
 If both the message digests are identical i.e. $M1 = M2$, then signature is valid.



IV. RESULTS AND DISCUSSION

1. Key Generation:

- 1) We have chosen two distinct prime numbers $p=23$ and $q=53$.
- 2) Compute $n=p*q$, thus $n=23*53 = 1219$
- 3) Compute Euler's totient function, $\phi(n)=(p-1)*(q-1)$, thus $\phi(n)=(23-1)*(53-1) = 22*52 = 1144$
- 4) Choose any integer e , such that $1 < e < 1144$ that is $\text{gcd}(e, 1144) = 1$. Here, we chose $e=3$
- 5) Compute d , $d = e^{-1} \pmod{\phi(n)}$, thus $d=3^{-1} \pmod{1144} = 763$
- 6) Thus the Public-Key is $(e, n) = (3, 1219)$ and the Private- Key is $(d, n) = (763, 1219)$. This Private-Key is kept secret and it is known only to the user.

2. Encryption:

- 1) The Public-Key $(3, 1219)$ is given by the Cloud service provider to the user who wishes to store the data.
- 2) Let the message to be send is "hello" which is converted to integer in the following manner: $A=0, B=1, a = 27, b=28, c=29$ and so on. So the message "welcome" is encoded to $m= 49313829413931$
- 3) Data is encrypted now by the Sender using the corresponding Public-Key which is shared by both the sender and the receiver. $C=m^e \pmod{n} = 49313829413931^3 \pmod{1219} = 625535179657807535$
- 4) This encrypted data i.e., cipher text is send to the recipient.

3. Digital Signature and Signature Verification:

- 1) First using MD5 algorithm the message gets converted to message digest i.e. to hexadecimal form.
- 2) $MD1 = H(m) = 0x000c00f0000000f0426f00f0726000f0$.
- 3) Message digest in decimal form $M1 = 01202400002406611102401141080240$.
- 4) Next digitally signed the message digest MD1 using its own private key d to generate digital signature S .
- 5) $S = (MD1)^d \pmod{n} = 0887025800025883929602588501240258$.
- 6) Sender then sends the digital signature S to the recipient.
- 7) Receiver then computes the integer V using S, e and n .
- 8) $V = S^e \pmod{n} = 01202400002406611102401141080240$.
- 9) Receiver the computes the message digest from S using MD5 algorithm
- 10) $MD2 = 01202400002406611102401141080240$.
- 11) Since $V = MD2$, so the Signature is verified.

4. Decryption:

- 1) The receiver decrypts the data by computing, $m = C^d \pmod{n} = 49313829413931$.
- 2) Once the m value is obtained, user will get back the original message using the same encoding technique. Some of the E-governance schemes that can provide security by implementing this type of algorithm to their users:
 - o E-payment: Every government should use this feature to get/receive the payment for the services offered by them.
 - o E-Tourist card: Tourists can get tourism card to visit any state/country from one portal only.
 - o E-Training: Any academic or professional training can be provided and more and more employees can get benefits from singleplace.
 - o E-Learning: The wide range of learning materials, audio, video will be provided through this medium and learners and tutors across the world can join this forum.

V. CONCLUSION

As the E-governance system is very wide and connected with citizens, business or another government, it must require maintaining the security concerns in any electronic transaction. There are so many cryptographic techniques available to provide the security. In this paper it is shown the use of digital signature in many government projects. It is also described how digital signature is implemented using the MD5 algorithm.

REFERENCES

- [1] Abhishek Roy¹, Sunil Karforma "Authentication of User in E-Governance: A Digital Certificate Based Approach" International Journal of scientific research and management (IJSRM) Volume-2 Issue-8, Pages 1212-1221, 2014, ISSN (e): 2321-3418
- [2] Shailendra Singh Member, IEEE; D. Singh Karaulia "E-Governance: Information Security Issues" International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec-2011



- [3] Nikhilesh Barik & Dr. Sunil Karforma “A Study on Efficient Digital Signature Scheme for E-Governance Security” Global Journal of Computer Science and Technology, Volume 10 Issue 3, February-2012 Online ISSN : 0975-4172
- [4] F.Jerlinmary, Dr.M.Deepamalar “Advanced E-Governance Security Using Certificate less Effective Key Management” International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 6, June 2017, ISSN(Online): 2319-8753
- [5] Shaikh Intiyaj, Er. Ratan kumar Agrawal, Dr A K Hota “Digital Signature Certificate: A Great scientific Knowledge for Nation Development” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 56-60
- [6] T. Sivasakthi, Dr. N Prbakaran “Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing” International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014 ISSN(Online): 2320-9801
- [7] Wojciech Kinastowski “Digital Signature as a Cloud-based Service” CLOUD COMPUTING 2013: The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization
- [8] Dhruvi Chaudhary, prof.Rakesh Shah “A Survey on Digital Signature with RSA encryption algorithm to enhance the Data security of cloud in cloud computing” International Journal for Innovative Research in Science & Technology, Vol-3Issue-8, 2016
- [9] Mr. D.Shiva, Rama Krishna “Providing Security to Confidential Information Using Digital signature” International Journal for Innovative Research in Science & Technology, Vol-2 Issue-6, 2015

BIOGRAPHY

Arpitha Martin is an Assistant Professor in the Information Science and Engineering Department, RR Institute of Technology, Affiliated to Visvesvaraya Technological University Belgaum. She received Master of Technology (MTech) degree in 2017 from Visvesvaraya Technological University Belgaum. Her research interests are Computer Networks (wireless Networks), Data Analytics, Data Mining etc.