Document tamper detection and verification using MD5 hashing algorithm and digital signature approach for online construction bidding System.

Madhura Kulkarni, MANALI DESHPANDE , SANIKA JOSHI, NEHA GOGATE

UG Student, Department of Computer Engineering.
NBN Sinhgad School of Engineering. Pune, India.

Abstract

In an online bidding system the bidder bid for the best deal. The documents shared are in electronic format and that leaves lot of scope for document tampering. Electronic files are typically shared by disc or download link using the honour system. Once these files have been dispersed, anyone can modify the contents to fit their narrative, and then distribute that version as an official exhibit. Such changes can be difficult or impossible to trace to their source due to the number of people with access to the files. To prevent this we will use MD5 with Digital Signature Standardization algorithm. We can identify each file by its unique Hash value and then use that identifier to ensure file integrity once file sharing has begun. In this system MD5(Message Digest 5) algorithm is used as a cryptographic hash function. MD5 hash is composed of 32 hexadecimal characters. Along with this digital signature approach(Digital Signature Standardization Algorithm) is used for verification Based on hash value calculations at sender and receiver side conclusion can be drawn whether document has been tampered with or not.

Keywords: *Cryptography, Encryption, Decryption, Message Digest 5, Digital Signature algorithm.*

I.INTRODUCTION

In an online bidding system the bidders bid for the best deal. The documents shared are in electronic format and that leaves lot of scope for document tampering. Electronic files are typically shared by disc or download link using the honour system. Once these files have been dispersed, anyone can modify the contents to fit their narrative, and then distribute that version as an official exhibit. Such changes can be difficult or impossible to trace to their source due to the number of people with access to the files.

To prevent this we will use MD5 with Digital Signature Standardization algorithm. We can identify each file by its unique Hash value and then use that identifier to ensure file integrity once file sharing has begun.

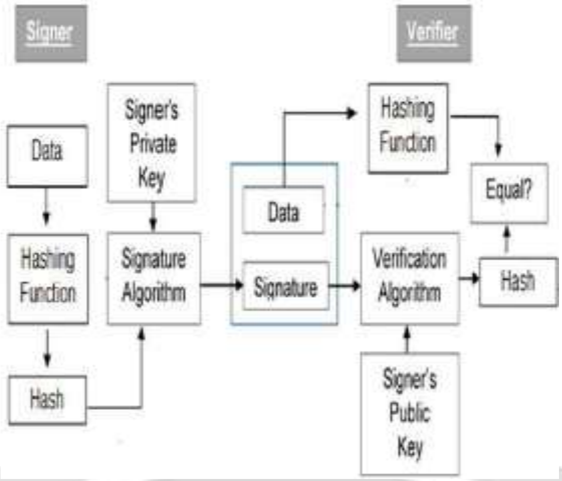
In an online bidding system the bidders bid for the best deal. The documents shared are in electronic format.

Once these electronic files have been dispersed, anyone can modify the contents, and then distribute that version as an official exhibit.

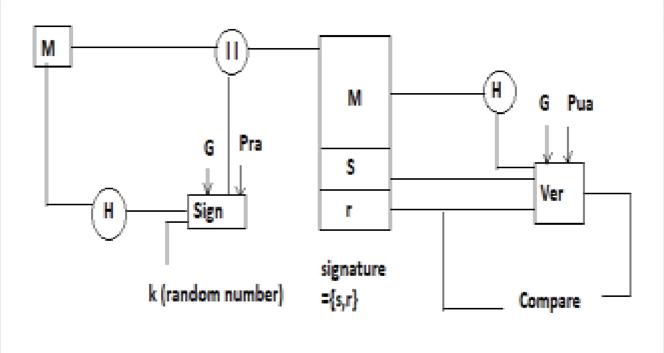
Such changes can be difficult or impossible to trace to their source due to the number of people with access to the files. To prevent this we will use MD5 with Digital Signature Standardization algorithm. We can identify each file by its unique Hash value and then use that identifier to ensure file integrity once file sharing has begun.

In this system MD5(Message Digest 5) algorithm is used as a cryptographic hash function. MD5 hash is composed of 32 hexadecimal characters. Along with this digital signature approach(Digital Signature Standardization Algorithm) is used for verification Based on hash value calculations at sender and receiver side conclusion can be drawn whether document has been tampered with or not.

II. SYSTEM ARCHITECHTURE



III. SYSTEM FLOW



- M-Original text document
- H-hash algorithm(output hash code)
- Encryption-Hash value ,global components ,k and private key input to signature algorithm.

Output of signature algorithm appended to original document(M+r+s).
Decryption-Hash value ,global components and public key input to verification algorithm.
R value computed again and compared with original to check for tampering.

IV. SYSTEM WORKING

The proposed system-online bidding site users bid to compete for the best deal.
To become a bidder-first step is to register on the web portal. After registration user can login.To make bid final user has to upload the quotation documents.

Verification:
The text document undergoes MD5 hashing algorithm to generate a hash code .This hash code is then encrypted using digital signature algorithm(Digital Signature Standard(DSS) approach) with the help of users private key and some public components(p ,q ,g and k).The output of this signature algorithm (r and s components) appended to the original text document and is then uploaded. On the server side the verification algorithm is applied wherein the hash code is calculated again by decrypting using the public key. The public key is calculated using users private key and compared with received r' value to check whether tampering has occurred.

V. SYSTEM DIAGRAMS

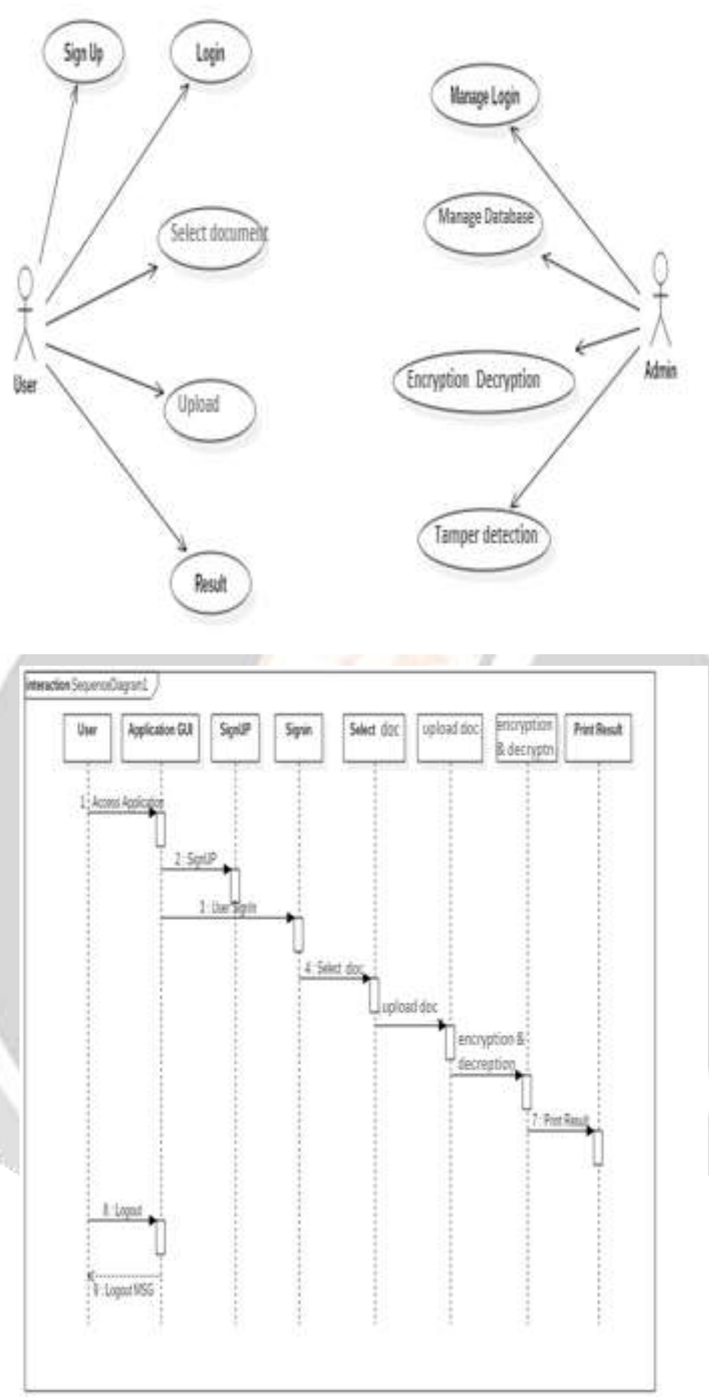
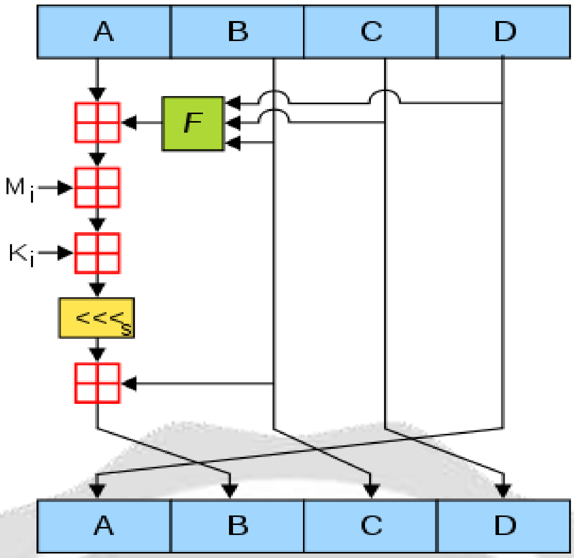


Fig: Use case diagram and sequence diagram

VI. ALGORITHMS USED

-MD5 is used for calculating hash value.
-DSS used for verification and encoding hash value.

i.MD5 WORKING



ii. DSS WORKING

-SERVER SIDE:

-Global public key components:

-p=prime number=2^L-1<p<2^L (L=length)

-q-prime divisor

-g=[h^(p-1)/q] mod p

-h any integer 1<h<p-1

-User private key

-X-random number 0<x<q

-User public key

-Y=[g^x]mod p

-K=any integer 0<k<q(secret number)

-Signature:

-r=[(g^k)mod p] mod q

-S=[k'(h(M)+x*r)]mod q

-H-hash of original file

-R and s appended to original file

-RECEIVER SIDE:

-v=[(g^u1)(y^u2)mod p]mod q

-u1=[H (M') w]mod q

-u2=[(r')w]mod q

-W=[(S')^-1]mod q

-Verification: v==r'

(S denotes sender side and S' denotes receiver side)

VII. ADVANTAGES

It uses two powerful algorithms namely-MD5 and Digital Signature together to detect tampering. It makes sharing and storing of online documents safe and secure.

VIII. CONCLUSION

We need security for handling sensitive online documents .Digital signature algorithm used together with MD5 algorithm enables document tamper detection along with user authentication.

In the future we are planning to compute an algorithm that can detect the exact affected area of tampering or percent of tampering.

REFERENCES

[1] Jing Lin, Chuqiao Mi and Yuanquan Shi ,"Approach of Tamper Detection for Sensitive Data based on Negotiable Hash Algorithm" 2012 International Conference on Computing Sciences.

[2]Xiaoyun Wang and Hongbo Yu,"How to Break MD5 and Other Hash Functions".

[3] Jing Lin*, Chuqiao Mi, Yuanquan Shi ,"Approach of Tamper Detection for Sensitive Data based on Negotiable Hash Algorithm."

[4] Cryptography and Network Security Principles and practices, William Stallings, Pearson Education, Fifth Edition.

[5] Fundamentals of Network Security, Artech House, London, ISBN 1-58053-176-8, John E. Canava (2001).