ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Implementation of Digital Signature Using Date Time Keyed HMAC Algorithm

Madhuri Mali, Prof. Santosh Waghmode

Student, Dept.of Computer Science JSPM's Imperial College of Engg. And Research, Wagholi, Pune, India

Assistant Professor, Dept. of Computer Science JSPM's Imperial College of Engg. And Research, Wagholi, Pune, India

ABSTRACT: Nowadays for document security methods, digital signatures can be used more securely. However, the documents authenticity has not been assure by the presence of frequent digital signatures. Government and enterprise settings often need to impose additional constraints on their signature workflows, such as restricting the choices of users and behavior of document during and after signing.security of Computer network addresses several problems, namely data secrecy, integrity, authentication and digital signature problems. Secret and reliable data communication between two communicating entities are dealing with problems like data secrecy and integrity. On the other hand, the identity proof among the users of the network are dealing with the problems of authentication and digital signatures. Identity proof is allowed by authentication to the peer entity whereas identity proof are allowed by digital signatures to anyone. The existence of a trusted third party is assumed by most of the authentication and digital signature protocols either as an authentication server or certification authority. However, security and fault intolerance bottlenecks within the protocols have been created by both servers and authorities. By combining a secret sharing scheme with authentication and digital signature protocols This problem can be solved. To combine a secret sharing scheme with the authentication and digital signature protocols and proposes a draft solution there are difficulties which are described by this problem definition.

I. INTRODUCTION

Time management is the most crucial and more focused aspect in the modern business processes which is taken under consideration at high priority in order to meet the business targets. Having timely deliveries and secured transportation in the business processes is the main aspect of most of the large scale organizations and product manufacturing companies. Goals and profits of the company leads to achieve this approach. But, to achieve all these goals and targets, some business intelligence techniques must apply by an organization that help them to keep track of their work and processes. One of the important key aspects that every organization must have taken into consideration is security. Very high level security is required for many documents,transactions and business deals as the huge amount of time and money is invested to develop a successful business. To prevent the loss caused by theft, intrusion etc. documents of such large organizations are always protected and kept safe.Some modes such as sealed envelopes and signatures are authenticate and protect all of these documents. It has become a common practice to fulfill the documentation process digitally in modern era in order to avoid the time loss and maintain security as well as confidentiality. With the help of digital documents, all the business processes are executed which provide timely results and implement advanced business intelligence. Most of the giant organizations all over the world implemented this system as it is the powerful and advanced ERP tool.

All the technical and functional tools which are required to run the business at a very large scale are provided by it. In this paper we are proposing an implementation method for logistics process and digital signature implementation in this logistics process for the authentication of documents in proposed system.

Supply chain management have logistic management as its part that plans, implements, and controls the efficient, effective forward, and reverse flow and storage of goods, services, and related information between the point of origin and the point of consumption in order to meet customer's requirements. Dedicated simulation software manages the complexity of logistics and can be model, analyze, visualize, and optimize it. A common motivation in all logistics

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

fields is the minimization of the use of resources. Logistician is nothing but a professional working in the field of logistics management

Significance of Logistics

Logistics management is one of the critical activities of businesses and forms the crux of entire dealings. In the highly competitive world of today, a quality Logistics management service keeps your company ahead of your competitors and gives you the extra edge needed to stay ahead. It is important to understand the requirement of clients first and then act accordingly. No two clients are the same and thus the entire procedure of planning, execution and processing completely differs from one customer to another.

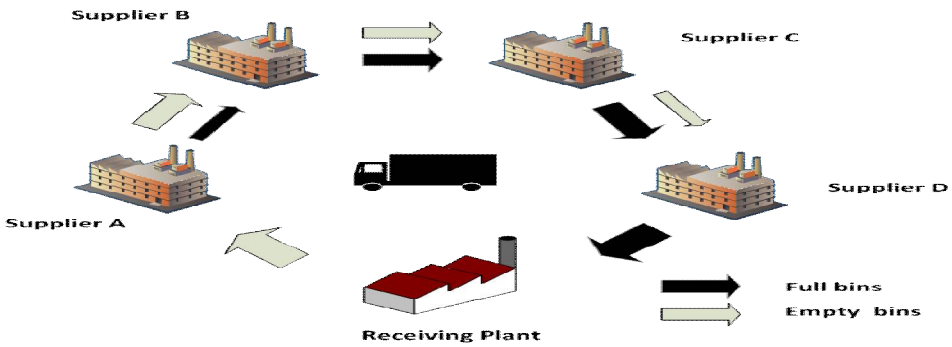

Figure 1.1: Process flow of logistics system

Digital Signature

Using a form of asymmetric cryptography digital signatures are generated which makes use of key pairs i.e. Public Key and Private Key. The Private Key is kept secret while The Public Key may be distributed to anyone who needs it.
The owner of the Private Key generates signatures and the event of signing while anyone with the sender's Public Key can verify that an authentic signature event took place.

II. EXISTING SYSTEM

There is no direct provision for checking, authenticating and preparing the Gate Pass system in the current system which allows secure and reliable logistics services. To keep the track of all the vehicles and the goods is a tedious job they carry from production plant to the consumer or from inventory to the supplier viz[3][4].

The primary benefit promised by elliptic curve cryptography. It is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key: for example, a 256-bit elliptic curve public key should provide comparable security to a 3072-bit RSA public key.

Disadvantages of Existing System
Secure and reliable logistics services are allows no direct provision for checking, authenticating and preparing the Gate Pass system. To keep the track of all the vehicles and the goods they carry from production plant to the consumer or from inventory to the supplier is a tedious job.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

III. PROPOSED SYSTEM

Using digital signature in the proposed system, user does not need to wait at the gate to clear the entry or exit at the gate for long time and for the transport of goods from one plant to another plant or inventory, secure authentication is needed. We are using RSA-based system in our proposed system with a large modulus and correspondingly larger key: for example, a 256-bit elliptic curve public key should provide comparable security to a 3072-bit RSA public key.Asymmetric cryptography is implemented by digital signatures which is also called a public key cryptography. Implementing a public key algorithm like RSA(Rivest-Shamir-Aldeman), we can generate two keys that are mathematically linked, one private and one public.Signing application creates a one-way hash of the electronic data to be signed to create a digital signature. Private key is used to encrypt the hash. Along with hashing algorithm,the digital signature is in this encrypted hash. Hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. Since hashing is much faster than signing it saves time.

.

IV. SYSTEM OVERVIEW

Modified RSA Algorithm :

Choose p , q and r are three odd prime numbers.
Compute n = p * q * r where n is a positive integer.
Compute φ(n) = (p - 1) * (q - 1) * (r - 1)
Choose e such that 1 < e < φ(n) and e and n are coprime.
Compute a value for d such that (d * e) % φ(n) = 1.
Compute X (to replace n)
• If p>q then consider X such that
n− p < X < n and GCD(X , n) = 1
If p<q then consider X such that
n − q < X < n and GCD(X , n) = 1
Public key is (e, X)
Private key is (d, X)

Date Time Keyed - HMAC ALGORITHM:

Unlike conventional HMAC, the DTK-HMAC implemented in this project, the hashing of the message is done using communication and user specific details i.e Date, Time and the Key information and thus DTK-HMAC scheme is not dependent on the message alone. It focuses on both Data integrity and Data Origin Integrity assurance. The communication specific details include the data and time information and the user specific detail include the secret key shared between the communicators.

HMAC Algorithm :

- Step 1 : The message is padded with zeros to enable the division of message into N (r * 8) bits block i.e. N 64 bits block .
- Step 2 : Each 64 bits block is further divided into r bits block.
- Step 3 : Each 64 bits block as whole is the input for mod process and r bits output is obtained.
- Step 4 : Bit swap is performed around the center .
- Step 5 : If N is odd r zeros i.e. 8 zeros are appended. Now we will have either N or N + 1 r bits block.
- Step 6 : Xor operation between the blocks is done in the order, first last, second second-last.... is done.
- Step 7 : Now we will have M r bits blocks i.e. M 8 bits block.
- Step 8 : If M > 1, mod process is called again over the remaining M 8 bits block and final 8 bits is obtained. The final 8 bits obtained is the final mod process result, R. If M < 1,
- R is the the final bits of previous step.
- Step 9 : Calculate Hashing Constant R.
- Step 10 : Calculate Hash Value using the hashing constant

Time Update Algorithm :

If send = a and rec = b{X = Xb - Xa
if 0 < x <20

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Y = 5}
If send = b and rec = c {X = Xc - Xb
if 0 < x <20
Y = 2 }

V. RESULTS

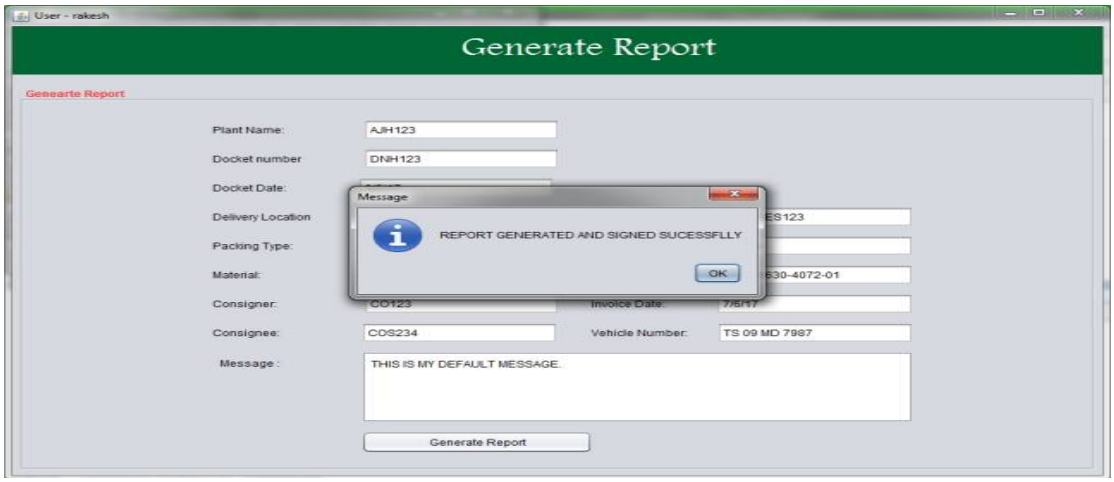

Fig.1 USER 1 (Manufacturer Side UI)

USER 1

1) Inputs some data in fields and message.
2) Encrypt using public key of receiver (user2).
3) Signs document with his own private key for signature generation data from all fields is used.
4) Report is generated in pdf format.
5) Default message : THIS IS MY DEFAULT MESSAGE.

Generate report and sign it
Report with generated message by sender encrypted in pdf:
Sample pdf file msg is encrypted and signature is appended at the end.
This system contains snapshots of overall project.

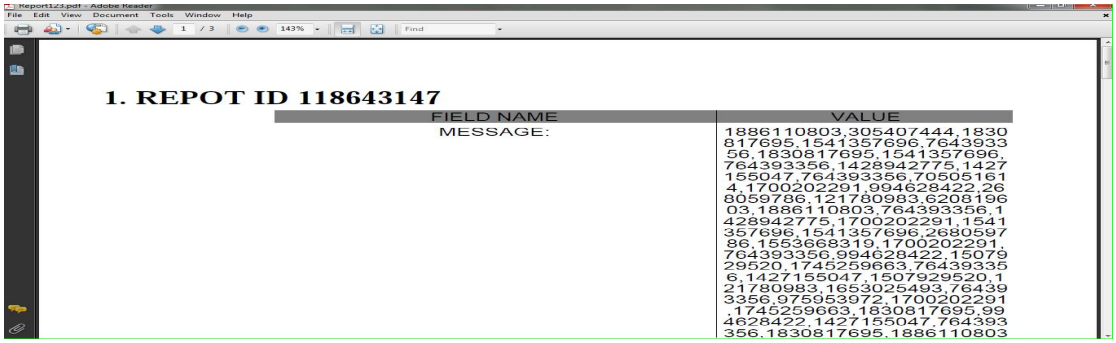

Fig.2 Generated Report

1. Generate report and sign it
2. Report with generated message by sender encrypted in pdf:
3. Sample pdf file msg is encrypted and signature is appended at the end

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

USER 2 :
Verify the document

1) Default name of file is report123.pdf
2) Verify button will
    1) First authenticate if document is sent by USER 1 or not
    DATA=For that document encrypted is first decrypted using his own (USER 2) private key
    DATA1=After that signature appended is applied on by public key of USER 1

    If (DATA==DATA1)
    DOCUMENT SIGNED BY USER 1
    Else
DOCUMENT NOT SIGNED BY USER 1

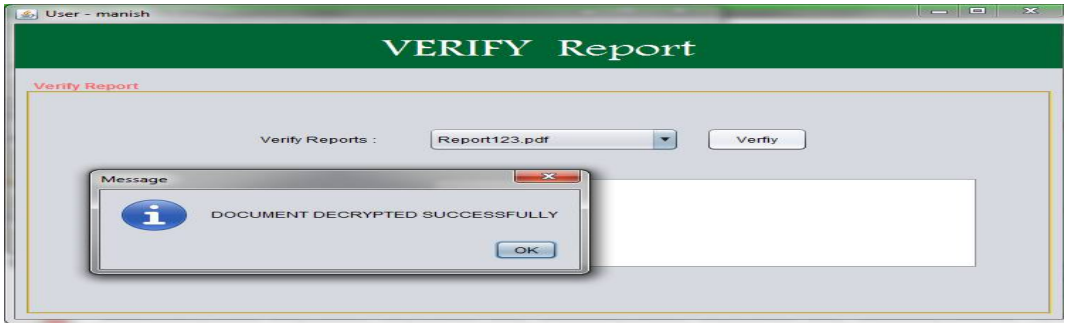

Fig. 3 Verify the Report

USER 2 :
Verify the document

3) Default name of file is report123.pdf
4) Verify button will
    2) First authenticate if document is sent by USER 1 or not
    DATA=For that document encrypted is first decrypted using his own (USER 2) private key
    DATA1=After that signature appended is applied on by public key of USER 1
    If (DATA==DATA1)
    DOCUMENT SIGNED BY USER 1
    Else
    DOCUMENT NOT SIGNED BY USER 1

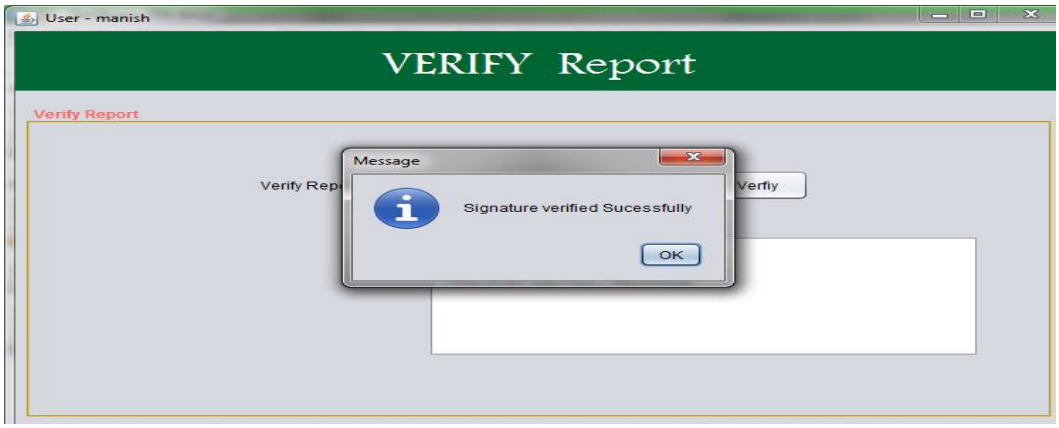

Fig. 4Signature validate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

1) Data integrity is checked to verify data is not modified during transfer.
2) ALL success then original MSG is SHOWN.

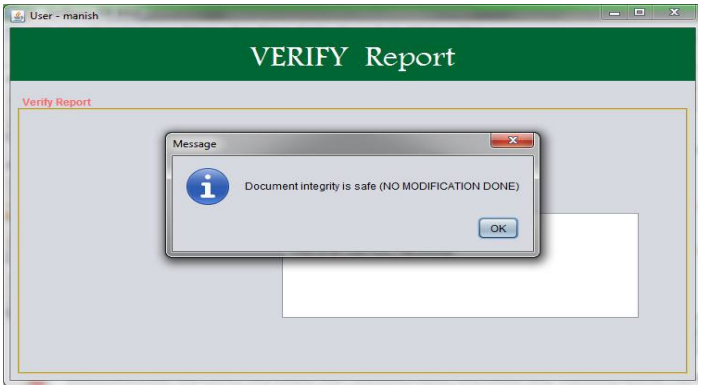

Fig. 5Data integrity checking

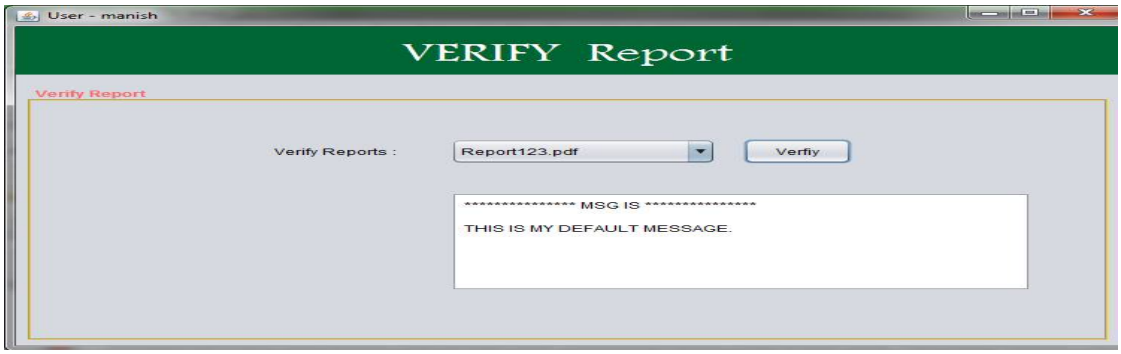

Fig. 6Data integrity Verify

also a pdf is generated which consist of original msg obtained after decryption and digital signature verification status. i.e shows signature verified successfully.

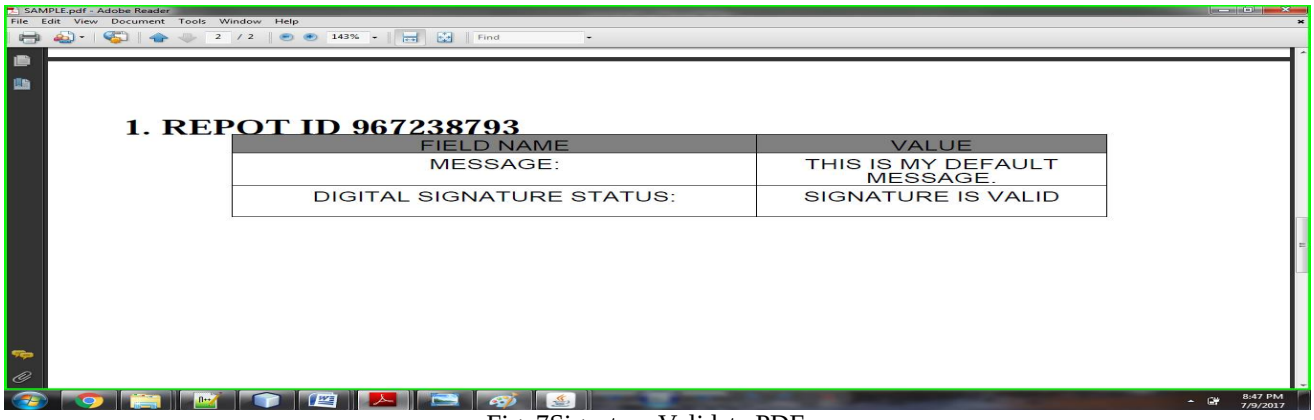

Fig. 7Signature Validate PDF

A PDF is generated which consist of original message obtained after decryption and digital signature verification status that is it shows signature verified successfully.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

VI. CONCLUSION

Form the analysis and study of the current logistics system implemented in current systems, we came to the conclusion that this proposed system can be improved for optimum performance in terms of time management, reliability and security in the field of logistics by implementing digital signature technology at the gate pass entry process. our system will provide data integrity is checked to verify data is not modified during transfer. original message is shown i.e not altered and also a pdf is generated which consist of original message obtained after decryption and digital signature verification status. i.e shows signature verified successfully.

ACKNOWLEDGMENT

With an immense pleasure and satisfaction, I am presenting this Implementation Paper as part of the curriculum of M.E. Computer Engineering. I wish to express my sincere gratitude towards all those who have extended their support right from the stage this idea was conceived. I am profoundly grateful to Prof. S. T. Waghmode, Project Guide, for his expert guidance and continuous encouragement throughout to see that project work rights its target since its commencement to its completion. I am thankful to Prof. Madhavi S. Darokar, Coordinator, ME (Computer Engineering), for supporting such research activities. I am also grateful to Prof. S.R. Todmal, HOD, Department of Computer Engineering, for his support and encouragement.
Finally, I am also grateful to Honorable Dr. Prof. D.D. Shah, Principal, JSPMs Imperial College of Engineering & Research, Wagholi, Pune, for his support and guidance that have helped me to expand my horizons of thought and expression.

REFERENCES

[1] "A Modified Signcryption Scheme using Elliptic Curve Cryptography", Anuj Kumar Singh, Special Issue on International Journal of Recent Advances in Engineering & Technology, 2016
[2] F.E.S.,Dunbar, 2002. Digital Signature Scheme Variation, presented in University of Waterloo.
[3] Solomon, M.M. (1987), "Algorithms for vehicle routing and scheduling problems with time window constraints", Operations Research, 35(2): 254–265.
[4] Z.,Liu, Y.,Hu, X.,Zhang, H.,Ma, 2010. Provably secure multi-proxy signature scheme with revocation in the standard model. Elsevier journal of computer Communications.
[5] Iuon-Chang Lin; Chin-Chen Chang, 2008,"A Novel Digital Signature Scheme for Application of Document Review in a Linearly Hierarchical Organization", International Conference on Intelligent Information Hiding and Multimedia Signal Processing.
[6] Hongjie Zhu, Daxing Li, "Research on Digital Signature in Electronic Commerce",Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21March, 2008, Hong Kong.
[7] L. Harn, Batch verifying multiple RSA digital signatures
[8] Tang Liansheng; Xu Huajie;NongXia,"Notice of Retraction Automotive supply chain logistics cost management research", Computer and Communication Technologies in Agriculture Engineering (CCTAE), 2010.
[9] George Thiers; Leon McGinnis, "Logistics systems modeling and simulation",Simulation Conference (WSC), 2011.