International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-2, December 2014

A Study on Online Contract Signing Protocols

Rakhi R. Naidu, Sweety S. Nawale, Neha P. Pawar, Preeti R. Sharma, Rajashree R.S

Abstract- Security services becomes crucial to many applications such as e-commerce payment protocols. Online contract signing protocol is fair as it allows two users to exchange their digital signatures in a secure manner such that both the users remain loyal to the transaction. The trusted third party is involved only in the situations where one party is cheating other or the communication channel is interrupted. Also, if the protocol is executed unsuccessfully, none of the parties can show the validity of intermediate results to others. As more business is conducted over the internet, the fair-exchange problem is gaining greater importance. In this paper, we make a comparative study of different online contract signing protocols and give the best efficiency results

Keywords- Fair-exchange protocols, TTP, digital signatures, security.

I. INTRODUCTION

Contracts play an important role in many business transactions. Traditionally, paper-based contracts were signed by the transacting parties who need to be present at the same venue and at the same time. Each party signs a copy so that every party has a copy of the singed contract. Along with this one contract copy needs to be submitted to the legal authority. Is the parties however, are not able to meet to sign the paper-based contract, then the transaction delays which may cause time and financial loss.

An alternative found to the above problems came up with rising usage of internet and every field going online. An electronic contract is an alternative. They deal with active usage of digital signatures as a token for authentication of users. A digital signature is a piece of information that is sent along with the message and can be generated only by the sender. Everyone (including the receiver) can verify this digital signature and make sure about the origin of message. By this way, the sender cannot later repudiate sending the message. Therefore, non-repudiation is achieved by digital signatures. [5]

Online Contract Signing works in an efficient way as follows *[2]:*

Let's say that the contract is to be signed between two users, User1 and User2, We are dealing with the authentication of the users and then exchanging the contract User1 registers itself with the certificate authority (CA) and then the Trusted third party (TTP).

Manuscript published on 30 December 2014.
* Correspondence Author (s)
Miss Rakhi R. Naidu, Student, Department of Computer Engineering, PCCOE, Pune India.
Miss Sweety S. Nawale, Student, Department of Computer Engineering, PCCOE, Pune India.
Miss Neha P. Pawar, Student, Department of Computer Engineering, PCCOE, Pune India.
Miss Preeti R. Sharma, Student, Department of Computer Engineering, PCCOE, Pune India.
Mrs. Rajashree R.S, Assistant Prof. Department of Computer Engineering, PCCOE, Pune India.

User1 will encrypt the partial signature and then sends the encrypted signature to user2. User2 will then verify the encrypted signature and if it is correctly verified, sends his signature to User1. If User1 finds that User2's signature is correct then it will send the decryption key to User2 to decrypt his encrypted signature. If User1 fails to send the decryption key, User2 will contact TTP to recover the decryption key. A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure, a CA checks with a registration authority to verify information provided by the requests of a digital certificate. If the registration authority verified the requester's information the CA can then issue a certificate Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name and the other information about the public key owner[5].

II. LITERATURE SURVEY

Compared to a protocol using online third party the optimistic approach greatly reduces the load on the third party, which in turn reduces the cost and insecurity involved in replicating the service in order to maintain availability.

A. Verifiable Escrows-Based Protocol[13]

The verifiable escrow based protocol is a fair protocol that allows two users to exchange digital signatures so that either each user gets the other's signature or neither does [3]. This protocol ensures timely termination for fair exchange. A trusted third party is needed only in cases where one user crashes or attempts to cheat. Here the trusted third party is used as an "escrow service". The basic idea is that Alice, the initiator, encrypts her signature under the public key of the trusted third party. So Bob, the responder, can have it decrypted by the trusted third party. Together with the escrow scheme a standard "cut-and-choose" interactive proof is used which makes it verifiable. In the sense that the user who escrows can verify that it is indeed the escrow of a signature of the desired form with a correct condition attached. This protocol makes use of three sub protocols: an abort protocol for the initiator, a resolve protocol for the receiver and a resolve protocol for the initiator. The protocol can also be used to encrypt data for maintaining data integrity while it is exchanged through the internet.

B. Park et al's RSA-Based Multisignature Protocol [14]

For e-commerce applications the fair exchange must be assured. In this protocol a method of constructing an efficient fair-exchange protocol by distributing the computation of RSA signatures is described.

By using the features of multisignature model[2], the protocol is constructed that requires no zero-knowledge protocol, so the computation can be reduced. Only in the protocol setup phase, the use of zero-knowledge proof's are needed. In this approach fairness is ensured by splitting an RSA private key into two parts. The signer holds both parts while the TTP holds just one of the parts [10].

C. Generic Fair Non-Repudiation Protocols with Transparent Off-Line TTP [11]

In non-repudiation service evidences need to be generated, exchanged and validated via computer networks. After the completion of such a transaction each involved party should obtain the expected items. If any dishonest party denies his/her participation in a specific transaction, others can refuse such a claim by providing electronic evidences to a judge. This non-repudiation protocol is a generic fair protocol with transparent off-line TTP [10] using the same principle. At the end of this protocol execution, either both parties obtain their expected items or neither party does, hence is said to be fair.

D. Bao et al's Fair Contract Signing Protocol [15]

In contract signing protocol two mutually distrusted parties exchange their commitments to a contract in a fair way such that either each of them can obtain the other's commitment, or neither of them does. A practical and efficient approach for fair contract signing is using an invisible trusted third party. This contract signing protocol preserves fairness while remaining optimistic in the sense that the trusted parry need not be involved in the protocol unless a dispute occurs. The protocol is a generic scheme since any secure digital signature scheme and most of secure encryption algorithm can be used to implement it.

E. An Abuse-free Fair Contract Signing Protocol Based on the RSA Signature [5]

A fair contract signing protocol[9], [5] allows two mistrusted parties to exchange their digital signatures to an agreed contract, here for achieving fairness the private key of the initiator is split into two parts and the TTP holds one part which is kept secret. The initiator holds both part of the private key. The digital contract signing protocol is based o the RSA signature and it is optimistic since the trusted third party is involve only in the situations where one party is cheating or the communication channel is interrupted. Furthermore, if the protocol is executed unsuccessfully, none of the two parties can show the validity of intermediate results to others.

III. ALGORITHMS

A. *RSA (Rivest, Shamir & Addlema)* [5]

RSA algorithm [7] is a cryptosystem for public key encryption, and is widely used to securing sensitive data particularly when being sent over an insecure network such as internet.

Algorithm.

1).Enter p and q such that p and q are co-primes to each other.

2)Calculate n such that n=p*q

3) Calculate value of z whi9ch is totient of n.

Z= (p-1)*(q-1)

4) Calculate e such that, 1<e<z

5) Calculate d such that,

(d*e) mod z=1

6) Public key is (e, n)

7) Private Key is (d, n)

Hash Algorithm

Hash algorithm is an algorithm which is used to so compute a data fingerprint of a data block. It is a one-way function which satisfied the following condition.

1) Can receive data wi9th any length

2) Can produce abstracts with fixed length

3) Can compute abstract easily.

4) Cannot compute message from abstract.

It is impossible to find two different messages which have same abstract.

Hash function can make short abstract with fixed length for the binary data with any length. The popular hash algorithms are MD5, Secure Hash Algorithm (SHA, having all kinds of security levels).

SHA (Secure Hash Algorithm)

SHA encryption is a series of five various cryptographic functions and this presently has three generations, SHA-1, SHA-2, and SHA-3.

The first SHA generation is SHA-1 and it is the fundamental 160-bit hash function, SHA-1 appears similar to the former algorithms MD5.

MD5 (Message Digest) algorithm

Algorithmic steps

1. Append padding bits

The input message is "padded" (extended) so that its length (in bits) equals 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512. Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448 mod 512. At least one bit and at most 512 bits are appended.

2. Append Length

A 64-bit representation of the length of the message is appended to the result of step1. If the length of the message is greater than 2^64, only the low-order bits will be used. The resulting message has a length that is an exact multiple of 512 bits. The input message will have a length that is exact multiple of 16(32-bit) words.

3. Initialize MD Buffer

A four –word buffer (A, B, and C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal lower-order bytes first:

Word A: 01 23 45 67

Word B: 89 ab cd ef

Word C: fe dc ba 98

Word D: 76 54 32 10

4. Process Management in 16-word blocks

Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

F(X, Y, Z) =XY or not (X) Z
G(X, Y, Z) = XZ or Y not (Z)
H(X, Y, Z) = X xor Y xor Z
(X, Y, Z) =Y xor (X or not (Z))

IV. MERITS AND DEMERITS OF DIFFERENT PROTOCOLS [6]

Protocols	Merits	Demerits
Verifiable Escrows Based Protocol	1. Intervention of TTP is reduced. 2.Implementation of common signatures scheme without modification ,RSA	1.Increased computation due to use of zero knowledge proof 2 .Inefficient as it is expensive.
Park et al's RSA-Based Multisignature Protocol	1. Multisignature compatible with std. signature scheme. 2.No zero-knowledge proof hence increase in efficiency	1. Insecure as TTP can derive private key. 2. No Abuse-freeness.
Generic Fair Non-Repudiation Protocols with Transparent Off-Line TTP	1. Each Party can use different signature schemes. 2. Non-Repudiation and fairness achieved.	1. Statelessness of TTP is not achieved.
Bao et al's Fair contract signing Protocols	1. Greater efficiency as only basic cryptographic operations required. 2.Fairness	1. Weak timeliness due to usage of deadlines
An Abuse Free Fair-Contract Signing Protocol	1. Abuse-freeness as RSA scheme is intractable. 2. Support Electronic transactions.	1.Increased Communication overhead

V. COMPARISON TABLE OF DIFFERENT PROTOCOLS [12]

The table [8] shows the comparison of different parameters that are used by different protocols. Some of the parameters for comparison are Fairness, Timeliness, Transparent TTP, No. of messages, TTP;s statelessness. In the category of basic features, the properties such as transparent TTP [10] or not, off-line TTP or on-line TTP are considered. Here two main security requirements are compared: Fairness and timeliness. In the efficiency evaluation the costs of communication is compared. Various types of TTP can be considered according to their involvement in the protocol. Online TTP- A TTP involved during each session of the protocol but not during each message transmission, is said to be online [6].

Parameters	Verifiable Escrows Based Protocol	Park et al's RSA Based Multisignature Protocol	Generic Fair Non-Repudiation Protocol	Bao et al's Fair Contract Signing Protocol
Fairness	Yes	Yes	Yes	Yes
Timeliness	Yes	Yes	Yes	Yes
Transparent TTP	No	Yes	Yes	Yes
No. of message	4	3	3	3
TTP's statelessness	No	Yes	No	No

REFERENCES

[1] Abdullah M. Alaraj "Optimizing One Fair Document Exchange Protocol "International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012 DOI : 10.5121/ijnsa. 4101 1 , 2012.
[2] Alptekin Kupcu and Anna Lysyanskaya, "Optimistic Fair Exchange with Multiple Arbiters", Brown University, Providence, RI, USA,2008.
[3] H.Jayasree1 and Dr. A.Damodaram "A Novel Fair Anonymous Contract Signing Protocol for E-Commerce Applications" 2012 International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.
[4] Alfin Abraham, "An Abuse-Free Optimistic Contract Signing Protocol with Multiple TTPs", IJCA Special Issue on "Computational Science – New Dimensions & Perspectives" NCCSE, 2011.
[5] Guilin Wang "An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1, March 2010.
[6] Alfin Abraham "A Survey on Optimistic Fair Digital Signature Exchange Protocols" , International Journal on Computer Science and Engineering (IJCSE),Feb 2011
[7] K.P. Thooyamani, R. Udayakumar and V. Khanaa "A Novel Ruin Gratis Fair Digital Contract Signing Protocol Based on Rsa Signature", School of Computing Science, Bharath University, Chennai-73, India
[8] Abdullah M. Alaraj "Simple and Efficient Contract Signing Protocol " (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012 67
[9] N. Asokan Victor Shoup Michael Waidner "Optimistic Fair Exchange of Digital Signatures", IBM Zfirich Research Laboratory, S~umerstr. 4, 8803 Rfischlikon, Switzerland.
[10] V.SWAPNA KUMARI, C. SREEDHAR "Efficient and Fair Exchange of Digital Signatures Based on RSA Algorithm", V Swapna Kumari et al ,Int.J.Computer Technology & Applications,Vol 3
[11] G. Wang, "Generic non-repudiation protocols supporting transparent off-line TTP," J. Comput. Security, vol. 14, no. 5, pp. 441–467, Nov. 2006.
[12] Sumit Kumar Pandey1, Umesh Lilhore2 "A Review on Various Contract Signing Protocol" , International Journal of Emerging Technology and Advanced Engineering, Issue 8, August 2014
[13] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 591–606, Apr. 2000.
[14] J. M. Park, E. Chong, H. J. Siegel, and I. Ray, "Constructing fair exchange protocols for e - commerce via distributed computation of RSA signatures," in Proc. PODC'03, 2003, pp. 172–181, ACM Press.
[15] F. Bao, G. Wang, J. Zhou, and H. Zhu, "Analysis and improvement of Micali's fair contract signing protocol," in Proc. ACISP'04, 2004, vol. 3108, LNCS, pp. 176–187, Springer-Verlag.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)