IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Abuse Free Fair Contract Signing Protocol

Aiswarya.V[1], R. Priyanka Raj[1], Reshma.S[1], Sreeka.S.Mohan[1], Remya.R[2]

Student, Information Technology, College Of Engineering Perumon, Kollam, India[1]

Assistant Professor , Information Technology, College Of Engineering Perumon, Kollam, India[2]

Abstract: A fair contract signing protocol allows two potentially mistrusted parties to exchange their commitments to an agreed contract over the Internet in a fair way so that either each of them obtains the others signature or neither party does. The existing protocols face the problem of more number of transactions in between TTP and party. Also the time complexity and computational complexities are more. In this paper we are proposing a fair contract signing protocol based on secret sharing scheme. The proposed method satisfies property of abuse freeness and fairness. That is if the protocol is executed unsuccessfully, none of the two parties can show the validity of intermediate results to others. The proposed scheme is more reliable, secure and less complex.

Keywords: Fair-exchange protocols, digital signatures, security, privacy preserving, dynamic groups.

INTRODUCTION

Purpose

An abuse free fair contract signing protocol[7],[2],[3], based on the standard RSA signature [6]scheme allows two potentially mistrusted parties to exchange their digital signatures on a contract in an efficient and secure way. Like the existing RSA-based solutions, the new protocol is fair and optimistic, i.e., two parties get or do not get the other's digital signature simultaneously. However, different from all previous RSA based contract signing protocol, the proposed protocol is further abuse free. That is, if the contract signing protocol is executed unsuccessfully, each of the two parties cannot show the validity of intermediate results generated by the other party to outsiders. In other words, each party cannot convince an outsider to accept the partial commitments coming from the other party. This is an important security property for contract signing, especially in the situations where partial commitments to a contract may be beneficial to a dishonest party or an outsider. The main aim of this project is to develop an interface wherein the two parties can interact with the abuse free fair contract signing protocol such that at any point of time they can be free of the thought that the other party is cheating them. The contract signing protocol does not give any results until and unless the entire contract is signed by both the parties and no intermediate results are available to both the parties through which they can get benefited by showing them to the third party. For example, if Bob is looking for a job and he has received two offers from competing companies A and C. Bob prefers to join company C though the offered salary is not so much satisfactory. In contrast, company A promises a higher salary but he does not really like to join it due to some personal reason, such as weather, culture or something else. In this scenario, Bob may first pretend to sign an employment contract with company A. Then, he terminates the execution of the contract signing protocol after he obtained the intermediate results generated by company A. By showing such universally verifiable proofs to company C, Bob may get a higher salary from company C.

MATERIALS AND METHODS

RSA Algorithm

The Rivest, Shamir, Adelman (RSA) scheme is an asymmetric cryptosystem [1]. In RSA system all the users must generate their private key pair (d, n) and kept it in secret and store their public key pair (e, n) in Key Distribution Centre (KDC). The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. For public key encryption sender receives the receiver's public key from the KDC and encrypts the message using the receiver's public key. The receiver uses his private key to decrypt the coded message. The private key is known only to the receiver himself. A method for creating digital signature for the originator of data is to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message. Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid. The digital contract signing protocol described here is based on RSA signature scheme. The members participating in the contract signing generate their own private and public key pair. Encrypt the message using their private key and it is authenticated by decrypting it using the public key.

PROPOSED SYSTEM

In this Project we mainly focus on the problem of digital contract signing. Since a party's commitment to a digital contract is usually defined as his/her digital signature on the contract, digital contract signing is essentially implied by fair exchange of digital signatures between two potentially mistrusted parities. There is a rich history of contract signing (i.e., fair exchange of digital signatures)

DOI 10.17148/IJARCCE.2016.5323

because this is a fundamental problem in electronic transactions. According to the involvement degree of a trusted third party (TTP), contract sign in protocols can be divided into three types: (1) gradual exchanges without any TTP; (2) protocols with an on-line TTP; and (3) protocols with an off-line TTP [2],[3],[4],[5]. Early efforts mainly focused on the first type protocols to meet computational fairness: Both parties exchange their commitments/secrets "bit-by-bit". If one party stops prematurely, both parties have about the same fraction of the peer's secret, which means that they can complete the contract off-line by investing about the same amount of computing work. The major advantage of this approach is that no TTP is involved. However, this approach is unrealistic for most real-world applications due to the following several reasons. First of all, it is assumed that the two parties have equivalent computation resources. Otherwise, such a protocol is favorable to the party with stronger computing power, who may conditionally force the other party to commit the contract by its own interest. At the same time, such protocols are inefficient because the costs of computation and communication are extensive. In fair exchange protocols an on-line TTP is always involved in every exchange.

In this scenario, a TTP is essentially a mediator: (a) Each party first sends his/her item to the TTP; (b) Then, the TTP checks the validity of those items; (c) The party who needs it will send a request to the TTP. (d) The TTP will send the request to the owner of the contract.(e)If the owner accept the request he/she will inform the TTP. (f) On receiving the acceptance the TTP will generate the digital signature using RSA algorithm and encrypt it and stores it in the cloud along with the contract. The proposed system also offers the option of a group. The group will be controlled by a group owner. When any member other than the group owner posts a contract, he will receive a notification and forward the contract to the TTP. The group admin will send SMS alert, regarding the contract, to the group members. The procedure will continue as mentioned earlier. Generally speaking, contract signing protocols with an on-line TTP could be designed more easily since the TTP facilitates each step of exchanging, but may be still expensive and inefficient because the TTP needs to be paid and must be part of every execution. In practice, the TTP is prone to become a bottleneck in the whole system, especially in the situation where many users rely on a single TTP.

RESULTS

The proposed method of Digital Signature Scheme based on the prime factorization and discrete logarithms problem. It is basically asymmetric key algorithm. Digital signatures help to establish Authenticity, Integrity, Non-repudiation and can also provide identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. For purpose of security, proposed scheme improved this problem by using multiple integers (e1, e2, e3…....en) to the primary integer number and increasing difficulty of decryption key.

SECURITY DISCUSSION

Reply Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently attack by the method of attach again and again over key. Here an attacker copies a stream of messages between two parties and replays the stream to other party as a authenticate user. To prevent replay attacks, we use a key that is generated only one in the life cycle of contract signing. Replay attacks will be defeated because the replier cannot know in advance the physiological value the sensor will generate.

Man in the middle attack

During the transmission of data from one party to other party or when the exchange of signatures takes place then the chances of a third party involvement is greater. The algorithm that we have implemented here prevents from such attack since the signatures has been verified by the TTP.

Confidentiality

It refers to the disclosure of the key that has been generated. Suppose one party may disclose his key to the other one and the other may try to attack the other party but using one time private key the session is for a limited time and master key is generated randomly and gets destroyed each time.

Authentication

The authentication property is made sure by the verifying the signatures by both the parties and also by the TTP. Authentication is an important issue when the contract signs between two parties since the chances of attacks are more but here in our technique the authentication is secure.

CONCLUSION

In this paper, based on the standard RSA signature scheme, we proposed a new digital contract signing protocol that allows two potentially mistrusted parties to exchange their digital signatures on a contract in an efficient and secure way. Like the existing RSA-based solutions, the new protocol is fair and optimistic, i.e., two parties get or do not get the other's digital signature simultaneously, and the trusted third party is only needed in abnormal cases that occur occasionally. However, different from all previous RSA-based contract signing protocol, the proposed protocol is further abuse-free. That is, if the contract signing protocol is executed unsuccessfully, each of the two parties cannot show the validity of intermediate results generated by the other party to outsiders. In other words, each party cannot convince an outsider to accept the partial commitments coming from the other party. This is an important security property for contract signing, especially in the situations where partial commitments to a contract may be beneficial to a dishonest party or an outsider.

DOI 10.17148/IJARCCE.2016.5323

Technical details are provided to show that our protocol meets a number of desirable properties, not only those just mentioned.

REFERENCES

[1]. Mr.P.Balakumar, Dr.R.Venkatesan, " Biometrics Based File Transmission Using RSA Cryptosystem". (IJCNS) International Journal of Computer and Network Security Vol. 2, No. 4, April 2010.

[2]. 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.

[3]. G. Ateniese, "Efficient verifiable encryption (and fair exchange) of digital signature," in Proc. ACMConf. Computer and Communications Security (CCS'99), 1999, pp. 138–146, ACM Press.

[4]. F. Bao, R. H. Deng, and W. Mao, "Efficient and practical fair exchange protocols with off-line TTP," in Proc. IEEE Symp. Security and Privacy, 1998, pp. 77–85.

[5]. G. Wang." An Abuse Free Fair Contract Signing Protocol Based on the RSA Signature". In: Proc. of the IEEE Information Forensics and Security vol. 5, march 2010.

[6]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[7]. 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.

DOI 10.17148/IJARCCE.2016.5323