An efficient fairness between parties for contract signing using OTP

Sumit Kumar Pandey
Department of Computer Science & Engineering
N.R.I. Institute of Science & Technology
Bhopal, India
Sumitbpl110@gmail.com

Umesh Lilhore
Department of Computer Science & Engineering
N.R.I. Institute of Science & Technology
Bhopal, India
umeshlilhore@gmail.com

Abstract — Contract signing protocol is a new way of interacting two parties online though communication devices. Since communication is done though internet or media so authentication is required between these parties to check the contract is done between right parties or not. The main aim of contract signing is fairness between parties. Although there are various techniques implemented to provide authentication and fairness between these parties such as by R. Song, but these techniques contains some issues, hence a new and efficient technique is implemented here to provide prevention from various attacks and fairness between parties.

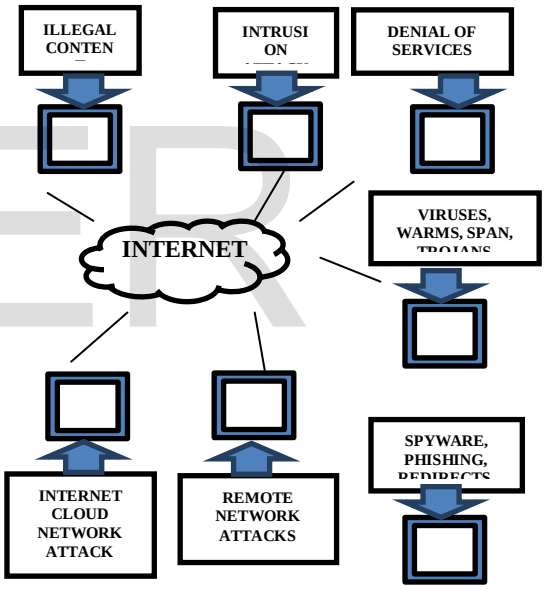
I. INTRODUCTION

Internet is a second world today interconnected through networking technology for exchange of information and data which is personal, military, health, government policies etc. over the whole world. This data can be highly confidential and is needed to be secured. Thus network security must be employed as it is required essentially for securing data exchange and providing easy, reliable and fast communication over the network. Network Security is analyzed with the help of monitoring history of security in networks, architecture of internet and vulnerable security points of the Internet, types of the attacks and security methods for safe browsing and also the development in network security of hardware devices and the software's. The secure network is developed on various criteria's like:

- Access - authorized users can only communicate within a network and outside.
- Confidentiality -the Information in the network is private.
- Authentication- Ensuring that the users are what they say
- Integrity- the message has not been modified.
- Non-repudiation-ensuring that the user should not refuse the usage of network.

The network is vulnerable to multiple type of attacks like connection oriented intrusions, Denial of Service attacks, content based threats such as Viruses, Worms, Trojans, Phishing etc. which is shown here [1]:

Figure 1. Various Attacks on Network



Internet consists of rapidly growing networks and systems which are large, diverse, complex, interconnected etc. The infrastructure is vulnerable due to complexity, accident due to attacks and hostile intent [2]. With the help of authentication protocols network security can be ensured in various ways by generating passwords or authentication keys, protocols etc. ensuring the authenticity of the users. Authentication protocols are base of security in many distributed systems and therefore these protocols should function correctly [3].

Authentication protocols give various techniques for network security in form of OTPK which is a type of protocol in which users generate signing keys and with the help of strong authentication the signing keys are certified and signing the

transaction after which the keys are erased. This is in the form of digital signature which is made and generated as follows for signing a transaction:

- A Message Digest is taken termed as hash through a Message Digest Algorithm like MD5 for the document or transaction that is to be signed.
- The hash is then encrypted with users Private Key.
- This gives the Digital Signature of the user.
- And thereafter on decrypting the Digital signature with public key of user the hash is obtained.

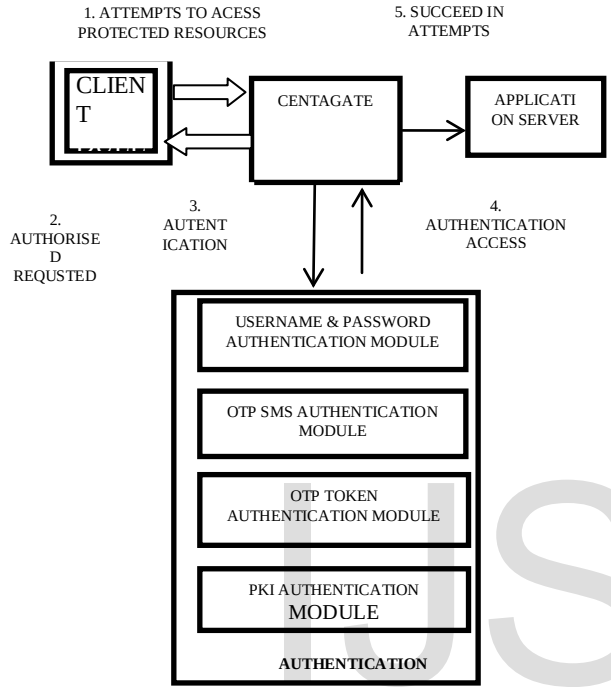


Figure 2. OTPK Process

Contract Signing Protocol explains contract as non-repudiable agreement on a given text. It proves agreement between its signatories to any verifier. The contract signing scheme fairly computes for the situation in which if the signatories misbehaves either both or none of the signatories obtains a contract. Basically two signatories participate in a contract signing protocol in which they use "Sign" which fairly computes a contract this is then used as input to a contract verification protocol and "Show" is used to convince any verifier that the signatories reached agreement on the given text [4].

Properties of Contract Signing:

- TTP (Trusted Third Party)
- Accountability to a TTP
- Fairness
- Non-repudiation
- Completeness
- Confidentiality
- Communication Channel
- Timeliness
- Abuse-Freeness
- Secure digital signature algorithm
- Efficiency

Various contract signing protocols have been like gradual release two party protocol and fixed round protocol. These protocols rely on trusted third party (TTP) this TTP can be used or may not be used as required based on various techniques [5]. Contract Signing Protocol involves:

- Signatories - Contracts must be signed by appropriate and valid signatory.

- Copies- Each party should have their own copy of the contract, with an original signature.

Execution- A contract does not execute until both signatories sign the binding agreement. If one signature is present the contract is partially executed. The second signature is necessary to execute a contract establishing a date for its commencement.

II. LITERATURE SURVEY

A. M. Alaraj [6] et.al. proposed contract signing protocol based on RSA signature scheme signing the contract for exchange of digital signatures which can be a possible exchange or may not. The scheme suggested by them is based on offline Trusted Third Party (TTP) which comes into consideration on failure of signing the contract and if it does not happen it remains inactive. Their proposed protocol consists of three messages that are exchanged between the parties. In their scheme if one party evades during the execution of the protocol, the protocol provides an online resolution for the disputes with the help of TTP making the protocol efficient as it has lowest number of modular exponentiations in exchange protocol [6].

V. M. Vaze [7] et.al. gave the concept, use and benefits of OTPK. They presented that due to smaller computer sizes higher security is being demanded with more enhanced security solutions. They explained that system should be twice safer than previous and should be suitable for hand held devices. One Time Private Key (OTPK) helps user generating their signing keys and certify the signing keys through their strong authentication and thereby signing the transaction and there after the signing keys are erased. They presented that OTPK is a two factor authentication technology which enhances transaction integrity and is difficult for transaction manipulation. They gave the mechanism of OTPK as user can generate a signing key in low cycle time. The concept behind OTPK is that on requirement of digital signature a private key is generated which is certified and is used to compute the digital signature and then deleted immediately. The digital signature and public key certificate from the Certification Authority is then used to verify the digital signature [7].

B. Kordy [8] et.al. gave optimistic multi-party contract signing protocol converting sequence of finite set of signers into protocol specification for signers. The TTP can handle multiple protocols variety as it is independent of signer's role specification. They presented classes of protocols and lower bounds explaining protocols complexity in terms of minimum number of messages and bandwidth. They highlighted connection between contract signing protocol and constructing sequences containing permutations of a finite set in the form of subsequences improving the efficiency through generalized notion of fair signing sequences [8].

Guilin Wang [9] et.al. explained the concept of contract signing protocol which allows the parties to obtain their signatures or no party is able to obtain the signatures. They proposed digital contract signing protocol based on RSA signature which provides optimization through involvement of third party in case of communication channel interruption or a non trusted party. Their proposed protocol scheme provides abuse freeness which restricts the parties to show validity of intermediate results which act as output on unsuccessful execution of protocol providing security and efficiency. Through this partial commitments are not allowed to accept by the outsider that may be important for dishonest party. This is explained as during the transaction the product is only delivered when the amount has been paid [9].

Mijin Kim [10] et.al. remarked the authentication and confidentiality of transmitted data for establishment of secure communications. They explained the use of one time password authentication (OTPK) which involves less computation and overcomes the limits of mobile devices. OTPK makes unauthorized access to restricted resources difficult. They discussed Kuo-Lee's one time password authentication scheme which withstands replay attack, theft attack and modification attack making the attacker impossible to log into the system. Their proposed scheme resolved the security flaws in Kuo-Lee's scheme by determining the flaws in Kuo-Lee's scheme which does not achieved its security goal of authenticating communicating entities by enhancing the scheme [10].

K. G. Paterson [11] et.al. suggested that with the help of one time passwords phishing and spyware attacks can be prevented or the damage can be limited. They explained that users have many passwords but each password can be used only once and even if a password is compromised it can cause damage only single time. They recognized the practical problem of sophisticated phishing attack in present approach and suggested a treatment for it with the help of password authenticated key exchange (PAKE) allowing mutual authentication, session key agreement making it resistance to phishing attacks. They proposed pseudo randomly generated and time dependent passwords for more security as a spyware can terminate the connection and send one time password to the attacker which can then cause harm. This can be overcome by using time dependant passwords by expiration features and procedures for passwords. They basically presented a one-time PAKE protocol for secure use of one time passwords [11].

B. Daya [12] et.al. explained the importance of network security in the field of organizations, military, space, personal computers etc. and with the help of history of security more better security technology can emerge. They stated that modification in internet architecture can reduce attacks being sent over the network. With the help of knowledge of possible attack methods security can be enhanced like using firewalls and encryption methods to secure personal data and services like business etc. securing from multiple possible threats. They studied brief history of beginning of internet and various developments in network security in current technical advancements reviewing various vulnerabilities, knowledge of internet and various attacks and methods. They gave that apart from being software based security technology common hardware are also being used for security purpose. They explained that internet protocol IPv6 provides benefits to internet users on embedding it with security therefore being used for securing intellectual property combining it with security tools like firewalls, authentication etc [12].

III. PROPOSED WORK

The proposed methodology implemented here for contract signing between two parties works in following stages:

1. Registration
2. Signing
3. Encryption
4. Decryption

Stage 1: Registration

Before providing signing between parties needs to be registered on the Certified Authority. The Certified authority in response will generated a token for the new parties through a secure channel or media.

If 'U1' and 'U2' be the two parties for the contract to be signed.

1. U1 (id) → CA
2. U2 (id) → CA
3. CA → Hash (Random) {Token to U1 and U2}
4. CA → count (timestamp → Send (Token) to User

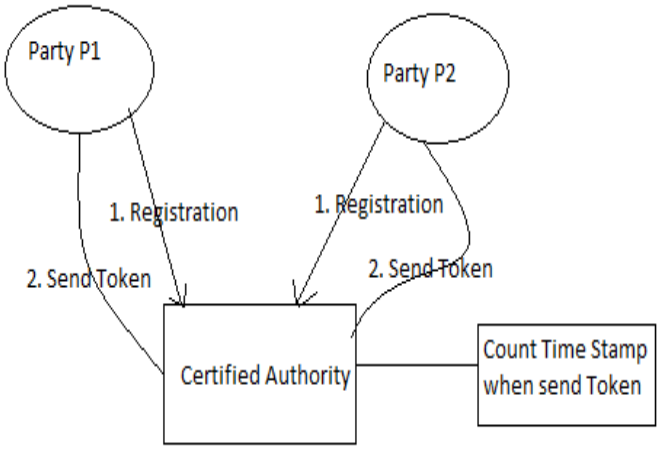


Figure 3. Registration Phase of the methodology

Stage 2: Signing

During Signing of the parties the parties needs to send generated token to the certified authority.

1. U1 (Token) → CA
2. U2 (Token) → CA
3. CA (timestamp) ← User
4. Check the difference of the time stamp between sending token and receiving token.
5. if timestamp > threshold
6. Destroy Token and Send → Error (U1 & U2)
7. else
8. Verifies Token (U1) & Token (U2)
9. Authenticate users and generates Session Key from Token.
10. Session Key (U1) ← Hash (Token)
11. Session Key (U2) ← Hash (Token)

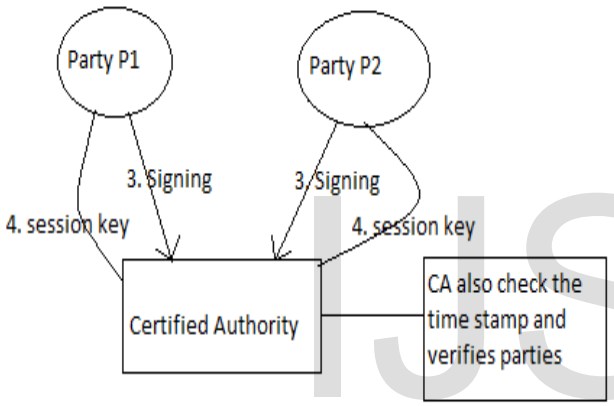


Figure 4. Signing Phase of the methodology

Stage 3: Encryption

After generating Session Key to User (U1), User encrypts the contract with the session key using AES technique.

1. E1=Enc1(session Key(contract)) from user U1
2. E2=Enc2(session Key(contract)) from user U2

The encrypted contract is then send to the second party via secure channel and vice versa.

Stage 4: Decryption

After receiving encrypted contract from both the parties, the encrypted contract is then decrypted using session Keys.

1. Contract=session_key(E1)
2. Contract session_key(E2)

IV. RESULT ANALYSIS

The figure shown below is the comparative analysis of the number of keys generated on the basis of which time stamp is calculated. The existing technique used for the contract signing between two parties takes more time as compared to the contract signing protocol implemented for proposed methodology.

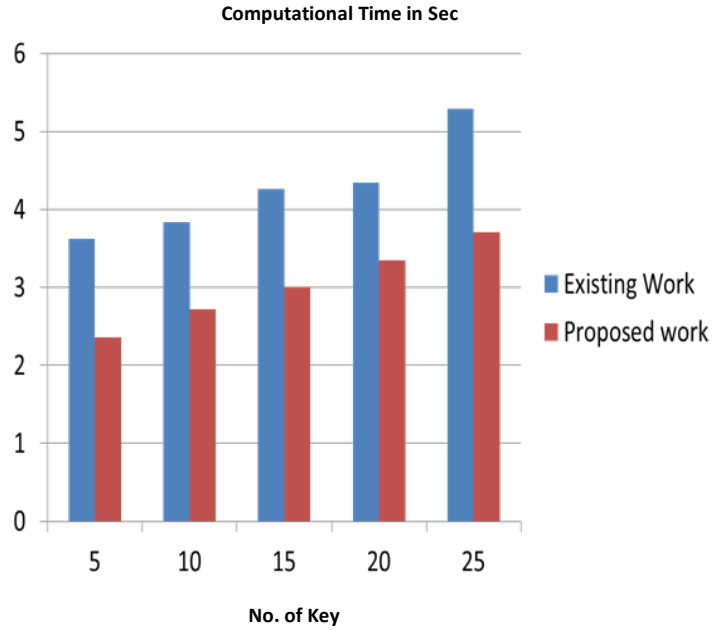


Figure 5. Analysis of Time Stamp

The figure shown below is the comparative analysis of the number of keys generated on the basis of which storage cost is calculated. The existing technique used for the contract signing between two parties takes more time as compared to the contract signing protocol implemented for proposed methodology

Storage Cost

Storage Cost in bytes

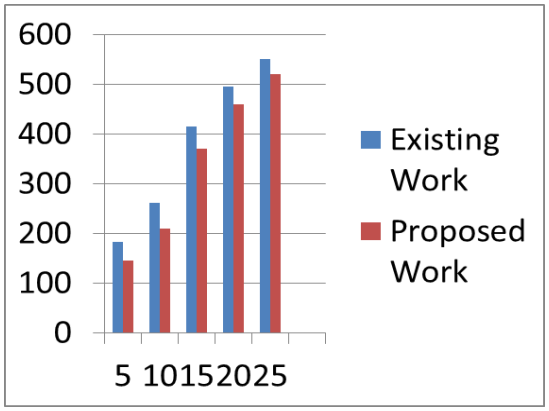


Figure6. Analysis of Storage cost

The table shown below is the attack prevention from various attacks by the existing and the proposed protocol.

Attacks	Existing	Proposed
DOS	No	Yes
DDOS	No	Yes
Identity Disclosure	Yes	Yes
Online/Offline	Yes	Yes
Password Impersonation	No	Yes
Danning Saccho	No	Yes
Public Verifiabilty	Yes	Yes
Confidentiability	Yes	Yes

Table 1. Attack Prevention from various Attacks

The table shown below is the comparison of various protocols used for the contract signing. Here in the table the analysis is done on various parameters such as:

Fairness: Fairness used in contract signing protocol means that that both the parties when finishes contract needs to be satisfied and there is no eavesdropping from both parts.

Timeliness: It is used for the finish of the contract signing in a particular time stamp and there is be no communication overhead.

	Protocols			
Parameters	**Park et. al,'s RSA based protocol**	**Bao et. al.'s Protocol**	**Escrows Based Protocol**	**Proposed Protocol**
Timeliness	Yes	Yes	Yes	Yes
Fairness	Yes	Yes	Yes	Yes
Multiple TTP's	Yes	Yes	Yes	No
Replay Attack	Yes	Yes	No	Yes
Extra Security	No	No	No	Yes

V. CONCLUSION

The methodology implemented here for the contract signing protocol using the concept of one time private key is efficient to use since it prevents from various attacks and also provides free fairness between two parties. The existing technique used here for the contract signing between two parties is efficient but the protocol suffers from timestamp and free fairness and there is no contract data verification. The above issue is resolve in the proposed methodology.

REFERENCES

[1] Bodkhe B, Jain P.,"An Efficient Free Fair Contract Signing Protocol using OTPK", Wireless and Optical Communications Networks (WOCN) Tenth International Conference on, vol., no., pp.1, 5, 26-28 July 2013

[2] Vinod Moreshwar Vaze," Digital Signature on-line, One Time Private Key [OTPK]", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.

[3] Nivedita Datta," Zero Knowledge Password Authentication Protocol", Volume 3, Issue 3, June 2012.

[4]Abdullah M. Alaraj "Simple and Efficient Contract Signing Protocol", (IJACSA) International Journal of Advanced Computer Science and Applications Vol. 3, No. 3, 2012.

[5]LeinHarna,Chu-Hsing Lin "Contract signature in e-commerce", Computers and Electrical Engineering vol.-37, pp-169–173, 2011.

[6] 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.

[7] Ying Zhang, Chenyi Zhang, Jun Pang and SjoukeMauw "Game-Based Verification of Multi-Party Contract Signing Protocols", Formal Aspects in Security and Trust, Lecture Notes in Computer Science, Volume 5983, pp 186-200, 2010.

[8]Mijin Kim, Byunghee Lee, Seungjoo Kim and Dongho Won "Weaknesses and Improvements of a One-time Password Authentication Scheme", International Journal of Future Generation Communication and Networking, 2009..

[9]Kenneth G. Paterson and Douglas Stebila "One-time-password-authenticated key exchange", 2009.

[10]Bhavya Daya "Network Security: History, Importance, and Future", 2008.

[11] G. Wang, "Generic non-repudiation protocols supporting transparent off-line TTP," Journal of Computer Security, vol. 14, no. 5, pp. 441–467, Nov. 2006.

[12] Professor Seymour E. Goodman, Pam Hassebroek, and Professor Hans Klein "Network security Protecting our critical infrastructures", 2003

[13] Birgit Pfitzmann, Matthias Schunter and Michael Waidner "Optimal Efficiency of Optimistic Contract Signing" Symposium on Principles of Distributed Computing (PODC), ACM, 1998.