Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

Implementation of Multifactor Authentication Using Optimistic Fair Exchange

Satheesh M,
Department of Information Technology,
St. Peter's Institute of Higher Education and Research,
Chennai, India.
msatheeshitech@gmail.com

Deepika M,
Department of Information Technology,
St. Peter's Institute of Higher Education and Research,
Chennai, India.
deepikamanickam8@gmail.com,

Abstract: In this work, two participants fairly send or receive things through the aid of intermediate who is only engaged if required. An up-to-date accepted necessity is with the aim of involving third party in the trade should be transparent, to save from privacy and evade terrible publicity. Together, a dishonest intermediate will negotiate the fairness of the trade and so the intermediate should be liable in case of any behavioural changes. Optimistic fair exchange (OFE) is one of the classical protocols to assure fairness of indulgence for a party. This exchange can be done by means of an arbitrator. The most important aspect of OFE is to describe security models so as to capture real-time attacks and design schemes secure in practical models. Signaller is confirmed with the data to send the correct person to address that to make sure it is. Since then the SMS has gone through to achieve that can hold the path to the right to see which if any is the fact that to ensure there is. After the signature is created by creating it to be able to well take care of it and then to the right of the person to pay off that is sure to make it. In this project, to avoid the third party attack (hacking) and unauthorized person access the particular important data. The data should be transmitted in sender to receiver that receiver only have a correct data without any data losses, protect a data security in cyber-attacks. A signature may be digitally and OFE design for the exchanged item have trade-off between transparency and accountability.

Keywords - OFE, Network, Signaller, Message, Add signaller, View signaller , Add arbitrator, View arbitrator, Get trajectory, Find Sybil attack , Signal verification. Triple DES algorithm, Public key, Private Key, Cipher text, Plain text.

1. Introduction

In this article, we are providing authentication to send or receive the information between the participants using Trusted Third Party. During the initial period of recent cryptographic systems, public key cryptography is normally revised in the single-user setting and the security model assumed only one public key. In 1997, Asokan, Waidner and Schunter established the term called Optimistic fair exchange (OFE) as a method to explain the fairness of exchange issues for trusting third party known as “an arbitrator”.

ISSN: 2582-337X (online)

Ubiquitous Computing & Communication Technologies

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

Based on OFE method, the complete signatures which are generated from the signer along with the party produced with the help of arbitrators relying on signaller partial signature to be considered while signaller checks full signatures and represents all signaller commitment on some statements. For those protocols, the arbitrator is employed effectively by the way which involves in working out the conflicts between participants, whereas the most of the Transactions, the arbitrator may not engage in each OFE.

There are two parties for fair exchange method called “Alice and Bob swap” which will not allow other parties to find benefits by suspending in advance or else it will go wrong for one receiver in the public key encryption and one signer in the public key signature. Though, some customers for real-time in addition to the security in the single-user setting will not guard against the attacks by joining dishonest users.

This authentication process is based on the OFE protocol. Here signaller and arbitrator performing the communication. Each party consists of Private Key and Public key, those keys are used for signature verification. And the communication is monitored by the Trusted Third Party Based on these signature verifications communication further take places.

2. Proposed System

The drawbacks which are faced in the existing system can be solved in the proposed system. The proposed system covers the concept of optimistic fair exchange (OFE). OFE takes control of a third party, however there is no constraints to be online for all time; instead, the third party will be occupied if anything goes wrong (for instance, a fault occurs when someone tries to cheat).

The exchange between the signer and the verifier has paid much interest towards various researches carried on OFE, and it is one of the reasons which OFE refers to in the rest of this project. The proposed system will include some cryptographic primitives which will be used in the implementation of Fair OFE for the model of accountable OFE.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

3. System Architecture

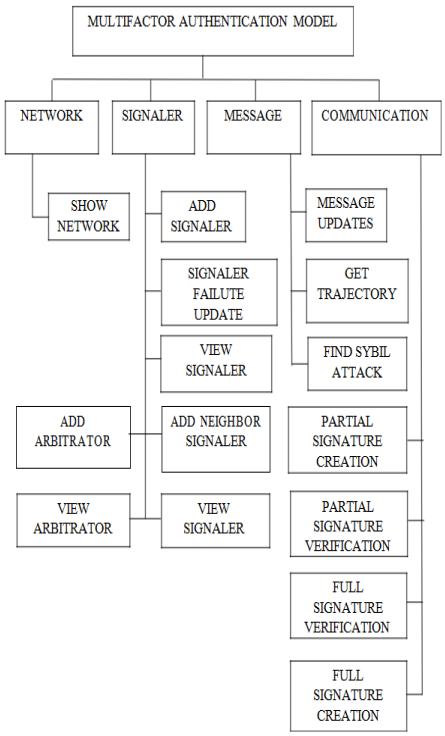

Fig.1: System Architecture

4. Modules

4.1 Module: 1 Sender Identic Creation

In TPA key creation, public key and private is generated. The key generated for security purpose is performed using RSA algorithm.

In Add signaller, road side unit details such as signaller id, public key, private key, trusted authority id are added and saved to ‘Signaller’ table. In update road signaller failure, failure occurred in road side unit details are updated and saved to ‘Signaller’ table. The signallers active status will be set to 0. In add neighbour signaller, neighbour signaller details such as signaller id, neighbour signaller id, distance are added and saved to ‘Neighbour signallers table.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

This distance information will assist the sybil attack detection. In view signaller, signaller details are fetched from 'Signaller' table. The records are displayed using data grid view control. In this additional, Signaller and its neighbour signaller details are fetched from 'Neighbour signallers table. The records are displayed using data grid view control. In add arbitrator, arbitrator details such as arbitrator id, public key, private key are added and saved to 'Arbitrator' table. In show trajectory information, trajectory path information for each arbitrator is verified. These details help to identify the path travelled by the arbitrator.

4.2 Module: 2 Authentication Message

The message module is used to update the message between signallers to arbitrator. The another process is used to know the trajectory of the desired arbitrator, the details contains such as issued arbitrator identity number, received arbitrator unit, trajectory id, signallers number and entry time of the arbitrator.

In finding suspected attack is used to detect the unauthorized Arbitrator in the network. Here the attack details is executed depend upon the Arbitrator id. The details contain such as traverse path of identity number, road side unit details, entry time of the Arbitrator at all transmission. Message should be create the actual details of the sending and receiving trajectory

4.3 Module: 3 Verification and Communication

In this module create a unique identify to send the authenticate receiver. Partially create one signature verified correct person to receive the data. This signature verified performed as cryptography technologies are used.

In signature verification, the partial signature creation, the input provided as two pairs namely public key for arbitrator and private key for the road side unit, the message should be provided then the message should be encrypted and partial signature value executed in the application.

Based on selecting both road side unit and arbitrator identity number, the partial signature is verified. The complete signature creation is finished when two pairs namely private key for road side unit and public key for arbitrator and then the information pass through to road side unit from board unit. The information can be used for future mention. Finally, the partial signature value and encrypted message is taken as ouput. The encryption and decryption process is carried out using Triple DES algorithm.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

5. Result

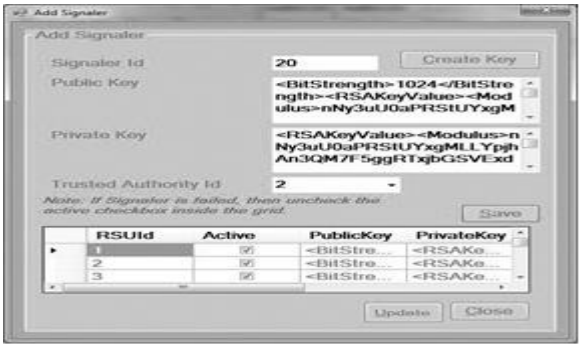

Fig.2: Add Signaller

In Fig.2 Road Side unit details such as signaller id, public key, private key, trusted authority id are added and saved to 'Signaller' table.

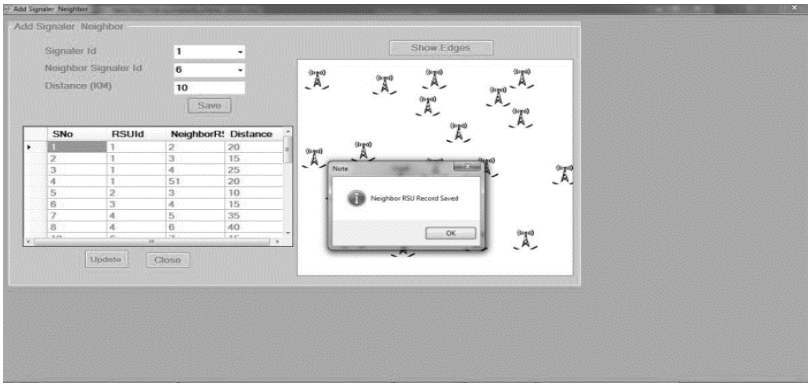

Fig.3: Add Neighbour Signaller

Fig.3 shows, neighbour signaller details such as signaller id, neighbour signaller id, distance are added and saved to 'Neighbour Signallers' table. This distance information will assist the Sybil attack detection.

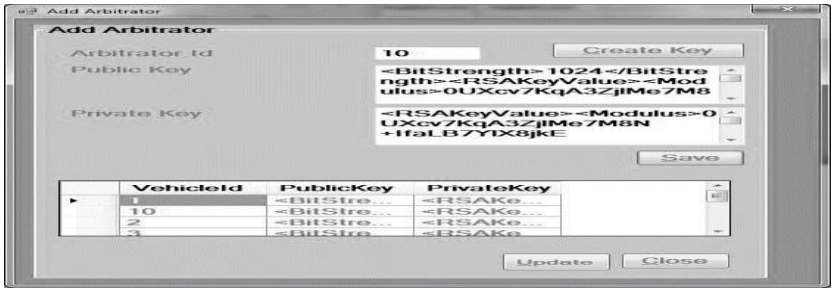

Fig.4: Add Arbitrator

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

Fig.4 shows, arbitrator details such as arbitrator id, public key, and private key are added and saved to 'Arbitrator' table.

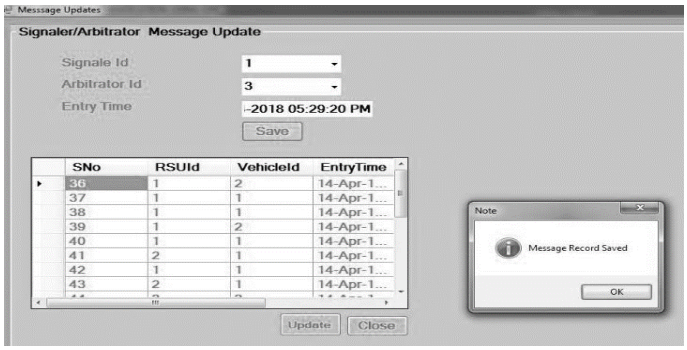

Fig.5: Message Update

Fig.5 indicates the message is used to update the message between signallers to arbitrator. The details contains such as issued arbitrator identity number, received arbitrator unit, trajectory id, signallers number and entry time of the arbitrator.

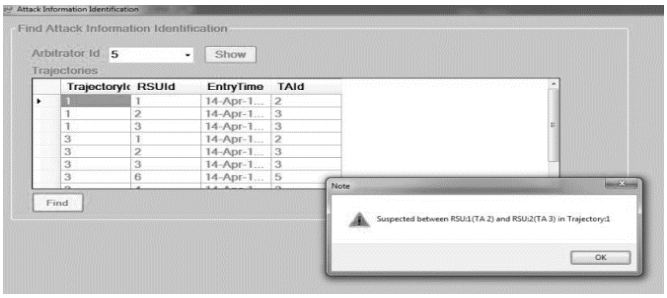

Fig.6: Find Sybil Attack

Fig.6 indicates the unauthorized arbitrator in the network. Here the attack details is executed depend upon the arbitrator id.

The details contain such as traverse path of identity number, road side unit details, entry time of the arbitrator at all transmission.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

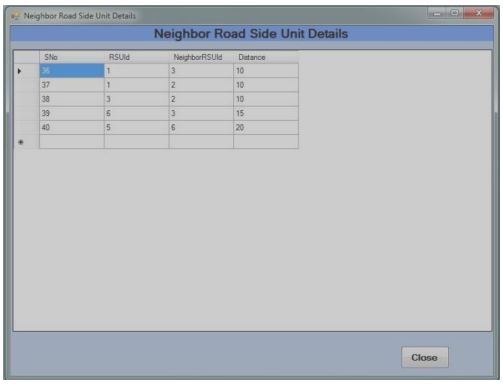

Fig.7: Signature Verification

Fig.7 In the partial signature creation, the input provided as two pairs of the Arbitrator, the message should be provided then the message should be encrypted and partial signature value executed in the application. The verification of partial signature can be done by selecting the road side unit and arbitrator identity number.

From these two pairs, the full signature creation is done and data exchanged from road side unit to on board unit for implications then the generated partial signature values and encrypted messages are the outputs. The encryption and decryption process is carried out using Triple DES algorithm.

6. Conclusion

The main objective of the proposed approach is to validate the concept of accountable OFE, where signer and the third party are liable for their behavioural affairs. The accountable and transparent third party with generic model of OFE is proposed. The proposed architecture depends on several well-studied cryptographic methods in order to meet all security requirements. The three categories of accountability are explained in this work just capturing the critical requirements of accountable OFE, in accordance with each OFE protocol should satisfy the characteristics. In addition to other particular requisites of accountability within existing state of affairs, identification of such demands and security issues are some of the works to be carried out in future.

Alternatively, the proposed protocol is verified securely based on random oracle assumption. Whereas random oracles have been extensively employed in security verifications, a deductible secure protocol certainly is much enviable in the absence of random oracles.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

References

[1] N. Asokan, M. Schunter, and M. Waidner, "Optimistic protocols for fair exchange," in Proc. CCS'97, 1997, pp. 7–17, ACM.

[2] Y. Dodis, P. J. Lee, and D. H. Yum, "Optimistic fair exchange in amulti-usersetting,"inProc. KC'07, 2007, vol.4450, pp.118–133, LNCS, Springer.

[3] Y. Dodis and L. Reyzin, "Breaking andrepairingoptimisticfair exchange from PODC 2003," in Proc. 2003 ACM Workshop on Digital Rights Management, 2003, pp. 47–54, ACM.

[4] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Efficient optimistic fair exchange secure in the multi-user setting and chosen - keymodel ith outrandomoracles," in Proc. CT-RSA'08, 2008, vol. 4964, pp. 106–120, LNCS, Springer.

[5] O. Markowitch and S. Kremer, "An optimistic non-repudiation protocol ith transparent trusted third party," in Proc. ISC'01, 2001, vol. 2200, pp.363–378, LNCS, Springer.

[6] H. Zhu,W. Susilo, and Y.Mu, "Multi-party stand-alone and setup-free verifiably committed signatures," in Proc. PKC'07, 2007, vol. 4450, pp.134–149, LNCS, Springer.

[7] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures (extended abstract)," in Proc. Eurocrypt'98, 1998, vol. 1403, pp.591–606, LNCS, Springer.

[8] Waidner, "Optimistic fair exchange of digital signatures," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 593–610, Apr. 2000.

[9] J. Camenisch and I. Damgård, "Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes," in Proc. Asiacrypt'00, 2000, vol. 1976, pp. 331–345, LNCS, Springer.

[10] J. M. Park, E. K. P. Chong, and H. J. Siegel, "Constructing fair-exchange protocols for e-commerce via distributed computation of RSA signatures," in Proc. PODC'03, 2003, pp. 172–181, ACM.

[11] YangWang, Man Ho Au, WillySusilo "Optimistic fair exchange in the enhanced chosen-key model" Volume 562, 11 January 2015, Pages 57-74, Elsevier.

[12] E.Baraneetharan, G. Selvakumar, "Smart Internet of Things (IOT) System for Performance Improvement of Dual Bridge LLC Resonant Converter by Using Sophisticated Distribution Control Method (SDC)" in proc IoT close loop, 2018, springer.

[13] Bai, H., Ma, Z., & Zhu, Y. (2012). The application of cloud computing in smart grid status monitoring. In Y. Wang & X. Zhang (Eds.), Internet of things. Communications in computer and information science, Vol. 312.

[14] Ye J., Sun H., Li S., & Hou, X. (2017). Simulation study low voltage power line carrier communication in noisy environments. In 2017 International Conference on Computer Network, Electronic and Automation (ICCNEA) (pp. 392–395).

[15] Arpit Agrawal, Gunjan Patankar," Design of Hybrid Cryptography Algorithm for Secure Communication" published by "International Research Journal of Engineering and Technology", Volume 3 Issue 1, Jan 2016.

[16] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Protection of Key in Private Key Cryptography" published by "International Journal of Advanced Research", Volume 5, Issue 2, Feb 2017.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 02
Pages: 70- 78
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.2.002

[17] Meenakshi Shankar, Akshay.P, “Hybrid Cryptographic Techniques Using RSA Algorithm and Scheduling Concepts” published by ”International Journal of Network Security & Its Application”, Volume 6, Issue 6, Nov 2014.

[18] S. Luo, J. Hu and Z. Chen, “Ciphertext policy attribute-based proxy re-encryption,” in Information and Communications Security, pp. 401–415, Springer Berlin Heidelberg, 2010.

[19] C. E. Gates, "Access control requirements for Web 2.0 security and privacy", IEEE Web 2.0 privacy and security workshop (W2SP'07) Oakland California USA, May 2007.

[20] Margolin, N. Boris Levine and, Brian Neil, "Informant Detecting Sybils using incentives", Proceedings of Financial Cryptography (FC), pp. 192-207, February 2007.

[21] J. R. Douceur, “The Sybil attack”, in proceedings for the First International Workshop on Peer-to-Peer Systems (IPTPS'02)", vol. 2429, pp. 251-260, Mar. 2002.

[22] Diksha Gupta, Jared Saia, Maxwell Young, "Peace through Superior Puzzling: An Asymmetric Sybil Defense", Parallel and Distributed Processing Symposium (IPDPS) 2019 IEEE International, pp. 1083-1094, 2019.

[23] Bergadano Francesco, D. Gunetti, C. Picardi, "User authentication through keystroke dynamics", Acm Transactions on Information & System Security 5, vol. 4, pp. 367-397, 2002.

[24] M.Nandhini, B. Praveenkumar, “Secure Smart Grid for Public Key Infrastructure using Wireless Communication System”, International Journal for Scientific Research & Development-IJSRD, Vol. 3(3), pp. 1247-1250, 2015.

Authors Biography

Satheesh.M, works in the Department of Information Technology, at St. Peters Institute of Higher Education & Research, in Chennai, TN, India. His area of research includes Mobile and ubiquitous networks, Big Data Analytics, Industrial System and Collective Intelligence on all fields of Computing and Communication Technologies

Deepika.M, works in Department of Information Technology, at St. Peters Institute of Higher Education & Research, Chennai, TN, India. Her area of research includes Cloud Computing, Parallel Computing, Distributed Computing, Service Computing, Software Evolution, Business Process Computing, Internet Computing and Human Computer Interactions

ISSN: 2582-337X (online)