INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

Implementation of Anonymous and Secure Communication System with Group Signatures: A Review

Mr. Vaibhav P. Thakare
P. R. Patil Collage of Engg and Technology, Amravati
vaibhavthakare93@gmail.com

Prof. Chetan J. Shelke
P. R. Patil Collage of Engg and Technology, Amravati
chetanshelke7@gmail.com

Abstract: For Privacy Preserving Communications Both Anonymity and end to end encryption mechanism is essential. Identity-Based Encryption technique is best suitable for secure and anonymous communications. For solving anonymous and secure communication problems both cryptographic and IBE based protocols needed which governs the proper communication between two parties. For the purpose of authentication of the user proxy server is maintained between user and service providers. The GM and KGC are essential in anonymous communication for issuing both signing and decryption keys for getting plaintext from ciphertext in original form. Public key encryption and digital signature mechanism needed for guarantees of secure communication between both ends. Finally, protocol realizes secure and anonymous communication between sender and receiver.

Keywords: Anonymous Communication, Anonymous Authentication, Secure Channel, Identity-Based Encryption, Group Signature.

1. INTRODUCTION

1.1 Overview

Now a day's security is an important factor in networking world. Security plays an important role at the time of performing communication in the network. Anonymity is an important aspect of privacy and systems that provide services to ensure user anonymity. Both anonymity and end to end encryption are recognized as important properties in privacy preserving communications. However secure and anonymous communication protocol that requires both anonymity and end to end encryption cannot be realized through simple combinations of current anonymous communications protocol and public key infrastructures. Indeed, the current PKI contradicts anonymity because the certificate for a user's public key identifies the user. Moreover, we believe that anonymous communication channels should have certain authentication mechanisms because such a channel could incubate criminal communication. To cope with this issue, we propose a secure and anonymous communication protocol by employing identity-based encryption for encrypting packets without sacrificing anonymity, and group signature for anonymous user authentication [1][2]. Several cryptographic primitives that can provide anonymity have been proposed. Among these is group signature which allows signers to prove anonymously the validity of signatures. A group manager (GM) with a pair of a group public key and a master secret key issues a secret signing key to a user that computes a group signature(on certain messages) using secret signing key. No user-dependent value is required in the verification phase; a verifier verifies using only the corresponding group public key. However, these approaches alone cannot guarantee anonymity when applied to online communication. For instance, let a signer compute a group signature and send it to a verifier. The verifier can anonymously verify the signature's validity. However, there is a question of how to send anonymously the group signature to the verifier. Usually, a source IP address is included in a packet that reveals the identity of the sender thus user anonymity is already infringed [1][3].

1.2 Motivation

In today's networking environment security is an important issue for proper communications. In our proposed system we mainly focus on anonymity and security principles which can be achieved by the concept of a group signature. Group signature allows signers to prove anonymously the validity of the signature. A group manager with a pair of public key and master secret key issues secret signing keys to the user that computer group signatures. Anonymous authentication can be done using anonymous communication protocols which are identity-based encryption (IBE) protocol. For encrypting packets and group signatures for

anonymous authentication of users. Identity-based encryption encrypt content without identifying key holder. The proxy server plays the role of key generation center which stores all the id keys of each user and provides access permission [4].

1.3 Objectives

The current dissertation is dedicated to achieving some of the following objectives.

1) To develop a secure and anonymous communication system.
2) Establishing identity and access control.
3) To preserve the integrity of the document.
4) To prevent unauthorized and illegal access of data.

1.4 Future scope

Now a day's security and anonymity is an important factor in data communication systems. In certain applications such as IB, CBI, etc. we need strong security and confidentiality during performing communication operations such as transmitting as well as receiving data. Our proposed system in such a format which provide secure and anonymous communications in the networking world. Using identification and authentication of users mechanisms we implement fully authorized communication system. In future, such systems facilitate secure, anonymous and authenticated communications over the Internet. Using such systems we achieved stronger security in the network.

2. LITERATURE REVIEW

2.1 Background History

In a networking environment communication is an important issue. Normally in the past environment communication is in very simple format. For making communication or transmission of data one client and one server is necessary and there are not any intermediate stations between them [5]. The most of the times communication between them should be uni-directional and sometimes bi-directional. Whenever a client wants to communicate with the server he was just forwarding one simple text message to the server to check whether the server is ready for communication or not. If the server is free then he sends an acknowledgement back to the client. But because of direct communication between client and server, there may be a large amount of possibility of attacks or data losses during communication [6]. For that reason, any attacker can easily read that message and make some modification in the original message. There was also some communication problems arises in Earlier days such as if there is only one server and multiples clients attach to that server so at that time server will fulfill request of only one client at a time if another client wants to access data from server he must wait until server is free so waiting time problem also introduced. So earlier communication system is not good as compare to today's anonymous and secure communication system [6][7].

2.2 Existing system

In the existing system, there are five important factors. Every factor has its own different working mechanisms which consist of User, Proxy, SP, GM, and KGC. A User wants to communicate with an SP without revealing its identity [5]. Here, we assume that users will never lie about their IP address [8]. The Proxy assists communication between the User and SP by relaying packets without revealing the User IP address. We assume that the SP is honest-but-curious. The SP provides services to the User but wants to authenticate it. The SP is not interested in the identity of the User but needs to confirm whether the User is legitimate. The GM manages a group key and issuer key and issues a signing key to the User to be used for generating an anonymously-authenticated token. We assume that the GM suitably authenticates the User before issuing the signing key. The KGC generates a decryption key for the User. We assume that the KGC suitably authenticates the User before issuing the decryption key [9].

These roles need to collaborate mutually in order to realize the proposed secure anonymous authentication. Their interaction sequence is as follows. A User (whose IP address is Add src) chooses a temporary ID Temp ID the User computer a group signature on temp ID and the User sends (Temp ID) to the Proxy. The Proxy associates Add src with this temporary ID, and forwards (Temp ID) to the SP. The SP can directly authenticate the users by verifying the group signature without compromising anonymous communication. If the user is successfully verified, the SP encrypts content using Temp ID as the public key of IBE; otherwise, it returns fails result. Here, we apply an IBE property to establish a secure channel between the SP and an anonymous user, where arbitrary values can be a public key, and a cipher text can be independently computed with the generation of the corresponding decryption key. The SP sends this IBE cipher text to the Proxy, which again forwards it to the corresponding user. Finally, the User decrypts the IBE cipher text using the corresponding decryption key issued by the KGC [10][11].

Communication sequences:-

Three types of communication sequences are implemented: User-GM, User-KGC, and User-Proxy-SP, and each of the sequences runs the modules.

The User-GM sequence begins with the Join module, which communicates with the GM. The GM then computes the signing key *sk*, and returns it to the User. This sequence needs to be run before the User-Proxy-SP sequence starts For simplicity [1].

The User-KGC sequence begins with the User Key Generation module, which communicates with the KGC. The User sends Temp ID to the KGC, and the KGC then computes the decryption key dk Temp ID, and returns it to the User. This User-KGC sequence and the User-Proxy-SP sequences are run in parallel, though the User-KGC procedure needs to be completed before the Get-Content module of the User-Proxy-SP procedure is run. For simplicity, the proof-of-concept implementation runs this sequence manually

and obtains dk Temp ID prior to the start of the User-Proxy-SP sequence. The User-Proxy-SP sequence begins with the Send Request module that sends a group signature and Temp ID [11]. Upon receiving them, the Proxy registers each pair (Temp ID, Adrsrc) in a table and runs the Relay Request module that forwards the pair to the SP. The SP then runs the Validity Check module as well as the Send Content module that returns an IBE ciphertext to the Proxy, which forwards that to the User. The User then runs the Get-Content module that decrypts the IBE ciphertext using the corresponding dk Temp ID [11][12].

2.3 Limitations

1) All the key generation mechanisms are done through group manager so proxy only assists communication between user and service provider.
2) If group manager fails during keys issuing authentication problem arises.
3) Identification and authentication can be done in very simple manner.
4) The group manager and KGC manager can break the security of the system.

3. CONCLUSION

Anonymous and secure communication system provide secrete communication between sender and receiver. By using the concept of identity-based encryption for identification and group signature concept of authentication we provide better security as compare to other secure mechanisms. By implementing this concept we provide integrity and confidentiality of document over the network. By using such approach we protect data from unauthorized access and provide better security. We believe this work can contribute to the management of anonymous communication systems. Assorted anonymous communication systems carry the risk of being used by malicious parties, but they can be sanitized by introducing our protocol and running anonymous user authentication; in this way, illegitimate users cannot use these systems whereas legitimate users can still use them without compromising anonymity. Through this work, we want to facilitate secure, anonymous, and authenticated communication over the Internet.

REFERENCES

[1] "Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation" Keita Emura and Akira Kanoaka and Satoshi Ohta and Kazumasa Omote and Takashi Takahashi TETC.2015, pp. 2-6.
[2] K. Emura, A. Kanaoka, S. Ohta, and T. Takahashi, "Building secure and anonymous communication channel: Formal model and its prototype implementation," in ACM Symposium on Applied Computing, 2014, pp. 1641–1648.
[3] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *CT-RSA*, 2005, pp. 136–153.
[4] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO, 1986, pp. 186–194.

[5] A. Sudarsono, T. Nakanishi, Y. Nogami, and N. Funabiki, "Anonymous IEEE802.1X authentication system using group signatures," JIP, vol. 18, pp. 63–76, 2010. **[6]** A. Houmansadr, C. Brubaker, and V. Shmatikov, "The parrot is dead: Observing unobservable network communications," in IEEE S&P, 2013, pp. 65–79.
[7] M. Edman and P. F. Syverson, "As-awareness in Tor path selection," in ACM Conference on Computer and Communications Security, 2009, pp. 380–389.
[8] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," J. Cryptology, vol. 13, no. 3, pp. 361–396, 2000.
[9] N. Attrapadung, K. Emura, G. Hanaoka, and Y. Sakai, "A revocable group signature scheme from identity-based revocation techniques: Achieving constant-size revocation list," in ACNS, 2014, pp. 419–437.
[10] T. Nakanishi, H. Fujii, Y. Hira, and N. Funabiki, "Revocable group signature schemes with constant costs for signing and verifying," in Public Key Cryptography, 2009, pp. 463–480.
[11] T. Nakanishi and N. Funabiki, "Verifier-local revocation group signature schemes with backward unlink ability from bilinear maps," in ASIACRYPT, 2005, pp. 533–548.
[12] B. Liberty, T. Peters, and M. Yung, "Group Signatures with almost-for-free revocation," in CRYPTO, 2012, pp. 571–589.

