Ensuring Secure and Anonymous Data Transmission using Proxy Server

Sumeena P. S.
PG Scholar, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology.

P. P. Joby
Professor and Dean, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology

ABSTRACT
Two important properties in privacy-preserving communication are anonymity and end-to-end encryption. The current anonymous communication protocols and public key infrastructure is not enough sufficient to realize a secure and anonymous communication protocol, that requires the above two properties. There is a secure and anonymous communication protocol which employs identity-based encryption for encrypting packets without sacrificing anonymity and group signature for anonymous user authentication. Proxy entities are used for communication in the protocol which hides user IP address from service providers. There is a possibility for users to communicate with service providers without using proxies. In the, service provider is not anonymous to users. So, users can simply use the service provider public key to build a secure channel. The objective of this project is to provide a secure communication from service provider to user. To cope with this issue, a filtering mechanism is proposed in which the service provider filters the IP address of users who already communicates through proxy entities.

Keywords
IP filtering, Proxy entity, Group signature, Cryptographic tools, Secure and anonymous communication

1. INTRODUCTION
The IP address of the user is always visible in the internet protocol packet sent from the sender to the receiver. In a two-way communication, it is not possible to erase or remove the sender IP address since it is unavoidable when the receiver wants to reply for the received packet. The solution that can be achieved during this situation is to use some intermediate agents. Here comes the use of proxy entities. But the major issue here is how to authenticate users without identifying them. In normal situation the service provider needs the user identity and password for providing certain services. But this contradicts to anonymity. Along with this, the server also requires the IP address of the requester so that it can send certain messages back to the user. One of the solutions to all these problems is that, the intermediate agent will do all the authentication functionalities. Thus this agent will be responsible for authentication functions and the service provider is unaware about the IP address of the user.

One of the cryptographic primitives that can provide anonymity is the group signature scheme. In this the validity of the group signature can be proved anonymously by the signers. The group manager uses a pair of keys to issue a signing key to a user. The pair keys used here are master secret key and a group public key. The user chooses a temporary identity and a group signature is developed based on this temporary ID. The authentication of identity is done by the group manager and the verification of IP address is done by the proxy server.

2. RESEARCH PROBLEM
The main research problem here arises are

1) How to ensure a secure communication?

Secure communication can be achieved by storing the data in an encrypted form. Whenever the user sends a message to the service provider, before sending the message the user will generate an encryption key. This encryption key is needed while decrypting the file. Thus it is possible to say that the data is secured.

2) How to achieve anonymous communication?

The service provided can be freed from authentication purposes if there are some authentication mechanisms before reaching the server. For this it is necessary to use some intermediate agents. For that a proxy server as well as a group manager is introduced for authentication purposes. Therefore the service provider can provide services without knowing the identity of the users.

3) How to achieve both secure and anonymous communication?

By doing authentication via intermediate agents and by storing data in the encrypted form it is possible to achieve a secure and anonymous communication.

3. LITERATURE SURVEY
In order to implement a secure and anonymous communication first of all it is necessary to look into what are the available methods for secure and anonymous communication. Here is a survey on some anonymous communication methods and secure communication methods.

A formal method for secure and anonymous communication and its prototype implementation is introduced by Keita et al. [1]. In this some proxy entities are used which can mask the IP address from the service providers. They can thus ensure secure communication. But the service provider here is not anonymous to users. Hence the major drawback of there is system is that they cannot provide anonymity.

For securing real time application data retrieval in wireless sensor networks Prosanta et al [2] introduces a realistic lightweight authentication protocol which is anonymous. The nodes in the wireless sensor networks are equipped with limited computing power, limited resources etc.. The anonymous user authentication in such environment is a very difficult task. The scheme consists of an authentication protocol which can provide user anonymity. Advantages

include traceability, low computation and communication costs, backward and forward secrecy etc..

Joseph et al. [3] proposed an anonymous authentication protocol which supports time bound credentials. This protocol is very much suitable in roaming networks which has a large scale network. The system embeds a timestamp along with the user secret key with the newly designed group signature scheme. There is no need to put the revoked users in the revocation list since the expired key can be used for authentication purposes. The main advantage of this protocol is that in terms of revocation checking it is much faster than other protocols.

A threshold authentication protocol for Vehicular Adhoc Networks which is anonymous is introduced by Jun et al. [4]. User privacy and communication trust are the two important properties of VANETs. The new protocol uses a new group signature scheme in a decentralized group. The protocol is secure and featured with a threshold authentication. The main disadvantage of the system is that computation cost is high and efficiency is low.

A threshold group signature scheme which is proactively secure and fully distributed is introduced by Johann et al. [5]. Here they introduces a Distributed Key Management Infrastructure which is based on discrete logarithm. It consists of a distributed key generation that is publicly verifiable and round optimal. This is a combined group signature scheme which allows a particular number of group members to sign a message. Here the message is arbitrary and the particular number is the threshold number.

Jody et al. [6] introduces a new work in anonymity which can prevent an active attacker from attacks. This can include the user's internet service provider also. The major design goal of dovetail is to provide protection without including a proxy during the transmission of data in the application layer. The dovetail concept consists of mainly two types of nodes, the dovetail node and the matchmaker node. They are also called a router and an end host respectively. The main advantages are scalability and efficiency. The main disadvantage of the system is that privacy consideration is very weak.

In order to analyze anonymous communication protocols Michael et al [7] introduces a new framework called Ano A. The properties of an anonymous communication channel can be easily identified by this Ano A. It can also define and quantify the properties of such anonymous communication channels. It can provide ideal functionalities. The main disadvantage of the system is that it cannot prevent attackers in the Tor communication channel.

Anon-pass is a protocol introduced by Michael et al. [8]. The system can prevent the large sharing of credentials and allows anonymous user authentication. It is not possible the service providers to correlate the user's actions. Balancing the computational resources of a service provider is the major issue here. Practical anonymity is the major focus of the anon-pass subscription services system. The main advantage of anon-pass is that it can provide low cost as well as flexible services. The main disadvantage of the system is that it cannot give unlinkability for its users.

Risto Laurikainen introduces a secure and anonymous communication in the cloud [9]. Any communication system can provide anonymity, confidentiality, integrity etc.. Mutual authentication is necessary in any communication. Thus preventing third parties during mutual authentication is thus a necessary thing. He introduces steps to find the requirements of such systems and how to implement these requirements. There are many programs, which may be single or multiple available for providing secure and anonymous communication.

Wei Feng et al. [10] introduces anonymous authentication applicable to social networking which can support rapid social activities. With the help of heterogeneous networks it can support those activities at any time in a privacy preserving environment. This can be achieved with the help of anonymous user authentication. This is such an authentication scheme which is based on group signature. Here authentication is for trust level rather than identities. The main advantage of the system is that it can guarantee secure communication among nodes.

4. PROTOCOL CONSTRUCTION

The protocol is fully implemented using java. It mainly consists of five roles which are implemented as different modules. The roles are User, proxy, group manager, key generation centre and service provider.

The different roles and their main functions are shown in Fig 4.1.

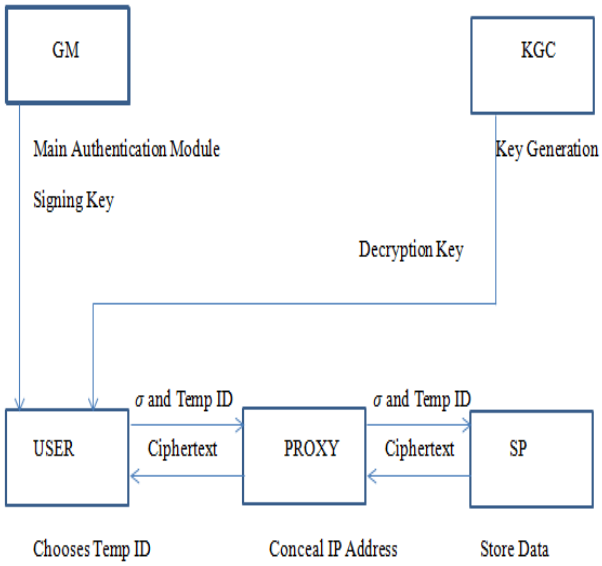

Fig 4.1: Framework of the protocol

1. The Group Manager Module
The group manager is responsible for authentication purpose and he has the sole authority to register each user by choosing their type and registering all the IP addresses into its own database.

2. The user module
This module includes the application from which the user can login into the system. This will be a basic web application which will compare the user details with the details of the user profile in the database of the group manager. This module will be used by the user to login to the system too. At the time of login the user will select a random key, called Temporary ID and that key will be used along with the group signature by the GM to generate sigma. The temporary ID will be lost whenever the section is over.

3. The proxy module
This module is used to hide the user details from the service provider to ensure privacy of the users and anonymity of the

user machines. The proxy will handle the user sigma and generate the session. This will be a web proxy in implementation.

4 The service provider
The service provider module will be an application which serves the user with the data needed. This module will check the user sigma and then calculate the group signature validity and then provide the data encrypted to the user with a session specific key which is called the temporary ID. The files or data normally saved in the server will be insecure. So in order to avoid this, the service provider application is implemented so as to handle all the data protected via ensuring a des encryption to the data saved. The saved data is identified by the admins master key only.

5. The KGC
This module is used as the key supplier for the user for decrypting the received data from the service provider. This module will first authenticate the user and then generate the decryption key and provide it to the user by which the user will decrypt the files.

5. SECURE AND ANONYMOUS COMMUNICATION PROTOCOL

It is very difficult to construct a secure and anonymous communication protocol with the help of currently available public key infrastructure and currently available protocols, because such a protocol should satisfy the properties such as anonymity and end-to-end encryption. The current public key infrastructure provides a certificate for users public key through which the user is identified, therefore it cannot provide an anonymous communication. All the communication channels have the authentication mechanism to prevent attackers or intruders. The proposed protocol uses both identity based encryption and group signature scheme. The group signature here used can provide user authentication anonymously and the IBE can provide encryption without compromising anonymity. Proxy is implanted in between the communication channel so as to mask IP address from service provider.

Among the many cryptographic primitives group signature is the most important. There are mainly five roles in the protocol which are implemented as different modules. The group manager can provide signing key for its users. Each user after choosing a temporary ID can then login into the system. In their home page they have the facility to send and receive messages.

6. PERFORMANCE EVALUATION

The proposed protocol is said to be secure since the protocol consists of a two way authentication mechanism. The first one is provided by the group manager and he second one is provided by the key generation center. The proxy used in the middle of user and service provider in order to mask the IP address from the service provider. The service provider only knows the IP address of the proxy server only. Thus it is possible to facilitate anonymous communication. The performance of the constructed protocol can be evaluated with the help of the time taken for executing the algorithms for sending, receiving data and also for validity checking and send request. This can be shown with the help of the graph shown in Fig 6.1.

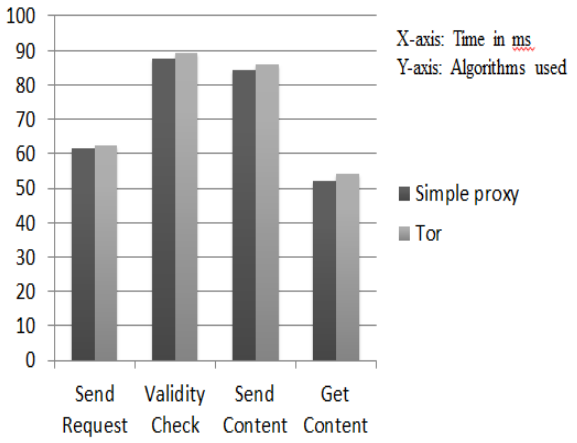

Fig 6.1 comparison of algorithms

From the above graph it is clear that proxy implementation can improve the performance of the protocol to a great extent and the time taken for each algorithm with this proxy is also within the range of practical acceptance.

7. CONCLUSION AND FUTURE SCOPE

With the help of Identity based encryption and the group signature , the proposed protocol can provide a secure and anonymous communication. Without sacrificing anonymity it is very difficult to construct a secure and anonymous communication. But here with the help of a proxy entity and the key generation module it is possible to construct a secure and anonymous communication protocol. The former can provide anonymity and the latter can provide security to the protocol. The protocol transaction time is within the range of practical acceptance.

It is possible to extend the work by eliminating the key generation module by supplying the key directly between sender and the receiver. Thus it is possible reduce the code length and time taken for executing KGC algorithm.

8. REFERENCES

[1] Emura, K., Kanaoka, A., Ohta, S., Omote, K. and Takahashi, T., 2016. Secure and anonymous communication technique: Formal model and its prototype implementation. *IEEE Transactions on Emerging Topics in Computing*, *4*(1), pp.88-101.

[2] Gope, P. and Hwang, T., 2016. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Transactions on Industrial Electronics*, *63*(11), pp.7124-7132.

[3] Liu, J.K., Chu, C.K., Chow, S.S., Huang, X., Au, M.H. and Zhou, J., 2015. Time-bound anonymous authentication for roaming networks. *IEEE Transactions on Information Forensics and Security*, *10*(1), pp.178-189.

[4] Shao, J., Lin, X., Lu, R. and Zuo, C., 2016. A threshold anonymous authentication protocol for VANETs. *IEEE Transactions on vehicular technology*, *65*(3), pp.1711-1720.

[5] Van Der Merwe, J., Dawoud, D.S. and McDonald, S., 2007. A fully distributed proactively secure threshold-multisignature scheme. *IEEE Transactions on Parallel and Distributed Systems*, *18*(4).

[6] Sankey, J. and Wright, M., 2014, July. Dovetail: Stronger anonymity in next-generation internet routing. In *International Symposium on Privacy Enhancing Technologies Symposium* (pp. 283-303). Springer International Publishing.

[7] Backes, M., Kate, A., Manoharan, P., Meiser, S. and Mohammadi, E., 2013, June. AnoA: A framework for analyzing anonymous communication protocols. In *Computer Security Foundations Symposium (CSF), 2013 IEEE 26th* (pp. 163-178). IEEE.

[8] Lee, M.Z., Dunn, A.M., Waters, B., Witchel, E. and Katz, J., 2013, May. Anon-pass: Practical anonymous subscriptions. In *Security and Privacy (SP), 2013 IEEE Symposium on* (pp. 319-333). IEEE.

[9] Laurikainen, R., 2010. Secure and anonymous communication in the cloud. *Aalto University School of Science and Technology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10*, pp.1-5.

[10] Yan, Z., Feng, W. and Wang, P., 2015. Anonymous authentication for trustworthy pervasive social networking. *IEEE Transactions on Computational Social Systems*, *2*(3), pp.88-98.