Privacy Preserving Authenticated Key-Exchange over Cloud

Prof. Priyanka Kedar[1] Ashvini Deshmukh[2] Trupti Bhong[3] Rachna Pandita[4] Juhee Sonarkhan[5]
[1]Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]DPCOE, Wagholi, Pune 412 217

Abstract— Key exchange for providing network security in particular Data encryption standard (DES) is the core cryptographic mechanism. For key exchange over the cloud security and privacy both are required. In this paper we have developed a family of privacy preserving authenticated DES algorithm both in traditional PKI setting and in the identity based setting. The newly developed DES are of conceptual level and practical based efficiency. It provides very useful privacy protection to protocol participants and add a new value to the IKE standard. As per our information, the protocols are the secure DES protocols which provide the following privacy protection advantages: 1) concurrent non-malleable statistical, forward deniability. 2) The session key and session transcript can be generated that cannot be traced to the pair of protocol participants. 3) Exchanged messages do not reveal the users identity and do not explicitly reveal the plays role information.

Key words: Diffie-hellman, key exchange, Data encryption standard, authentication, security

I. INTRODUCTION

User authentication is one of the important legitimacy in real time world. let us take the example of client-server application, in this a service provider needs to be authenticated before providing services to the consumer of any user. Similarly the consumer or any user receiving the services from the provider. Since both the parties need a common internet key exchange [5] mechanism which is common only to the intended parties. In case of key agreement protocol the user without authentication can misuse the identity of an innocent user which leads to attacks, misuse of resources and unknown key share. In this paper we have introduced different encryption standard. The different encryption standards are DES, AES and for key exchange we use Diffie-Hellman algorithm (DHKE) [4]. Encryption is the method of transforming original data which is known as plaintext or clear text which transforms into a cipher text which is not readable by the user. Again the cipher text is decrypted and after decryption we get our original text. This is all about encryption and decryption which we will use in our paper. In many environments it is more important that communication must be authenticated rather than it is encrypted. Also there are many different techniques for authentication. Authentication of the message means conformation of the sender sending the message. Infrastructure as a service is a model in which an organization outsources the equipment which is used to support operations including storage hardware servers and networking components. The Internet key exchange (IKE) protocol [1], [2] is used to offer confidentiality authentication and privacy for communication protocols [6] in the higher layers of ISO-OSI. Providing privacy protection serves as one of the vital role in underlying the evolution of a list of important industrial standards of KE cryptographic protocols [7].

II. EXISTING SYSTEM

The internet key exchange protocols ensure internet security hich provides key exchange mechanisms to establish shared keys while communications process. The IP layer preserves the privacy characteristics from the upper layer i.e the application layer for deniability service. The communication protocol security depends upon one or more assumptions. For example a key agreement protocol is built upon one or more cryptographic assumptions. A protocol with multiple assumptions has different security mechanism. By using multiple cryptographic algorithms an authenticated key establishment protocol is constructed which are also based on various cryptographic assumptions. In this paper various specified feature for key exchange protocol have been defined. Cryptography is one of the techniques for storing and transmission of data in a form that only authenticated users can read and process the information and knowledge.

The ultimate moto of cryptography is to hide the secured data and information from unauthorized users while transmission of data and other information. So the ultimate goal of cryptography is to provide protection and protect the data from the attacks. Generally authentication is the process by which we can validate a user who login to the information. E-MAC based hash function can be used against the key recovery attacks. The use of universal hash function was first introduced by Carter and Wegman. The existing system is based on internet which also provides key exchange mechanism between the sender and receiver. But because of key exchange over internet it cannot provide overall securities to the intended usera hich of the examples of the existing system are dropbox, google drive and client serves architecture. The protocol security should be processed entirely rather than processing at the individual level. Authenticated key establishment is the process used to verify the legitimacy of both the communicating parties i.e the sender and receiver. Authenticated key establishment is most important for all secure communication such as e-commerce, wireless wired and internet application. Various authenticated key establishment protocol is constructed using different cryptographic assumptions. In this paper various features for key exchange protocol are considered depending upon multiple cryptographic techniques.

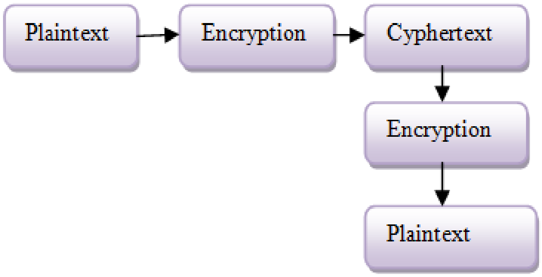

Fig. 1: Cryptography process

III. Proposed System

The proposed system consists of cloud storage and it is used to provide a secure system for customers. The proposed system is highly secure and realiable. Here in this paper the system implements various algorithms such as Deffie-Hellmen key exchange, DES algorithm and many more as per the users requirement by using this algorithm the system provides authenticated user and security of data and information which is based on cloud. The functions of the proposed system are as follows:

(1) It provides multilevel security.
(2) It provides security during data transmission.
(3) It provides data availability to the customer.

The system feature provide efficient and fast result, also provides negligible chance to have wrong and bulky result. The proposed system helps us in providing high level security to the user accounts and avoids the attacks such as hacking. In the proposed system there are number of users who tend to use the system, the users include:

(1) General user who want to use the authentication system.
(2) The user may be sender, receiver and server.
(3) Providers are the users who want to share or store data on to the server.
(4) Server manages and provides storage space, computational resource and storage services.
(5) Receivers are the users who want to access data.

The system product will be operating in java script, JDBC, HTML file also it will be compatible with JRE and Windows 7. Most of the features will be compatible with the my SQL server. The only requirement to use this project would be LAN connection proposed system is intended to store, retrieve, update and manipulate information related user.

Data present in database such as file and key. Different files such as txt, pdf, media etc.

The system consist of user and server as an actor and in the system the provider uploads the file on server, receiver receives the file through key exchange and secure encrypts and decrypts the file. The development of the system will be manipulated by the availability of the required software such as web servers, database and development tools. The availability of this tool will be governed by the developer of the software. The user interface must be customizable by the administrator of the system. The user integration must be easy to handle by the user.

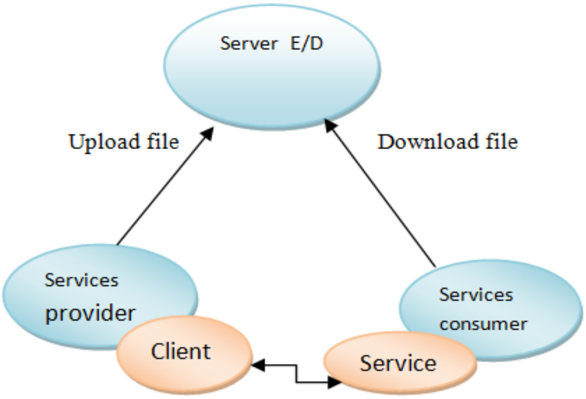

Fig. 2: Structure of SOA

IV. Conclusion

The proposed system is designed to provide security for data over cloud. The data related to any type of fields is secure and protected by using data encryption standard. The newly proposed system is of great efficient, practically secure on conceptual level. The system also provides authentication from unauthorized users. The main moto of this proposed system is to provide protection and security of data over cloud and also helps to find in authorized users who can misuse the data and provides protection from data attacks. Deniability, key exchange by using deffie-hellman key exchange, by using different encryption and decryption algorithm the system provides security to the data and are the basic building blocks of the system. It ensure security with related services like confidentiality, integrity, authentication and privacy preservation while communication.

Reference

[1] D. Harkins and D. Carreal, “The Internet key-exchange (IKE),” IETF (The Internet Engineering Task Force), New York, NY, USA, Tech. Rep 2409, Nov. 1998.
[2] C. Kaufman, “Internet key exchange (IKEv2) protocol,” The Internet Engineering Task Force, London, U.K., Tech. Rep. 4306, Dec. 2005.
[3] J. Camenisch, N. Casati, T. Gross, and V. Shoup, “Credential authenticated identification and key exchange,” in Proc. CRYPTO 2010pp. 255–276.
[4] U. Maurer and S. Wolf, “Diffie-Hellman oracles,” in Proc. CRYPT 1996, pp. 268–282.
[5] A. C. Yao and Y. Zhao, “Deniable Internet key-exchange,” IACR (The International Association for Cryptologic Research), San Diego, CA, USA, Tech. Rep. 2011/035, Jan. 2011.
[6] R. Canetti and H. Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels,” in Proc. Eurocrypt 2001 pp. 289–307.
[7] R. Canetti, “Security and composition of cryptographic protocols:
A tutorial,” SIGACT News, vol. 37, no. 3, pp. 67–92, 2006