International Journal of Engineering & Technology, *7 (2.33) (2018) 912-914*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An efficient token based authentication mechanism for IP trace back

Deepthi S. MTech Scholar [1] *, Arun P. S [1]

[1] MTech Scholar, Department of CSE Sree Buddha College of Engineering Pattoor, India
[2] Arun P S Asst. Prof, Department of CSE Sree Buddha College of Engineering Pattoor, India
**Corresponding author E-mail: sreedeepthiss@gmail.com*

Abstract

IP traceback plays an important role in the cyber investigation process. Because of the trusting nature of protocol the source IP address is not authenticated. So there may be the chances of occurring one way attack is very high. As a result the receiver does not accept the data properly. It is known as IP traceback problem. So the IP traceback traces the source of packets and also the traversed path of these packets. Some applications of the IP traceback are network diagnosis, path validation, performance testing and forensic analysis and so on. Objective of the paper is to prevent unauthorised users requesting from traceback information for malicious operations. So developed a token based packet marking mechanism .It uses token for identifying the sources. In token based authentication IP traceback it uses a token passing mechanism. The traceback server generates the token. The data along with token is send to the end host. Only the actual data arrives at end host. The cloud based sever stores the token, data, node details and transmission details. If an attack occurs the token can be used for identifying the sources as well as traversed path of packet.

Keywords: *IP Trace Back; Forensic Analysis; Token; Trace Back Server*

1. Introduction

Now a days the attacks on the internet are growing. Therefore the forensic crimes are increasing. The possible solution for this problem is IP traceback. IP traceback traces both source and traversed path of the packets. Some of the IP traceback techniques are based on packet appearance, link testing, and ICMP based traceback and so on. The disadvantage of this technique is processing of router's overhead. There are different types of IP traceback techniques to be employed. They are based on packet logging, packet marking, ICMP based and so on. The most commonly used technique is based on packet marking. Examples of packet marking techniques are probabilistic packet Marking (PPM), Deterministic Packet Marking (DPM), and Flexible DPM and so on. In PPM the packet is marked with some fixed probability and forwarded. The receiver can be used by this information to reconstruct the attack path.

The attack such as DoS causes delay on internet. Therefore it increases the traffic flow. Besides technical shortcomings, economic inefficiency, such as lack of financial incentive for ISPs, also hinders the practical deployment of existing traceback solutions. The advent of cloud services, however, offers a new appealing option to support IP traceback service over the Internet. It provides an opportunity to design a traceback system that is incrementally deployable. Cloud storage also increases the feasibility of logging traffic digests for forensic traceback.

2. Existing system

The internet is the global media organization which can able to access by any number of users. There are several IP traceback techniques has been employed. The existing research work such as PPM, DPM, and OPM can't track the ip attackers. And also these techniques will lead to high computational cost. The device information can be easily track by the attackers. Another disadvantage of the existing system is the privacy for a user is low.

3. Proposed system

The aim of the proposed system is to prevent unauthorized access of data stored in the cloud storage. So an authentication mechanism should be developed. In the proposed system, for authentication there are three enhanced security mechanisms are used. They are user name and password, random key generation process and radio frequency identification smart card. The user sends the data in an encrypted format. The cloud server stores the encrypted data. For accessing data stored in the cloud server is an important problem. Therefore it proposes a token based authentication mechanism for accessing the data stored in the cloud server. So traceback processing becomes easier and also the traceback service more accessible. The main idea is to embed temporal access tokens in traffic flows and delivers them to an end host in an efficient manner. When an unauthorized user tries to access the data in the cloud server the administrator verify the user and blocks that user. When the user search the data in the server, then the server sends the user details to user details. The token is generated only for the registered users. While using the token the user decrypts the data. The properly authenticated user has the token to download and decrypt the data. And also traces the source of the data. The cloud storage increases the ease of access of data. After authenticating user the data uploaded in the cloud storage in an encrypted format. Whenever the data provider registers into the system it generates a password and encrypts the password using

MD5 algorithm and it is stored on the server. After registering the provider, the user has login to the system using user name and password. Then verify the user using random key generation process and after that verify using smart card. So the user is properly authenticated and user has to download the data and decrypt the data. The proposed system focuses on the user privacy and security.

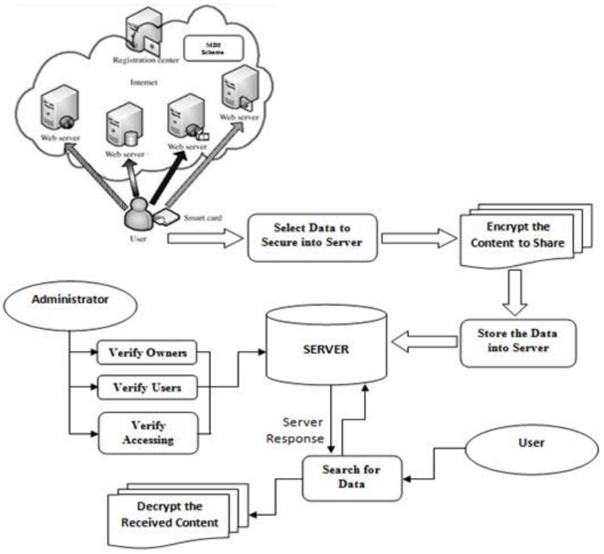


Fig. 1: Architecture of the Proposed System.

4. System model

This system contains three different modules. They are:

- User Authorization and Authentication.
- Secured and Encrypted Data Maintenance.
- Authorized Party Data Search.
- Administrator.

1) User Authorization and Authentication

The User Authorization and Authentication module is one of most popular and important factor to enter into the required portals and applications. This enhanced authentication and authorization norms module allows the user (Data Owner and Data User) to register and authenticate them into the system with proper identities such as Name, Mobile Number, E-Mail-Id, address, Username and Password and so on. Once the authorization and authentication processes are done, the users have specific rights to proceed into the application and access all the features present into it. The User Authorization and Authentication module is derived based on three-factor authentication, which enables user to proceed with three levels of authentication features such as Automatic Password Generation, Username and Password authentication and Key Generation process. For the entire authentication module is the pathway of all users to proceed into the system and accessing the features.

2) Secured and Encrypted Data Maintenance

The Secured and Encrypted Data handling process allows the data owner to maintain the data into the remote cloud server with proper authentication strategies and security. In this module, the base is derived from Advanced Encryption Standard (AES) algorithm. The AES algorithm, which is used to perform the Encryption as well as Decryption process efficiently, which converts the plain text into encrypted text and then maintained the data into remote server. So, that no one can break the server as well as break the data presented into it. For all the entire module of Secured and Encrypted Data Maintenance is helpful to data owner to maintain the data securely in remote place without any hesitation.

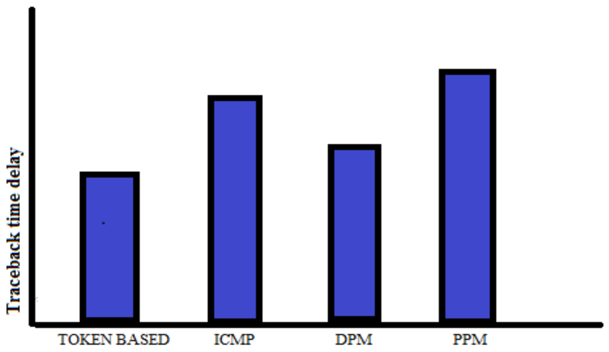
3) Authorized Party Data Search

The Authorized Party Data Search module is helpful to data user to search for the stored records into the server. The user has several stages of validations such as authentication with three-factor law and needs to request for the required data which is presented into the server. Once the request is raised, the system generates the random security key for the respective user and allows them to enter the key into the portal. The key verification strategy checks the entered key is valid or not, if the key is proper then allows the user to download the requested data from the server, if the key is not proper then immediately the system blocks the user to proceed further.

4) Administrator

Administrator can verify the traces of both data owners and data users at any time and also have an option to activate or deactivate them at any time.

5. Evaluation and results



The graph is plotted along the x-axis the traceback techniques and along the y axis traceback delay time. As compared to other techniques it reduces the traceback delay time. And also efficiently token is delivered to the destination. The system is evaluated into number of datasets. The existing research methods takes longer traceback delay time .Some of techniques produces router overhead and fails for identifying the source. In this method it reduces the processing of router's overhead.

6. conclusion

In token based authentication mechanism for IP traceback architecture has several favorable features that the previous traceback scheme fails. The proposed framework has been implemented successfully. The framework reduces the traceback delay and increases the robustness against attack. Token based authentication mechanism also reduces the traffic flow. The proposed system is secure, advanced and efficient as compared to the existing techniques. The evaluation result shows that the proposed system is more secure and efficient. The proposed system also ensures that there is no duplication of records in the cloud server.

Acknowledgment

I am grateful to my project guide Prof. Arun P S for his remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. We are also thankful to all the staff members of the Department

References

[1] H. Aljifri, "IP traceback: a new denial-of-service deterrent?" IEEE Security and Privacy, vol. 1, no. 3, pp. 24–31, 2003.

[2] L. Lu, M. C. Chan, and E.-C. Chang, "A general model of probabilistic packet marking for ip traceback," in ASIACCS '08, 2008, pp. 179–188.

[3] Luis A. Sanchez,2 Walter C. Milliken, Alex C. Snoeren , "Hardware Support for a Hash-Based IP Traceback," in IEEE DARPA Information survivability conference , pp. 179–188,2001

[4] B. Al-Duwairi and M. Govindarasu, “Novel hybrid schemes employing packet marking and logging for IP traceback,” IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 5, pp. 403–418, 2006.

[5] Y. Xiang, W. Zhou, and M. Guo, “Flexible deterministic packet marking: An IP traceback system to find the real source of attacks,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, 2009.

[6] Belenky and N. Ansari, “On deterministic packet marking,” Computer Networks, vol. 51, no. 10, pp. 2677–2700, 2007.

[7] V. Aghaei-Foroushani and A. Zincir-Heywood, “IP traceback through (authenticated) deterministic flow marking: an empirical evaluation,” EURASIP Journal on Info. Security, 2013.

[8] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, “A survey on software-defined networking,” IEEE Communications Surveys Tutorials, vol. 17, no. 1, pp. 27–51, 2015.

[9] Y. Lu, B. Prabhakar, and F. Bonomi, “Perfect Hashing for Network Applications,” in 2006 IEEE International Symposium on Information Theory, July 2006, pp. 2774–2778

[10] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency,” in TRUST’10, 2010, pp. 417–429.