ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

DLD ENHANCEMENT USING SHA ALGORITHM

LEHNASH LATHEEF[1], Dr JAYAPRAKASH[2]
[1]M.Tech Computer Science and Engineering Mohandas College of Engineering and Technology Trivandrum, Kerala, India
Email: lehnash@gmail.com
[2]Department of Computer Science and Engineering Mohandas College of Engineering and Technology Trivandrum, Kerala
Email: jpavithran2011@gmail.com

***Abstract*-The number of data-leak instances have grown rapidly in recent years from security firms, research institutions organizations. The data loss mainly occurred by human mistakes.. In this paper I present about the data leak detection solution and their privacy in it. In my method the main advantage is the data owner to safely delegate the detection operation to a semi honest provider without revealing the sensitive data to the provider. This method can support accurate detection with very small number of false alarms under various data- leak scenarios. We also describe how Internet service providers can offer their customers DLD as an add-on service with strong privacy guarantees**

Index Terms— Data leak, network security, privacy.

1. INTRODUCTION

We know that a lots of data leaks are reported by risk based security in the last few years, i.e., from 412 million in 2012 to 822 million in 2013.Most of the data-leak incidents is happened from deliberately planned attacks, inadvertent leaks and human mistakes.

To detect and prevent the data leaks requires a set of solutions and include about the data-leak detection [4],[5], data confinement [6–8],and policy enforcement [11].

In the most cases network data-leak detection (DLD) performs deep packet inspection (DPI) and searches for any occurrences of sensitive data patterns. DPI is a technique to examine methodolically the detail of payloads of IP/TCP packets for inspecting application layer data, e.g., HTTP header/content.

In this paper, I propose a data-leak detection solution which can be obtained because the data owner and data receiver cannot know their actual details in it. We can easily design and evaluate the fuzzy fingerprint technique that enhances the privacy of data during data-leak detection operations. We approach a fast detection of data leak and privacy can also be very accurate in this technique.

2. MODULES AND OVERVIEW

In this paper I describe about 3 modules. They are,

1.Data Owner

2.Fuzzy finger Print

3.DLD

2.1 Data Owner

The system enables the data owner to securely authorized to represent others about the content-inspection task to DLD providers without exposing the sensitive data. The data owner make sense a special set of digests of fingerprints from the sensitive data and then allow to seen only a small amount of data to the DLD provider. It is the data owner, who check the details of the data and it will have any leak obtained in it. Then the sensitive data is sent by a valid user for a valid purposes. The data owner is aware of legitimate data transfers and permits such transfers. So the data owner can tell whether a piece of sensitive data in the network traffic is a leak using legitimate data transfer policies.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

2.2 Fuzzy Fingerprint

To achieve the privacy goal, the data owner generates a special type of digests. The digests are called fuzzy fingerprints. The fuzzy fingerprints is to hide the true sensitive data in a crowd. It prevents the DLD provider from learning its exact value. The data owner chooses four public parameters. The data owner transforms each fingerprints into a fuzzy fingerprint. All fuzzy fingerprints are collected and form the output of this operation.

2.3 DLD

The DLD provider computes fingerprints from network traffic and identifies potential leaks in them. To prevent the DLD provider from gathering exact knowledge about the sensitive data, the collection of potential leaks is composed of real leaks and noises. It is the data owner, who post-processes the potential leaks sent back by the DLD provider and determines whether there is any real data leak. The DLD server detects the sensitive data within each packet on basis of a stateless filtering system. DLD provider inspects the network traffic for potential data leaks. The inspection can be performed offline without causing any real-time delay in routing the packets. However, the DLD provider may attempt to gain knowledge about the sensitive data.

3. Architectural View

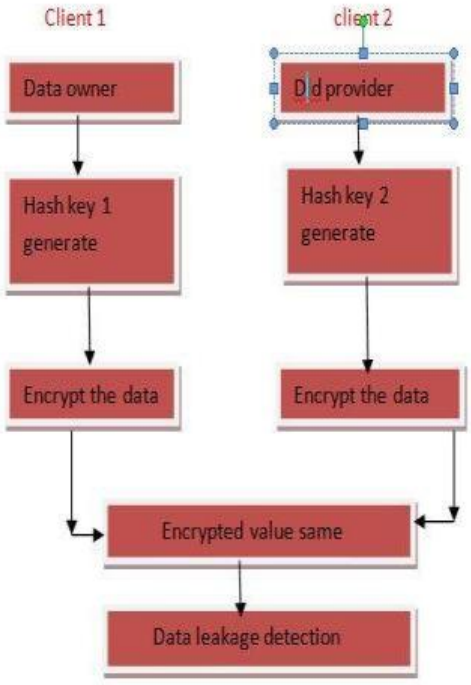

Fig 1: Architecture view of proposed system

4. PROPOSED SYSTEMS

The system propose a privacy-preserving data-leak detection model for preventing data leak in network traffic. the DLD provider may learn sensitive information from the traffic, which is inevitable for all deep packet inspection approaches. the proposed system uses (secure hash algorithm (SHA) to generate short and hard- to-reverse digests through the fast polynomial modulus operation. by using these techniques, an internet service provider (ISP) can perform detection on its customers' traffic securely and provide data-leak detection as an add-on service for its customers. in another scenario, individuals can mark their own sensitive data and ask the administrator of their local network to detect data leaks for them. mainly use SHA algorithm to compare the hash value that provided by data owner and DLD provider. by using the SHA algorithm. It will provide a high security when compare to existing algorithm. more no of data can be send to the data provider at the same time. then the data owner as well as DLD provider will encrypt the data in it. if the data have the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

same encrypted value then it will easily detect the data leak. [3] discussed about a method, End-to-end inference to diagnose and repair the data-forwarding failures, our optimization goal to minimize the faults at minimum expected cost of correcting all faulty nodes that cannot properly deliver data. First checking the nodes that has the least checking cost does not minimize the expected costin fault localization. We construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. We proposes efficient inferring approach to the node to be checked in large-scale networks.

STEPS:

DATA OWNER

1) Gave admin name, email id and password.
2) Browse data owner image.
3) Join in group.
4) New login page is viewed.
5) Gave Email id and password.
6) Gave the text files.
7) It will gave the file size in encrypted format
8) Generate a hash key.

STEPS

DLD PROVIDER

1.Create the datas.

2.Encrypt the datas.

3.Create a hash key.

4.Check wheather the data are same in it.

5. If data are same it will detect data leak.

6. If the data are not same then it will retain in to data

. owner.

5. EXPERIMENTAL RESULT

The following figure shows the proposed system results,

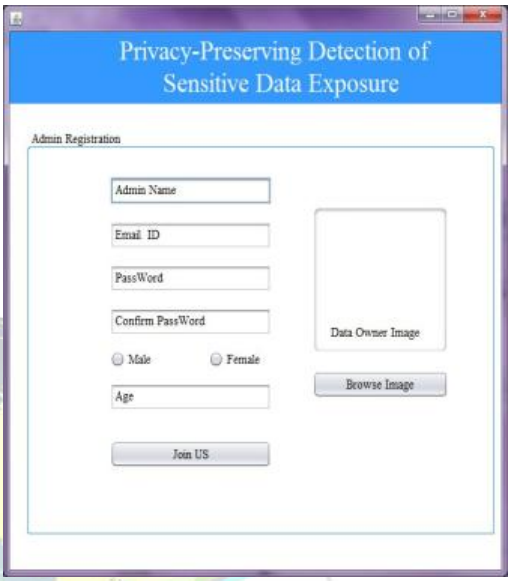

Fig.5. 1 Admin Registration

This fig 5.1 shows about how a data owner can register in it.Here we gave our name, email id and password and image also given to it.

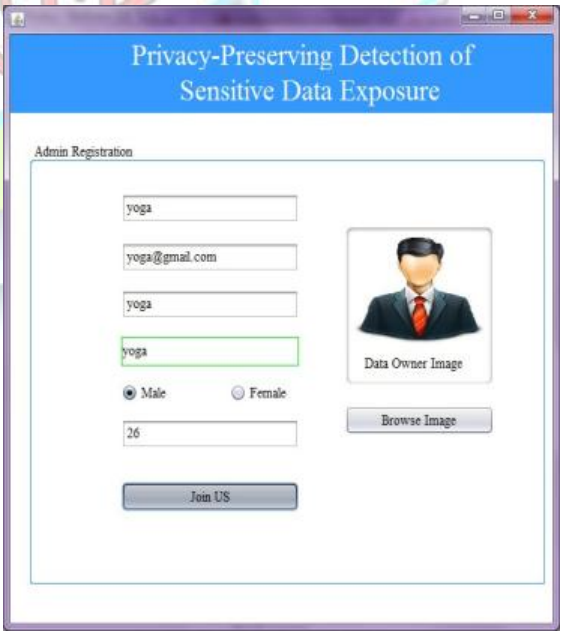

Fig 5.2 joining admin registration

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

This fig 5.2 shows about the name, email id password and data owner image to joining in it.

Fig 5.3 Data Owner Registration

In fig 5.3 shows about the email id and password of the data owner to register it.

Fig 5.4 files created by data owner

In fig 5.4 shows about the data browsed by the data owner. Here lots of data are selected by the data owner and their file name is created in it.

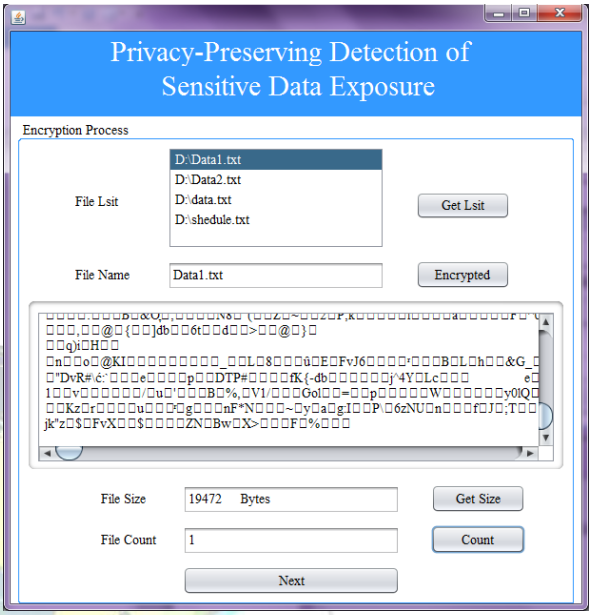

Fig 5.5 Encrypted value of data selected by data owner.

In fig 5.5 shows the encrypted value of any one of the data that is selected by the data owner. It will also gave about the file size and file count present in it. After encryption is completed then click the next button. At that time a hash key window is created by data owner.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

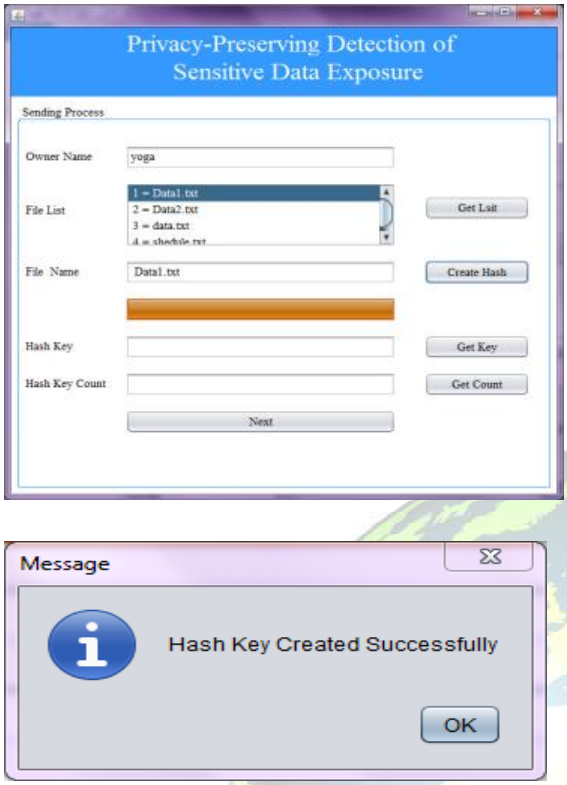

Fig 5.6 Hash key created by data owner

In fig 5.6 shows about the hash key that is created by the data owner .After creating the hash key the data are sent to DLD provider.

In the same way DLD also provide some data and we can see the file name, file count also be obtained. After that the DLD created a hash key for the data provider. Then the both hash key will be compare by using fuzzy finger prints. If the encrypted hash key value is same then it will detect the data leakage.

Fig 5.7 Data Leak Detected

In fig 5.7 will describe about the comparison of the hash key that is created by the data owner and DLD provider. By using the SHA algorithm we can easily detect the data leakage in it.

6. CONCLUSION

In this proposed system, data leakage is easily detected by comparing the hash keys provided by the data owner and DLD provider .This algorithm is much more faster and secure when compare to previous algorithm. For comparing the hash key we use fuzzy finger print technique. The privacy is very because all data are obtained as text format and it is encrypted.

REFERENCES

[1]F. Liu, X. Shu, D. Yao, and A. R. Butt, "Privacy-preserving scanning of big content for sensitive data exposure with MapReduce," in Proc. ACM CODASPY, 2015.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 6, April 2017

[2] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in Proc. 33th IEEE Conf. Comput. Commun., Apr./May 2014, pp. 2112–2120.

[3] Christo Ananth, Mary Varsha Peter, Priya.M., Rajalakshmi.R., Muthu Bharathi.R., Pramila.E., "Network Fault Correction in Overlay Network through Optimality", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Volume 2, Issue 8, August 2015, pp: 19-22

[4] K. Borders and A. Prakash, "Quantifying information leaks in outbound web traffic," in Proc. 30th IEEE Symp. Secur. Privacy, May 2009, pp. 129–140.

[5] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing system-wide information flow for malware detection and analysis," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 116–127.

[6] K. Borders, E. V. Weele, B. Lau, and A. Prakash, "Protecting confidential data on personal computers with storage capsules," in Proc. 18th USENIX Secur. Symp., 2009, pp. 367–382.

[7] A. Nadkarni and W. Enck, "Preventing accidental data disclosure in modern operating systems," in Proc. 20th ACM Conf. Comput. Commun. Secur., 2013, pp. 1029–1042.

[8] A. Kapravelos, Y. Shoshitaishvili, M. Cova, C. Kruegel, and G. Vigna, "Revolver: An automated approach to the detection of evasiveweb-based malware," in Proc. 22nd USENIX Secur. Symp., 2013, pp. 637–652.

[9] X. Jiang, X. Wang, and D. Xu, "Stealthy malware detection and monitoring through VMM-based 'out-of-the-box' semantic view reconstruction," ACM Trans. Inf. Syst. Secur., vol. 13, no. 2, 2010, p. 12.

[10] G. Karjoth and M. Schunter, "A privacy policy model for enterprises," in Proc. 15th IEEE Comput. Secur. Found. Workshop, Jun. 2002, pp. 271–281.