International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 8 Issue 07 Series. II || July 2019 || PP 44-48

"Secured Data Retrieval Disruption tolerant network"

Noori saba Sheikh, Manish Rai
(Computer Science Department, RKDF College RGPV University Bhopal, India)
Corresponding Author : Noori Saba Sheikh

Abstract : *The information leak of sensitive data on systems has a serious threat to organization data security. Statistics show that the improper encryption on files and communications due to human errors is one of the leading causes of information loss. So there a need tools to identify the exposure of sensitive data by monitoring the content in storage and transmission. However, detecting the exposure of sensitive data information is challenging due to data transformation in the content. Transformations result in highly unpredictable leak patterns. In this paper, the sequence alignment method used for detecting data leak patterns. This algorithm is designed for detecting long and inexact sensitive data patterns. This detection is paired with a comparable sampling algorithm, which allows one to compare the similarity of two separately sampled sequences. The method have efficient detection accuracy in recognizing pattern data leaks. It implement a the algorithms in data processing to get high analysis data. In the case of collective privacy preservation, organizations have to cope with some interesting conflicts. The personal information verifies by analysis processes that give new facts about users' shopping patterns, hobbies, or preferences, these facts could be used in recommender systems to predict or affect their future shopping patterns. In general, this scenario is beneficial to both users and organizations. However, when organizations share data in a collaborative project, the goal is not only to protect personally identifiable information but also sensitive knowledge represented by some strategic patterns. To demonstrate the high multithreading scalability of the data leak detection method required by a requirement of organization.*

Keywords : *Information leak detection, content inspection, sampling, alignment, dynamic programming, sensitive data patterns.*

Date of Submission: 07-07-2019 Date of acceptance: 25-07-2019

I. Introduction

To minimize the exposure of sensitive data and documents, an organization needs to prevent clear text sensitive data from appearing in the storage or communication. In today's increasingly digital world, there is often a tension between safeguarding privacy and sharing information. Although, in general, sensitive data clearly needs to be kept confidential data owners are often motivated, or forced, to share sensitive information Privacy-Preserving Sharing of Sensitive Information , and proposes one efficient and secure instantiation that functions as a privacy shield to protect parties from disclosing more than the required minimum of sensitive information. We model in the context of simple database-querying applications with two parties: a server that has a database, and a client, performing simple disjunctive equality queries Detecting the exposure of sensitive information is challenging due to data transformation in the content. Transformations result in highly unpredictable leak patterns. In this paper, we utilize sequence alignment techniques for detecting complex data-leak asymmetric cryptography, facilitate the creation of a verifiable association between a public key and the identity other attributes of the holder of the corresponding private key, for uses such as authenticating the Identity of a specific entity, ensuring the integrity of information, providing support for non repudiation, and establishing an encrypted communications section.

Most of the networks offer a distribution of many data among many users with the assistance of wireless devices. For these infrastructure, a network provide a safe statement amongst the network for data transmission to the all members/users in the grid. With the wireless community, relocation of records wherein performed with the help of the intermediary node. In node, data may be lost cause of unapproved user/member in the community may also slave the records. Disruption-tolerant community (DTN) is a technical process were enables the hub to Interact with one another in at secure way. One of the effective keys for transmitting the data over the network. The majority of the military clients utilize the innovation for protected exchange of the information. In the extensive amount of exceeding viable situation such as military, each and everything in light of the another bases to communicate the information firmly and keep up the information too in the ordered medium

II. BRIEF LITERATURE SURVEY

sno	Author	name	Method	problem	year
1	Sung-Hwan Chung	Big data analysis system concept for detecting unknown attacks	analysis techniques that can extract information	Does not detect future Advanced Persistent Threat	2017
2	Dr.Kiran Joyti	Big Data Analytics with Hadoop to analyze Targeted Attacks on Enterprise Data	Security and Information Event Monitoring	find hidden patterns	2017
3	Bhawna Gupta	Zero Day Attack Signatures Detection	Using Honeypot	Unexpected behavior	2018
4	Dajiang Lei Liping Zhang	Cloud Model based Outlier Detection Algorithm for Categorical Data	. LCS algorithm	detection efficiency	2017
5	Fuye Han, Junwei Cao	Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management	Botnets	Distributed Denial of Service	2016
6	Jing Zhang	Fast Detection of Transformed Data Leaks	sequence alignment techniques	complex data-leak	2016
7.	Sung-Hwan Ahn	Analysis system concept for detecting unknown attacks	analysis techniques	Unknown Attacked	2015
8	Liping Zhang	Cloud Model based Outlier Detection Algorithm	Outlier detection algorithm	faulty behavior	2016
9	Zhen Chen	Internet security problems major challenge	distributed security	phishing attacks	2015
10	Bhawna Gupta, Dr.Kiran Joyti	Data Analytics with Hadoop to analyze	correlations	vulnerabilities and intrusions	2015
11	Boyang Wang,	Toward Practical Privacy-Preserving Frequent	computation-intensive mining process	minor trade-off of privacy	2017
12	R. Agrawal, R. Srikant	Fast algorithms for mining association rules,	**Threat Model**	intrusion detection	2015
13	S. J. Rizvi and	Maintaining data privacy in association	Apriori algorithm.	privacy-preserving	2014
14	W. K. Wong	Security in outsourcing of association rule mining	intersection cardinality protocol	anonymization preserves	2016
15	L. Chen	When private set intersection meets big data	leveraging a minor leakage of privacy	stronger privacy guarantee.	2015

Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System: Zhen Chen*, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen.1, February 2013. Internet security problems remain a major challenge with many security concerns such as Internet worms, spam, and phishing attacks. Botnets, well-organized distributed network attacks, consist of a large number of bots that generate huge volumes of spam or launch Distributed Denial of Service (DDoS) attacks on victim hosts. A distributed security overlay network with a centralized security center leverages a peer-to-peer communication protocol used in the UTMs collaborative module. These new security rules are enforced by collaborative UTM and the feedback events of such rules are returned to the security center. Collaborative network security management system can not identify the intrustion.[6] Understanding privacy in data mining requires understanding how privacy can be violated and the possible means for preventing privacy violation. In general, one major factor contributes to privacy violation in data mining: the misuse of data. Users' privacy can be violated in different ways and with different intentions. Although data mining can be extremely valuable in many applications (e.g., business, medical analysis, etc), it can also, in the absence of adequate safeguards, violate informational privacy.

IV . Problem Detected

The evaluate the accuracy of our solution with several types of datasets under a multitude of data leak scenarios. This module allows the user to register their identity into the system with proper input parameters. The key generation centers play a vital role in it, which generates secret parameters . The key authorities consist of a central authority and multiple local authorities. taking account that there are secure and trusted communication between super authority and each local authority during the initial key and key generation . Each local authority gets different attributes and issues corresponding attribute keys to users. They give differential access rights to individual users based on the users' attributes. The key authorities are provide secured key. That is, they will execute the assigned tasks in the system they would like to information of encrypted contents.

V. PROPOSED SYSTEM

The purpose of this proposed work is to provide the functions as a privacy to protect parties from disclosing more than the required minimum of their respective sensitive information. Usage for prompts many problem, The experimental results attest to the practicality of achieved privacy features and show that our approach incurs quite low overhead. For efficient attack detection, big data incorporates attack analytical procedures into the data leak detection processes. There is a note that the does not intend to improve any of the existing data content leakage algorithms indeed, employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

The proposed method has several advantages.

1. To avoid the attacker.
2. Secrecy of the data should be maintained.
3. The scheme is robust to withstand brute force attacks.

The privacy in data mining requires to how privacy can be violated and the any means for preventing privacy violation. One main factor contributes to privacy violation in data mining the misuse of data. Users' privacy can be violated in different ways and with different intentions. the not proper adequate safe protects, violate informational privacy. Privacy can be violated if personal data are used for other purposes subsequent to the original transaction between an individual and an organization when the information was collected (Culnan, 1993).

One of the sources of privacy problem is known as data magnets (Rezgui et al., 2003). Data magnets are method and tools used to collect personal data. The method include explicitly collecting information through registration, identifying users through IP addresses, software downloads that require registration, and indirectly getting the information for secondary usage. In many cases, users may or may not be aware that information is being collected or do not know how that information is collected. The collected user data can be used for secondary usage beyond the users' access control and privacy laws. This has led to an uncontrollable privacy violation not because of data mining, but fundamentally because of the misuse of data.

- Individual privacy preservation: The primary goal of data privacy is the protection of personally identifiable information. The information is considered personally identifiable if it can be linked, directly or indirectly, to an individual person. when personal data are taken in for to mining, the attribute values linked with individuals are private and must be protected from disclosure Miners are then able to learn from global models rather than from the characteristics of a particular individual.
- Collective privacy preservation: Protecting personal data may not be enough. There is necessary to protect data against sensitive knowledge representing the activities of a group. The protection of sensitive knowledge as collective privacy preservation. The goal here is similar to that one for databases, in which security control mechanisms provide aggregate information about groups and, at the same time, prevent

disclosure of confidential information about individuals. It, unlike as is the case for databases, the main objective of collective privacy preservation is to protect sensitive knowledge that can provide competitive advantage in the commercial world.

In the case of collective privacy preservation, organizations have to scope with some interesting problem. The information analysis processes that produce new facts about users' shopping patterns, hobbies, or preferences, these facts could be used in recommender systems to predict or affect their future shopping patterns. This scenario is beneficial to both users and organizations. When the share data in a collaborative system, the aim is not only to protect personally identifiable information but also sensitive data knowledge represented by some strategic patterns. To increase the security level this proposed scheme overcomes the limitation of "Hybrid encryption algorithm proposed . The proposed enhanced scheme has Triple DES, MD5and RSA. Triple DES strengthens the security of Data transmission. The purpose behind for selecting triple DES rather than Double DES is that in double DES algorithm the key used for encryption and decryption is suspected to middle man attack. key distribution problem and in addition to this, MD5 to verify the data of the message. The message digest algorithm in combination of cryptographic algorithm.

VI. Conclusion

The corresponding attribute group keys are updated and delivered to the valid attribute group members securely . In addition, all of the components encrypted with a secret key in the ciphertext are re encrypted by the storage node with a random , and the ciphertext components corresponding to the attributes are also re encrypted with the updated attribute group keys. Even if the user has stored the previous ciphertext exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the pervious ciphertext..

VII. Future work

Detecting multiple common data leak scenarios. The parallel versions of our prototype provide substantial speedup and indicate high scalability of our design. For future work, we plan to explore data-movement tracking approaches for data leak prevention on a host. Privacy guarantees are formally defined and achieved with provable security.

References

[1]. Hiroki Nishiyama, Desmond Fomo, Zubair Md. Fadlullah,, and NeiKato,Fellow," Traffic Pattern Based Content Leakage Detection for Trusted Content Delivery Networks" IEEE Transaction on Parallel and Distributed System , Volume 25, No 2 Feb 2014

[2]. K. Ramya, D. RamyaDorai, Dr. M. Rajaram "Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns" IJC A 2011

[3]. A. Asano, H. Nishiyama, and N. Kato, "The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection" Proc. Int'l Conf. Computer Comm. Networks (ICCCN '10), pp. 1 6, Aug. 2010.

[4]. Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture," Proc.ACM SIGCOMM, pp. 55 67,Aug. 2010

[5]. O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intell igent Environments, pp. 25 - 30, 2008

[6]. M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments," Proc. IEEE Global Telecomm. Conf., pp. 1 5, Nov./Dec. 2006.

[7]. S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541 553, Sept./Oct. 2006.

[8]. R.S. Naini and Y. Wang, "Sequential Traitor Tracing," IEEE Trans. Information Theory, vol. 49, no. 5, pp. 1319 1326, May 2003.

[9]. D. Geiger, A. Gupta, L.A. Costa, and J. Vlontzos, "Dynamic Programming for Detecting, Tracking, and Matching Deformable C ontours," Proc. IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 3, pp. 294 302, M ar. 1995

Examples follow:

Journal Papers:

[10]. M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116.

Books:

[11]. R.E. Moore, Interval analysis (Englewood Cliffs, NJ: Prentice-Hall, 1966).

Chapters in Books:

[12]. P.O. Bishop, Neurophysiology of binocular vision, in J.Houseman (Ed.), Handbook of physiology, 4 (New York: Springer-Verlag, 1970) 342-366.

Thesis:

[13]. D.S. Chan, Theory and implementation of multidimensional discrete systems for signal processing, doctoral diss., Massachusetts Institute of Technology, Cambridge, MA, 1978.

Proceedings Papers:

[14]. W.J. Book, Modelling design and control of flexible manipulator arms: A tutorial review, Proc. 29th IEEE Conf. on Decision and Control, San Francisco, CA, 1990, 500-506

Noori Saba Sheikh "Secured Data Retrieval Disruption tolerant network" International Journal of Engineering Science Invention (IJESI), Vol. 08, No. 07, 2019, PP 44-48