"ENHANCE SECURITY PRIVACY PRESERVING FOR CONTENT LEAKS"

Shradha V. Raghorte
Student Of M.Tech.(CSE)
R.C.E.R.T
Chandrapur, India
email: shradharaghorte16@gmail.com

Dr . Rahila Sheikh
Department (CSE)
R.C.E.R.T
Chandrapur, India
*email:*rahila.patel@gmail.com

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, it is utilize sequence alignment techniques used for detecting complex 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 system achieves good detection accuracy in recognizing transformed leaks. It implement a parallelized version of our algorithms in graphics processing unit to achieves high analysis data. In the case of collective privacy preservation, organizations have to cope with some interesting conflicts. For instance, when personal information undergoes 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. 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.*

KeyWords: Information leak detection, content inspection, sampling, alignment, dynamic programming.

I. INTRODUCTION

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, It Is Utilize Sequence Alignment Techniques Used For Detecting Complex 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 System Achieves Good Detection Accuracy In Recognizing Transformed Leaks. It Implement A Parallelized Version Of Our Algorithms In Graphics Processing Unit To Achieves High Analysis Data. In The Case Of Collective Privacy Preservation, Organizations Have To Cope With Some Interesting Conflicts. For Instance, When Personal Information Undergoes 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. 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.

II. PROPOSED SYSTEM

1) Key authorities: they are key generation centers that generate public/secret parameters for. The key Authoritiesconsist of a central authority and multiple local authorities. We assume that there are secure and Reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

2) storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static . Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious.

3) sender: this is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attributebased) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4) User: This is a mobile node who wants to access the data stored at the storage node. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext-policy attribute-based encryption (cp-abe) and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; they should be still able to issue secret keys to users.

III. DESIGN MODULES

1. Identity Authorization module :

User module

In this module, user should register their details and get the secret key for login and user can the clients uploaded files the users are able to access the content stored , depending on their access rights which are authorizations granted by the on the bases of the rights re-store the modified data.

Client Module

In this module, a **client** makes use of provider's resources to store, retrieve and share data with multiple users. A **client** can be either an individual or an enterprise. **client** can check the uploaded file he can upload the file. **client** can view the file based on this **client** data.

2. Encryption module :

In this module can view all the user details , **client** uploads clients details and clients activities. Regarding this it Secure **client side** in Storage Environments. In this module , the clients uploaded files can be stored in database it can be very secure .clients can view the file from the database based on the factor it can be very secure. Data encryption using 3 DES .The encrypt method goes like this. the cipherMode of the tripleDES cryptographic service provider. We used the **ECB(Electronic Code Book).**

3. Server verification module:

Starting the server In order to start accepting connections of clients and a client is authorized or not it should be verify.In This we select the path in which only authorize person can access the file form the path.

4. Key generator module:

MD5 algorithm .A commonly used technique in the Internet is to provide a MD5 – Hash.String so the receiver can compare if the file has been transmitted without any modifications.

5. Detection of attack:

The intrusion detection is defined as a mechanism for a PACKET IN NETWORK to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.

IV. CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION (CP-ABE)

Ciphertext-policy attribute-based encryption (CP-ABE) encrypts a 64-bit block of plaintext to 64-bit block of ciphertext. It usesa 128-bit key. The algorithm consists of eight identical rounds and a "half" round final Transformation. There are 216 possible 16-bit blocks: ,. Each operation with the set of possible 16-bit blocks is an algebraic group. Bitwise XOR is bitwise addition modulo 2,and addition modulo 216 is the usual group operation. Some spin must be put on the elements – the 16-bit blocks – to make sense of multiplication modulo 216 + 1, however. 0 is not an element of the multiplicative group.

Fig 1. Data Encryption system

Confidentiality : In order to protect sensed data and communication exchanges between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. Furthermore, while confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station. Hence, confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information.

Integrity and Authentication : authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that

Fig2. Secured Data retrieval system

Safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still authenticate themselves to the network. Hence authentication mechanisms should be "collective" and aim at securing the entire network. In particular, the following requirements must be supported by the key management scheme, in order to facilitate data aggregation and dissemination process: First we focused on the establishment of trust relationship among wireless sensor nodes, and presented a key management protocol for sensor

networks. The protocol includes support for establishing four types of keys per sensor node: individual keys shared with the base station, pair wise keys shared with individual neighbouring nodes, cluster keys shared with a set of neighbours, and a group key shared with all the nodes in the network. We showed how the keys can be distributed so that the protocol can support in-network processing and efficient dissemination, while restricting the security impact of a node compromise to the immediate network neighbourhood of the compromised node. Applying the protocol makes it really hard for an adversary to disrupt the normal operation of the network.

Safety-Critical Applications Require Authentication, It Is Still Wise To Use It Even For The Rest Of Applications Since Otherwise The Owner Of The Sensor Network May Get The Wrong Picture Of The Sensed World Thus Making Inappropriate Decisions.

Fig 3. Authentication Process

If Multiple Users Collude, They May Be Able To Decrypt A Cipher Text By Combining Their Attributes Even If Each Of The Users Cannot Decrypt The Cipher Text Alone They May Succeed In Decrypting A Cipher Text Encrypted Under The Access Policy To Decrypt The Secret Information By Combining Their Attributes. We Also Consider Collusion Attack Among Curious Local Authorities To Derive Users' Keys. Thus, Users Are Not

Fig 4. Key verification

Required To Fully Trust The Authorities In Order To Protect Their Data To Be Shared. The Data Confidentiality And Privacy Can Be Cryptographically Enforced Against Any Curious Key Authorities Or Data Storage Nodes In The Proposed Scheme.

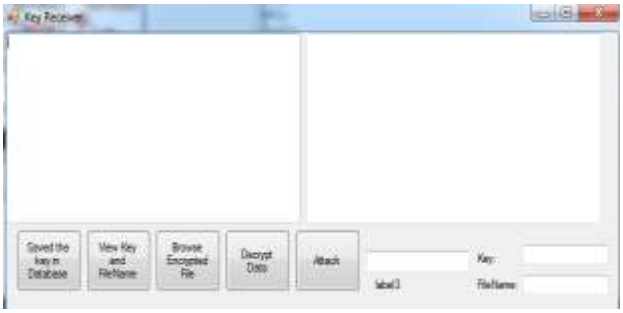

Fig 5. Secured Data Retrieval

Traffic Attacks: Traffic Flooding Attacks Send A Huge Volume Of Flood Attack, Udp And Lan Packets To The Target. Legitimate Requests Get Lost And These Attacks May Be Accompanied By Malware Exploitation.

Bandwidth Attacks: This Ddos Attack Overloads The Target With Massive Amounts Of Junk Data. This Results In A Loss Of Network Bandwidth And Equipment Resources And Can Lead To A Complete Denial Of Service.

Application Attacks: Application-Layer Data Messages Can Deplete Resources In The Application

Layer, Leaving The Target's System Services Unavailable.

V. RESULT

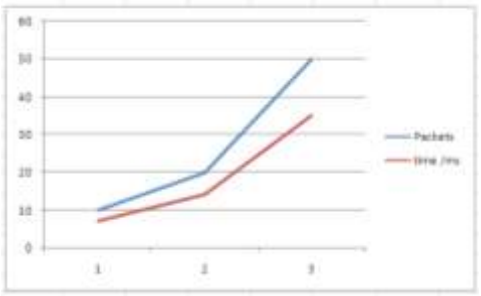

Fig 2. Packet Delivery Ratio

VI. CONCLUSION

The corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key in the ciphertext are reencrypted by the storage node with a random ,and the ciphertext components corresponding to the attributes are also reencrypted 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.

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.

[10] H. A. Kholidy, F. Baiardi, and S. Hariri, "DDSGA: A data-driven semi-global alignment approach for detecting masquerade attacks," IEEE Trans. Dependable Secure Comput., vol. 12, no. 2, pp. 164–178, Mar./Apr. 2015.

[11] S. F. Altschul, W. Gish, W. Miller, E. W. Myers, and D. J. Lipman, "Basic local alignment search tool," J. Molecular Biol., vol. 215, no. 3, pp. 403–410, Oct. 1990.