IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 10, October. 2019, Series -IV, PP 68-72

Hybrid Secured Data Retrieval Disruption tolerant network

Noorisaba Sheikh
RKDF College of Engineering and technology Bhopal , Madhya Pradesh
Corresponding Author: Noorisaba Sheikh
Received 16 October 2019; Accepted 31 October 2019

Abstract: The sensitive data information leak of on systems has a big threat to system data. Research show that the encryption on files and communications due to human errors is one of the leading causes of information loss. However, finding the exposure of sensitive data information is important due to data transformation in the content. Transformations result in highly unpredictable leak patterns. In this paper, the sequence alignment techniques for detecting data-leak patterns. This algorithm is designed for detecting long and inexact sensitive data patterns. The system has detection accuracy in recognizing data leaks. To demonstrate the high multithreading scalability of the data leak detection method required by a requirement of organization.

Key Words: Information leak detection, content inspection, sampling, alignment, dynamic programming, etc.

I. INTRODUCTION

To reduce the excess of sensitive data documents, an company needs to prevent cleartext 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 leak of sensitive information is challenging due to data transform in the other type. Transformations result in highly unpredictable leak patterns. In this, utilize sequence alignment applying techniques for detecting difficult 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. Knowing privacy in data mining which understanding the privacy can be misused and the means for preventing privacy leak. The one important factor c to privacy violation in data mining the misuse of data. Users' privacy can be misused in different types and with different ways. Were data mining can be very valuable in many applications , it can also, in the absence of adequate safeguards, violate information. Privacy can be miss used if personal data

II. RELATED WORK

Uncertain cyber-attacks has been increasing due to existing security systems are not able to detect them. Analysis techniques for Big data that can extract information from a different sources to detect new attacks. The generation of all unknown attacks, detection rate becomes very low and false negative increases. To defend against these unknown attacks. Does not detect future Advanced Persistent Threat (APT) detection.[1]

Analytics Big data security is used for the security practice of companies to gather and analyze security data to detect vulnerabilities and intrusions. Security and Information Event Monitoring system. Various malicious attacks have main subject for government, organization or industries . Analytics Big data is the process of finding big data to find patterns hidden, unknown correlations and other useful information that can be extracted to make better decisions. It is used effectively and at the same time, hackers can leave their targets forever.[2]

Unexpected behavior. Fault distribution studies show that there is a correlation between the number of lines of code and the number of faults. For the LCS algorithm which will on the packet content of connections going to the same services. DayZero attack is a threat that tries to exploit r application vulnerabilities that are unknown to others or undisclosed to the software developer. Vulnerability window which is the time between

the first exploitation of vulnerability and when software developers start to develop a countermeasure to that threat. [3]

Numerical data but there will be a large number of categorical data in real life. Some outlier detection algorithm shave been designed for categorical data. There are two main problems of outlier detection for categorical data, which are the similarity measure between categorical data objects and the detection efficiency. Outlier detection algorithm for categorical data. Efficient outlier detection can help us make good decisions on erroneous data or prevent the negative influence of malicious and faulty behavior. Many data mining techniques try to reduce the influence of outliers or eliminate them entirely. The in formation manner may result in the loss of important hidden information.[4][5]

III. PROPOSED SCHEME

1) Identity Key Generation The key generation module helps the users to share the information between source and destination. when the confirmation results from the receiver side the sender will correct the information along with encryption . Every time a key will be created and sent to the receiver area. the hybrid key is has the access for decrypt the data at receiver end. As the value that stores data from senders and provide the access to users. It may be any type. As the existing method , and also the storage node to be least trusted.
2) 3DES Based Encryption In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The method can be formed with the attributes. In access policy is sent along with the ciphertext. A method uses the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This method encrypted data can be kept confidential all thought storage server is untrusted. Moreover, our methods are secure against collusion attacks. Previous Attribute The systems works on attributes to secure the encrypted data by Enhance Encryption and built policies into user's keys while in our system attributes are used to describe a user's credentials, and a party encrypting content secure a policy for which can decrypt.
3) Confidential Data Interchange This is an entity who owns confidential messages or data and wishes to store them into the external data storage node for ease of sharing and for secured delivery to in the extreme networking environments. A sender is has right for defining access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node. This is a hop node which to access the data stored at the storage node. If a user has a set of attributes give the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then it will be able to decrypt the cipher text to retrieve the data.
4) Administrative Access Controller The administrator owns full access rights of this entire site. Once the administrator find out any illegal activity or other misusing happens into the way of transaction between the respective sender and receiver then the admin immediately block the user access rights to transact using this site. The block will be unblocked after getting meaningful reason from the user end.

IV. ALGORITHMS

The encrypted key used component gets the client to share the information between client to server destination. After verification the confirmation response from the receiver side the sender fix the information and encrypt it. When a time a key will be generated and sent to the receiver area. Hybrid key is useful for data at receiver end. Similar to the preceding methods, and also suppose the storage nodule to partially confidence that is truthful but curious. A key aggregate encryption system has of polynomial time algorithms as follows. The data has the public system parameter and generates a KeyGen. Messages can be encrypted by anyone decides what ciphertext class is associated with the plaintext message to be encrypted. The data can use the mastersecret to generate an secured decryption key for a set of ciphertext classes via Extract. The generated keys can be passed to delegatees securely (via secure e mails or secure devices) Finally, any user with an aggregate key can decrypt any ciphertext provided that the aggregate key is in ciphertext's class is contained in.

1. Implementation of 3DES ALOGRTHIM
2. 3DES encrypts a 64-bit block of plaintext to 64-bit block of ciphertext.
3. It uses a 128-bit key. The By HasMD5algorithm consists of eight identical rounds and a *"half" roundfinal Transformation.*
4. There are 216 possible 16-bit blocks: 0000000000000000,11111111111111

Flow chart

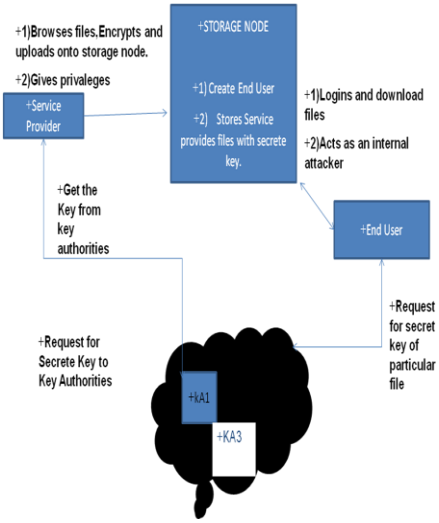


Figure 1 Dataflow diagram

V. EXPERIMENTAL ANALYSIS

The A typical setting involves two parties: one that seeks information from the other that is either motivated, or compelled, to share (only) the requested information. Consequently, in numerous occasions, there is a tension between information sharing and privacy. The other way sensitive data has to be kept confidential, data owners may be willing, or forced, to share information. The hybrid secured the accuracy of our solution with several types of datasets under a multitude of real-world data leak scenarios.

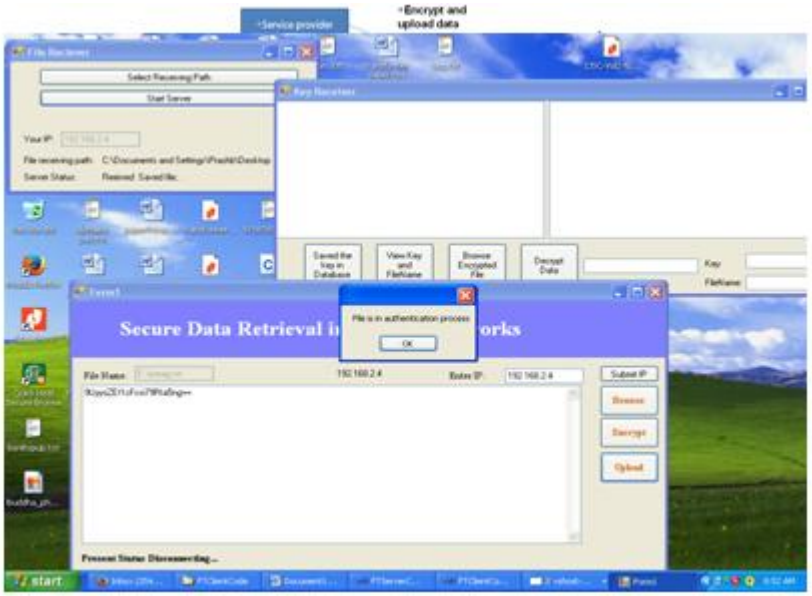
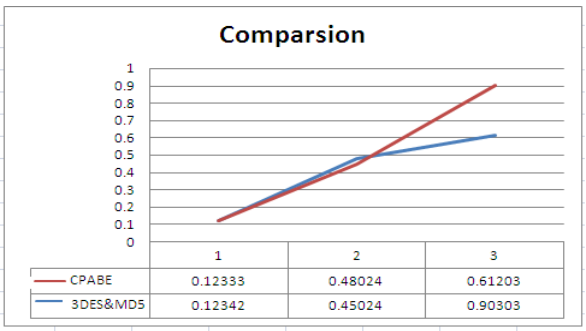


Figure 3. Data Verification system



Characteristics	Exiting Scheme	Developed Scheme
Platform	.Net framework	.Net framework
Keys Used	Same Key Is Used For Encryption And Decryption Purpose.	Same Key Is Used For Encryption And Decryption But Additional Authentication Key Is Used.
Scalability	It Is Scalable Algorithm Due To Varing The Key Size.	It Is Scalable Algorithm Due To Varing The Key Size And Used Of Different Keys For Authentication.
Security Applied To	Only From Providers Side.	Both Providers And Client Side.
Authenticationtype	Key Authentication Used.	Hybrid Data + Key Encryption Authentication Is Used.
Security	Single Encryption Used.	Double Encryption And Authentication Also Used.

Figure 4 Result Comparison

In my project security is combination of more algorithm than base paper still requires less time to

Verify and process.
These are not present in the base paper in my project to enhance the security we use combination of algorithm.

1. Idea algorithm
2. MD5
3. ECB (ELECTRONIC CODE BOOK)
4. Hashing code

Confidentiality :

In order to protect sensed data and communication ex-changes between sensor nodes it is important to guarantee the secrecy of messages. In the node network case this is gets achieved by the use of symmetric cryptography as asymmetric key cryptography in general is considered too expensive. However, while encryption protects for outside attacks, but it does not secured against inside attacks compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. Further, which gives confidentiality gives the security of data 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 Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that 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:

Intermediate Data aggregation is only nodes have access to encrypted data so that they can extract measurement values and apply to them aggregation functions. Therefore, nodes hop send data packets to the base station which encrypt them with keys to the aggregator nodes.

Data dissemination implies broadcasting of a message from the aggregator to its group members. If an shares a other key with each of the sensor within its group, then it will have to make multiple transmissions, encrypted each time with a different key, in order to broadcast a message to all of the nodes. The data transmissions is as low as possible due to their high energy consumption rate. The blue line show that in same amount of time we encrypt more data with hybrid algorithm were as in previous the red line show that with the same amount of time it encrypt less data with single algorithm.

The Previous Technique contents, the low Encryption Method, Single layer Still it required more time for the encryption of data. Since, our technique consists of hybridization of two Method still, it required less time as compare to the previous method. The y axis give the data packet size and the x axis gives time require for encryption. the previous method only protect data from insider attacks but it does not protect the data from outsider attacks so it only has the data security upto 70% but in your method of hybrid we protect the data from insider as well as outsider so your method give 90 % of secured data system.

VI. CONCLUSION

Detecting multiple common data leak scenarios. The parallel versions of our prototype provide substantial speedup and indicate high scalability of our design. r future system, the explore data detection tracking approaches for data leak prevention on a host. Privacy guarantees are formally defined and achieved with provable security. Experimental results show that our approach is sufficiently efficient for real world applications. To data efficient secure of multiple attacks tasks, To explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

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. 2530, 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.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Noorisaba Sheikh. "Hybrid Secured Data Retrieval Disruption tolerant network." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 10, 2019, pp. 68-72.