DOI 10.29042/2018-3989-3992

Helix Vol. 8(5): 3989- 3992

Prevention of Data Content Leakage

[1]Meghana N. Jadhav, [2]Prof. Jignyasa Sanghavi

[1]Student Shri Ramdeobaba College of Engineering and Management, Nagpur, India.

[2]Assistant Professor Shri Ramdeobaba College of Engineering and Management, Nagpur, India.

Email: jadhavmn@rknec.edu

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract

The leaks of sensitive data have a major threat to the security of an organization. The statistical details show that the inappropriate encryption on data and transmission caused by individual mistakes is the major reason of data diminution. Hence there is a requirement of functions to recognize the content in database and communication. Although, the recognition of, revelation of sensitive details of data is challenging because of the transmission of information into the contents. The transmission consequences are uncertain leak patterns. In this proposed research work, 3DES and MD5 algorithms are combined in order to improve the security of data that is to be transferred to the outside world. This method provides the satisfactory results by preventing leaks of transformed data. In another case of cooperative preservation of privacy, the association copes with few exciting conflicts. For example, when private information go through the testing procedure that creates new details regarding the individuals patterns, sequences, or priorities and precedence's all these details can be used in recommender systems to guess and influence that future patterns. However, this situation is useful to the individual and the association. Although, when the association allocates the data in the collective project, the aim is to not only protection of individually distinguishable information but also the delicate details shown by few strategic patterns for having the high-level multithread scale-ability.

Keywords: Information Leak Prevention, Triple DES, Message Digest (MD5), Data Encryption (DE), Privacy, Security.

Introduction

Data leak is an illegal transference of data from the firm to the outside. An organization requires to blocking the clear text sensitive to shrink the subjection of the sensitive document or information from emerging in the repository. Nowadays as the world is moving towards digitization so it is very important to protect the privateness and transmission of data. There is consistently stress regarding the privacy and the security. The data owner always required to transmit the sensitive information. The privacy-preserving transferring of sensitive data suggests systematic instantiation that works as a privacy protection that preserves from revealing extra information than the needed information. The recognition of disclosure of sensitive information is the difficult task because of the transferred content.

Many times, the data owner do not familiar with the data is being gathered or not aware of the data is already gathered. In some cases, the personal information may be utilized for alternative use largely exceeding the person's law of security and control. This situation results in privacy infraction that is not controlled not as of data mining, but basically for illegal use of data.

In proposed research work we utilize combination of 3DES and MD5 in order to make transmission of data more secure. We use symmetric key algorithm for encryption to enable the generations of verifiable corporations to ensure the authentic users and the integrity of the transmission of data. With this proposed work, privacy is achieved guaranteed with empirical security and data is protected. Also proposed approach is adequately effective for real-world applications.

Encryption and Decryption Overview

Encryption is a procedure of converting coding of data that can be information, files, message or mails into cipher text. It converts the plaintext into the cipher text coding is done in cipher text form unreadable without key of decode for preventing anyone excluding intended user from read the data.

Decryption is a reverse method. It reverses the encryption for the process of decryption. It transmits the encoded data to plaintext. A key is used for accessing the original data but it has to match the secret key that was generated when encrypting.

Literature Review

Related to the work of data leakage prevention, (Rezgui et al., 2003) introduced the concept of data magnets. The lack of enough safeguards, infract the informational privacy. "One of the, sources of privacy violation is called as data magnet" [1]. Data Magnet is the method and technique that is used for the collection of individual's information. Examples of data magnets consist of explicitly gathering information via online registration, recognize users by IP addresses, downloading of the software that needs registration and incidentally gathering of data for subordinate use.

Croft and Caesar utilised the data tracking over a network and make use of shadow packets to identify leaks [8]. iLeak is a system for prevention of unintended information leaks on a computer
[11]. It makes use of the keyword searching utility present in various operating systems. It also keeps track on file access logs of processes and searches for system call inputs that involve sensitive data. iLeak is designed for securing personal data on a single machine.
Bertino and Ghinita point out the important issue of data leaks in database from the viewpoint of anomaly detection [10]. Normal user activity patterns are observed and structured in DBMS, and anomalous activities are found with respect to potential data leak. Bertino also discussed watermarking and provenance methods used for data leak prevention [4].
Privacy is a very well-known issue in the cloud environment. Lin and Squicciarini proposed a generic data protection model in order to secure data on cloud [3]. They proposed a three-tier data security model for dealing with the data leak caused by indexing [9]. Privacy-preserving data leak preventive model was proposed and further developed in [6] and [7], where data leak preventive operations are outsourced to a semi-honest third-party.

Methods and Techniques:

Proposed System

The motive behind this proposed mechanism is that giving the approach to the functions that act as a privacy protector to secure the data from revealing to the intruder.
For effective security of data, we must note that the design make better of the existing intrusion prevention algorithms. The proposed research method has few of the advantages.
1. Privacy of the information must be preserved.
2. Efficiently managing the data.
3. Dedicated, reliable and safe environment.

•*Privacy preservation*: The main aim of privacy of information is to safety. The information is privately identifiable if it is associated with the person. Hence, when the private data is exposed to mining; the elements related to the person are private and should be secured from exposing. The miners are capable of gaining the knowledge from the universal model than elements of a specific person.

•*Common privacy protection*: It may be not sufficient to protect the personal information or data. We might need securing sensitive knowledge representing movement of an association. We concern to security of data as cumulative privacy security. The aim is much same to prevent the private data regarding to an individual [10].

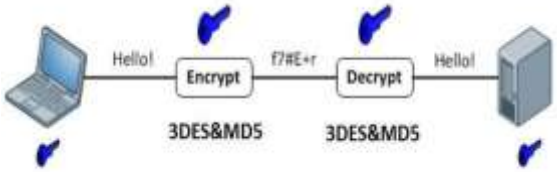

Figure 1: Process of Encryption and Decryption with Symmetric Key.

The goal of common security protection is to secure the confidential that can give the competitive advantages in the world of business Considering the instance of collective privacy preservation, the association have to handle with the absorbing conflicts.

Figure 2: Proposed Approach

When private data is go through the procedure of analysis that provides new detail regarding to the user about the patterns of searching, interests or priorities, these details used by the suggestion system to estimate and influence their prospects searching sequence and patterns [3][6].
This outline is useful to individual and the association both. Proposed research work consists of 3DES and MD5. 3DES is a form of DES (i.e. Data Encryption Standard) which boosts the security of data communication.

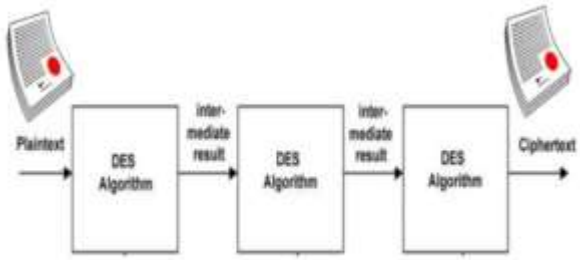

Figure 3: Triple DES

The purpose of choosing 3DES rather than 2DES is the key that is utilized for the purpose of decryption and the encryption might be expected to meet in man-in-middle attack by running the triple DES algorithm

in succession it enlarges the size for giving better security [4]. It produces 64 passes of three blocks through the algorithm. This can be difficult to implement because the resultant file is of 192 bits hence there is option provided in triple DES that execute through a technique called Encrypt-Decrypt-Encrypt (EDE).

1. Encrypt – Encryption is implemented to the data.
2. Decrypt - The encrypted data is decrypted.

3. Encrypt- Ultimately, the decrypted data from second step gets encrypted.

Double DES doesn't actually give us that much more security than DES and the complications of allocation of bits and in addition to triple DES, MD5 to verify the integrity of the data [11]. Thus we have used secure hash algorithm in combination of cryptographic algorithm.

Algorithm for encryption

Steps are as follows:

1. Take a file [F].
2. Perform the 3 DES and MD5 algorithms for encryption and it generates final key as 320-bits.
3. BLOCK= T+DK
4. BLOCK is send to receiver.

With the technique of encryption that is 3DES it is practicable to utilize a 3DES, hardware execution for DES by situating identical values. It gives reverse similarities with the DES. We can also say the individual encryption blocks of plaintext and then can be decryption performed, and then final encryption is performed. MD5 is a 128-bit hash function. Total BLOCK Length is 320 bits Value given by a secure hash function and they are also called as secure hash algorithm or simply hash value.

Algorithm for decryption

1. Received BLOCK= T+DK
2. Check the key if match or not
3. If key match then data decryption
4. Display contents of original File

Result and Discussion

The conceptual design is executed into a running system in the execution stage. Thus most critical stage can be considered as providing the users' assurance that newly developed system will function properly, useful and achieve successful efficient new system. This method provides the satisfactory results by preventing leaks of transformed data. It provides users as well as to the organization security which is of 320 bits and due to this it is very difficult to crack the sensitive data which is most valuable asset of any organisation. Hence, system provides preventive measures for data content leakage.

Figure 4: Original Message

Figure 5: After Applying 3DES and MD5 (Encrypted File)

Figure 6: Generated Secret Key

Conclusion

With this proposed research work, privacy is achieved guaranteed with empirical security. The data is protected from exposure. The observational outcome proves that this approach is adequately effective for real-world applications. We have used highly-secured protection by using the combination of the algorithms. The evaluation of security and performance prove the proposed systems are provably efficient and highly secure.

Nothing can be ended in a single step. So this project also has some future enhancements in the evergreen and booming IT industry in IT world. Change are inevitable. The project entitled "Prevention of data leakage" was successfully designed and developed.

The system and the architecture is a compatible one, so addition of new modules can be done without any difficulty. In future work, data leak prevention can be used with SIEM i.e. Security Information and Event Management for tracking network traffic and logs of devices. A further challenge for future work is to achieve more security by implementing it on big data. We can also develop this system for sharing of other resources like image, video, audio etc.

References

1. Rezgui, A., Bouguettaya, A., &Eltoweissy, M. Y, "Privacy on the Web: Facts, Challenges, and Solutions", IEEE Security & Privacy, 1 (6), 40-49, 2003.
2. Stanley R. M. Oliveira, Osmar R. Za¨ıane. "Revisiting Privacy Preserving Clustering by Data Transformation", Journal of Information and Data Management, Vol. 1, No. 1, 2010,
3. K. Ramya, D. RamyaDorai, Dr. M. Rajaram. "Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns", IJC A, 2011.
4. A. Asano, H. Nishiyama, and N. Kato,"The Effect of Packet Reordering and EncryptedTraffic on Streaming Content Leakage Detection", Proc. Int'l Conf. Computer Comm. Networks (ICCCN '10), pp. 16, 2010.
5. O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment" Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25 – 30, 2008.
6. S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior", KKU Eng. J., vol. 33, no. 5, pp. 541 553, 2006.
7. 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. 15 ,2006.
8. Mr. Sagar Prasad, Ms.Malti Nagle, Mr.Tarique Zeya Khan, "PREVENTION OF DATA CONTENT LEAKAGE WITH SECURED ENCRYPTION ALGORITHM", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5, Issue 12, 2016.
9. 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, 2010.
10. Lakshamana Chari, Dr G. Rama Swamy, "Content Leakage Detection for Trusted Delivery Networks using DRM Technology", International Journal of Computer Engineering In Research Trends,Volume 2, Issue 11,pp. 872-876, 2016.
11. Pooja Pawar, SupriyaPalwe, Shweta Munde, Priyanka Gadhave, Mrs. Shikha Pachouly, "Privacy Preservation and Detection of Sensitive Data Exposure over Cloud", International Journal of Advanced Research in Computer and communication Engineering Vol. 5, Issue 3, 2016.
12. 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, 2014.
13. Xiaokui Shu, Jing Zhang, Danfeng (Daphne) Yao, "Fast Detection of Transformed Data Leaks",IEEE TRANSACTIONSON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, 2016.
14. Shradha V. Raghorte, Dr .Rahila Sheikh, "Security privacy preserving for content leaks", International Journal of Engineering Research in Computer Science and Engineering, Volume 4, 2017.

