A Review on insider Collusion Attack on Text, Video and Image File using Privacy-Preserving Kernel based System

Nilima V. kayarkar Wainganga college of engineering Nagpur

Abstract:- The unauthorized transfer of classified information from computer to outside word is called data leakage.For business purpose, it is necessary to send important data to trusted parties. But from this trusted parties thisinformation is reach at unauthorized place such as website or somebody's laptop. It is very challenging and necessary to detect leakage and guilty person responsible for data leakage.In this system distributor means owner of data and agents means trusted parties. The aim of this system is to find data of owner which is leaked and detect agent who leaked data. In this paper the agent which is responsible for data leakage is the insider. Means agent is a person who is present within the organization.Insider attacks arise not from system errors but from staffworking inside the company's enterprise.

Keywords: *Data leakage, insider attack.*

*****

I. Introduction:

Now a day data breaching problem due to insider attacks are one of the rapidly increase type of attack. Data breaching is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. According to the"2015 Verizon Data Breach Investigations Report" insider attack is increases from 2013 to 2015.In 2013 it is 8% and in 2015 it is 20.6% means it is increases at triple rate. Therefore it is necessary to prevent this attack and also find the guilty person responsible for this attack. Many data mining applications contain large amounts of personal information therefore; extensive research has mainly focused on dealing with privacy breaches.

In proposed system we find the guilty person who responsible for data leakage of text data, image as well as video. To find guilty person we used fake object, means distributor add fake object in the data before distributed to agent.

II. Literature Review

Peter Shaojui Wang, Feipei Lai, Hsu-Chun Hsiao, And Ja-Ling Wu: In this paper, we propose an insider collusion attack that carried out on most data mining systems and it discuss how many insiders are sufficient to do this type of attack. In this system insiders within organizations collude with outsiders. This paper introduced several proposed privacy-preserving schemes to counter this attack.

P.S.Wang, S.-W.Chen: In this paper it combine intelligent dietary planning mobile system with cloud technology. In this system user collect his personal information like weight, height, food, sports etc. and send this information to mobile dietary planning app. Then this app sends information to the cloud server for data analysis. According to this analysis the app provide best diet plan and related suggestion to the user.

Fang Liu, Wee Keong Ng, Wei Zhang: Now a day there is rapid growth in data of many field and industry. Many applications like, large-scale financial and medical data analysis, real-time monitoring and social network need to collect large amount of data from different data sources. Then this data is outsourced to public server. The owner does not have any control on the data after being outsourced. To avoid this problem in this system, data is encrypted first before sending it to the server. Means here data is encrypted as well as outsourced.

Lei Xu, Chunxiao Jiang, Jian Wang, Jian Yuan, And Yong Ren: This paper discussed how to protect important information from the security threats brought by data mining. For this we used user-role based methodology.In this paper we used four different user roles that are commonly used in data mining applications, i.e. data provider, data collector, data miner and decision maker.

Anandarup Sarkar, Sven K¨ohler, Sean Riddle, Bertram Lud¨ascher, Matt Bishop: This paper proposed Data Annotation Step Agent Interaction analysis (DASAI). DASAI is a logic rule-based static analysis approach used when an attack can take place on a process. DASAI determines in which ways the attack can be performed on the process and who are the rogue insiders responsible for this attack. DASAI can be used to improve the processes by making them robust against this attack.

William R Claycomb, Alex Nicoll: In this paper cloud computing services provide resource for organizationsto improve business efficiency but also expose newpossibilities for insider attacks. Fortunately, if any rogue administrator attacks have been successfulwithin cloud service providers but insiders continue to abuseorganizational trust in other ways such as using cloudservices to carry out attacks.

Slawomir Goryczka, Li Xiong, Benjamin C. M. Fung: In this paper, we explained a new type of potential attackers in collaborative data publishing – a coalition of data providers

called as *m*-adversary. To prevent privacy disclosure we introduced a new notion, *m*-privacy to ensure that any *m*-adversary or any of its subsets is not able to compromise the privacy.

Keke Chen, Gordon Sun,Ling Liu: In this paper, we proposed some potential attacks to random geometric perturbation and design several methods which reduce threat of these attacks. Perturbation techniques are often evaluated with two basic metrics first is the loss of privacy and second is the loss of information. An ideal data perturbation algorithm used for minimizing both loss privacy loss and information loss.

Kun Liu, Hillol Kargupta: This paper explains the use of random projection matrices as a tool for privacy preserving data mining. It proves that after perturbation the distance-related statistical properties of the original data are still maintained without divulging dimensionality and exact data values. The experimental results demonstrate that this technique can be successfully applied to different kinds of data mining tasks including inner product/Euclidean distanceestimation, outlier detection correlation matrix computation, clustering, outlier linear classification, etc. The random projection-based technique may be more powerful when used with some geometric transformation techniques like scaling, rotation andtranslation.

III. Existing System:

In this system, we consider new insider threat for privacy preserving work of distributed kernel-based data mining (DKBDM). Now a day data-breaching problems due to insider attacks are the fastest growing attack types. This type of attacks arises not from system security errors but from staff working in the company's enterprise.

In this system, we propose an insider collusion attack that is carried out on most data mining systems. This attack operates on kernels and discusses how many insiders are sufficient for this type of attack.The existing system is used to find the insider guilty person responsible for this type of attack. The limitation of this system is as follows.

1. This system cannot avoid the attack. It only find guilty person responsible for this attack.

2. It only detects the attack which is carried out on text data.

III. Proposed Method:

In this system, model is developed for finding the guilty agents. For this purpose we add fake objects using steganography LSB algorithm while distributing objects to agents. We inject realistic but fake data records to further improve our chances of detecting leakage and identifying the guilty person which is insider.

This system is used to find out attack carried out on text data as well as video and image file. Because now a day attack on video and image file increased rapidly as compared to text data.

The system architecture is defined below with the help of block diagram which explain the overall technique for our system.

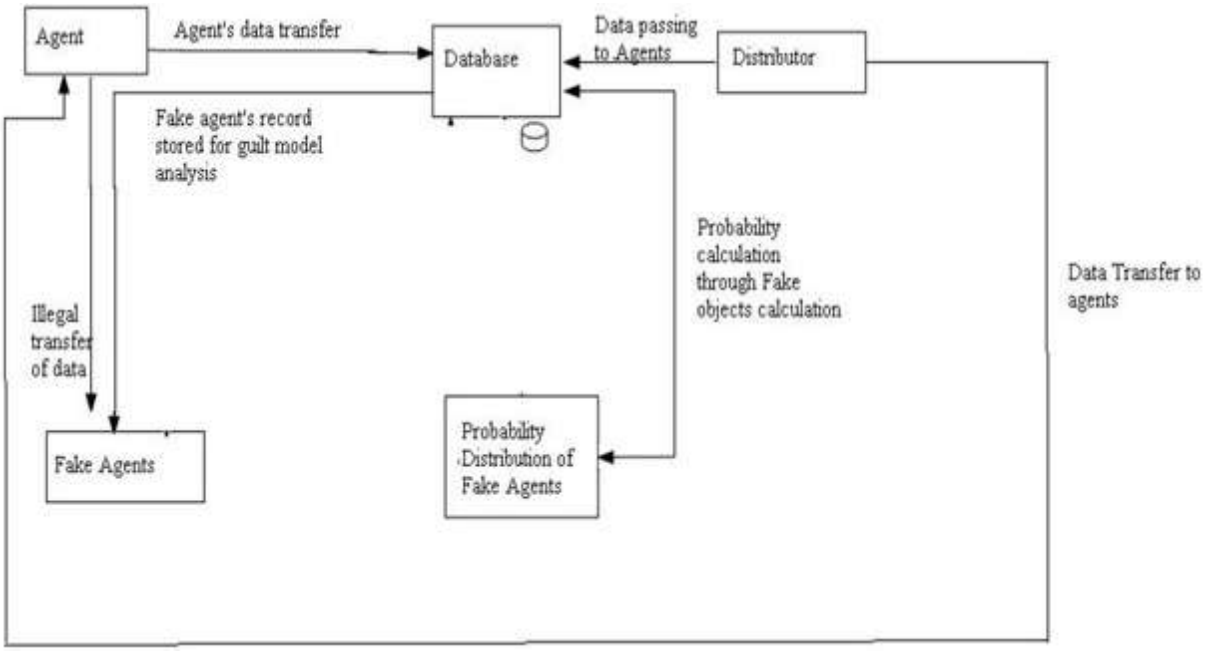

Fig: - Block Diagram of System Architecture

Conclusion:

The propose system can identify the attack carried out only on text data but we can implement the system which can detect the attack carried out on text as well as video or image file. This system is very useful because now day attack on video and image file increased significantly as compared to text data.

Using this system we can increase the security and also find the guilty person which is responsible for attack. Here the guilty person is insider. This system cannot avoid the attack means in this system the exact recovery of data is not possible.

Therefore in future, we can implement the system which can be avoid this attack and protect the system from attacks. Means we increase the security level of the system.

References:

[1] Peter Shaojui Wang, Feipei Lai, Hsu-Chun Hsiao, And Ja-Ling Wu, "Insider Collusion Attack on Privacy-Preserving Kernel-Based Data Mining Systems", *IEEE Trans*, Apr.2016.

[2] P. S. Wang, S.-W. Chen, C.-H. Kuo, C.-M. Tu, and F. Lai, ``An intelligent dietary planning mobile system with privacy-preserving mechanism," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*,Jun. 2015, pp. 336_337.

[3] F. Liu,W. K. Ng, andW. Zhang, ``EncryptedSVMfor outsourced data mining," in*Proc. IEEE Int. Conf. Cloud Comput. (CLOUD)*, Jun./Jul. 2015, pp. 1085_1092.

[4] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, ``Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149_1176, Oct. 2014.

[5] A. Sarkar,S. Köhler, S. Riddle, B. Ludaescher, and M. Bishop, ``Insider attack identification and prevention using a declarative approach," in*Proc.IEEE Secur. Privacy Workshops (SPW)*, May 2014, pp. 265_276.

[6] W. R. Claycomb and A. Nicoll, ``Insider threats to cloud computing: Directions for new research challenges," inProc. IEEE 36th Annu. Comput.Softw. Appl. Conf. (COMPSAC),Jul. 2012, pp. 387_394.

[7] S. Goryczka, L. Xiong, and B. C. M. Fung, ``*m*-privacy for collaborative data publishing," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 10,pp. 2520_2533, *Feb*. 2012.

[8] K. Chen and L. Liu, ``Geometric data perturbation for privacy preserving outsourced data mining," *Knowl. Inf. Syst.*, vol. 29, no. 3, pp. 657_695, Dec. 2011

[9] K. Liu, H. Kargupta, and J. Ryan, ``Random projection-based multiplicative data perturbation for privacy preserving distributed data mining," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 1, pp. 92_106, Jan. 2006.