Survey on Data Leakage Prevention through Machine Learning Algorithms

Er. Garima Agrawal
PhD. Scholar, Dept. of Computer Engineering, Amity University, Gwalior, Madhya Pradesh, India, 474006

Dr. Samta Jain Goyal
Assistant Professor, Dept. of Computer Engineering, Amity University, Gwalior, Madhya Pradesh, India 474006

2022 International Mobile and Embedded Technology Conference (MECON) | 978-1-6654-2020-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/MECON53876.2022.9752047

Abstract: **As the Internet develops and network data transmission keeps on expanding, managers are confronted with the errand of holding private data back from leaving their organizations. In different information leakage cases, information misfortune is caused mostly by human missteps. Currently government associations show that the quantities of information leakage occasions have developed rapidly. One of the significant issues in the data security research is information spillage or information misfortune particularly brought about by insider danger as insider dangers can possibly deliver serious harm to the association's assets, monetary resources and notoriety. Therefore protection and suspection of data detection can restrict the associations from willing to share the information from one another and this is one of the significant errands in the data security. In this paper, we study various literatures showing mitigation of data leakage. There is a need to develop and design a framework or sensitive data detection model for data leakage prevention.**

Keywords: Data leakage, Data misuse, Sensitive Data, Insiders, Network Security, Privacy-Preservation.

I. INTRODUCTION

Privacy protection assumes a significant part to give security to information. Information openness implies unapproved transmission of delicate information to an obscure objective where the classification of data is compromise. Number of information leakage examples have increased quickly in research foundation and government association in ongoing years. Human mix-ups are one of the significant justifications of accidental information leaks. To give protection from the information leakage unique finger impression might be the answer for this issue. The goal is to further develop precision of discovery.

Organization's information is vital and demonstrates as a fundamental constituent in epitomizing the centre of the association's force and this force ought to be saved and kept up with. On the opposite side, this information is needed for day-by-day chipping away at various cycles. Customers inside the association, for example, representatives or accomplices perform various strategies on this information and might be presented to the significant data while getting to the information. Because of this preparing and activity, it may lead to information spillage and abuse. Identifying and forestalling information leakage play out certain means, for example, information leakage discovery, the danger to information security from insider's danger is turning out to be increasingly more basic due to the interminable utilization of the PCs and furthermore correspondence frameworks. Different techniques have been proposed for guarding information from external assaults yet those components neglect to shield information from approved clients who might abuse their advantages in completing malignant exercises.

Literature Survey

S. No	Author Name	Year	Title of Paper	Technique /Method /Algorithm	Research Gap
[1]	Xiang Yu et al.	2018	A Data Leakage Prevention Method Based on the reduction of confidential and context terms for Smart Mobile Devices	The Approach determines cluster graph structure based on data leakage protection based on context model by removing duplicity and noise to detect modified private data.	DLP solutions securities against intentional data leaks as firewalls, IDS, anti-malware, etc. don't prevent intentional data leaks. Hence, topics for the research gap are DLP from mobile devices and accidental data leakage by
[2]	Brunella Karamani	2018	Improving Data Loss Prevention Using Classification	Classification Approach for determining users based on their access to confidential data, & then making a decision which concerns request exceptions.	As Method useful for a financial rise in decision making of institution's need to risk knowledgeable agreement. Financial institutions need to improve policies and procedures for DLP resolution

[3]	Michael Hart et al.	2011	Text Classification for Data Loss Prevention	The Approach determines the method to train classifiers for classification, to achieve data loss prevention. They also proposed a technique that reduces the false-positive rate for files unrelated to enterprises.	The Proposed research uses text content for classification; hence needs to include encrypted and multimedia content & also to investigate how meta data of content improves classification. Also, need to research on non-English sources as sensitive data can be of any language.
[4]	Ghouse & Nene et al.	2020	Graph Neural Networks for Prevention of Leakage of Secret Data	The Approach uses GCN for classification on network and AES encryption is done to achieve data loss prevention for data in transit.	In the future, the primary aim will be on addressing data leakage prevention via smart devices and prevent encrypted data leakage.
[5]	Donlan Liu et al	2020	Research on Leakage Prevention Technology of Sensitive Data based on AI	Risk analysis & data visualization display, based on classification techniques & application technology, reduces the risk of data	The system can record, alarm, block sensitive data but cannot secure sensitive data.

II. Data Loss Prevention (DLP) Methods

To ensure the security of user's sensitive data we design a framework to detect the Sensitive data of the user using machine learning techniques that may help the organization to identify the private or confidential information of its customer's and protects sharing of this information with intruders.

A. Data Collection

Big Data (Ram Mohan Rao et al., 2018) is obtained from various sources like Free Sources Such as Cloud storage, internet, drives & social media, etc. & Data access via APIs such as online media. Data storages providing HTTP-based access to the data by APIs (e.g., Twitter, Facebook, and wikis). Social media data types include data from interpersonal organization media, Websites, wikis, RSS channels, Blogs, Newsgroups & chat services. This data collection includes progressively significant continuous real-time information of monetary information, client Exchange information, telecoms & Spatial data information. (Hart et al 2011)

B. Data Defining

Big Data obtained from various sources like cloud storages, the internet, drives & social media, etc. are Generally of two types: Structured & Un-Structured data. The four most common formats used to Markup texts are: HTML, XML, JSON and CSV. (Neerbek et al, 2020)

C. Data Reduction

A technique for reducing the size of data and providing meaningful data from the Collection of unstructured datasets. It increases efficiency and reduces the time to get an exact result, also increase the storage capacity to minimize the cost. The reduced data is more useful and relevant than the in-consistent, noisy, redundant, and raw - data. It involves text cleansing which includes Dealing with missing, incorrect, inconsistent, or semantic data and tagging of unstructured data (Winter et al., 2013).

D. Data Storage

Data obtained after reduction has to be stored possibly so that it can be used further. Hence, data storage comprises data storing in flat- file systems, R-DBMS, No-SQL & SQL Databases (Ravi Prasad, 2017).

E. Data Classification for Sensitive data identification

F. The Classification technique of ML is the method of predicting concepts like Sensitive Data from a large amount of big data available in the form of structured or unstructured format. It is used for determining to predict or to learn a model that is used for the detection of sensitive data. Some of the existing classification methods are KNN, SVM, Naïve Bayes classifier, CNN, DNN, etc. (Vasu & Pari, 2019).

G. Data Analytics

Complex- analysis for data analytics of online data for sentiment analysis or opinion mining based on unknown dialects, unfamiliar words, slang, spelling mistakes, and the NLP. Hence, the sensitive

Data is analyzed using a predictive classifying model (Sampaio & Garcia, 2016).

H. Data Protection

Sensitive data identified through a predictive model of classification needs to be protected. Hence, sensitive data identified has to be encrypted, so that it can be protected from Intruders and also notifying the administrator and blocking user request. So, that no Confidential information goes outside the organization without the user's permission (Hassan et al., 2020).

III. Conclusion & Future Scope of Work

Recently, WhatsApp & other social networking apps such as Facebook has updated their privacy policy, and according to it, they are sharing the private & confidential customer's sensitive data with marketing & business companies to earn profit & growth. In this case, these companies utilize customer's sensitive data for their profit or gain. Similarly, any hacker or intruder can also use the user's sensitive data to gain personal benefits or to cause harm to the user.

As we all know sensitive data is very important for the user. Hence, it is important to secure the sensitive data of the user. For this purpose, we designed a framework that detects and predicts the sensitive data of the customer, and based on

the detection it blocks, notifies, and encrypts the user request hence doesn't allow sensitive data to go out of the designed framework. It makes the identification of sensitive data easier and hence easy to secure the sensitive data of the user. This framework will help the organizations who don't want to leak the confidential information of their user's such as, hospitals, banks, government Organizations, military, defense etc., or the individuals who want to detect and prevent their sensitive data and avoid data leakage.

IV. REFERENCES

[1] Adhikari, B. K., Zuo, W., Maharjan, R., Han, X., & Liang, S. (2020). Detection of sensitive data to counter global terrorism. Applied Sciences (Switzerland), 10(1). https://doi.org/10.3390/app10010182

[2] Alzahrani, A., Alqazzaz, A., Almashfi, N., Fu, H., & Zhu, Y. (2017). Web Application Security Tools Analysis. Studies in Media and Communication, 5(2), 118. https://doi.org/10.11114/smc.v5i2.2663

[3] Awang, N. F., & Manaf, A. A. (2013). Detecting Vulnerabilities in Web Applications Using Automated Black Box and Manual Penetration Testing. Communications in Computer and Information Science, 381 CCIS, 230–239. https://doi.org/10.1007/978-3-642-40597-6_20

[4] Bozic, J., & Wotawa, F. (2020). Planning-based security testing of web applications with attack grammars. Software Quality Journal, 28(1), 307–334. https://doi.org/10.1007/s11219-019-09469-y

[5] Chen, D. J. I. Z., & S., D. S. (2020). Social Multimedia Security and Suspicious Activity Detection in SDN using Hybrid Deep Learning Technique. Journal of Information Technology and Digital World, 2(2), 108–115. https://doi.org/10.36548/jitdw.2020.2.004

[6] García-Pablos, A., Perez, N., & Cuadros, M. (2020). Sensitive data detection and classification in Spanish clinical text: Experiments with BERT. LREC 2020 - 12th International Conference on Language Resources and Evaluation, Conference Proceedings, 4486–4494.

[7] Ghouse, M., & Nene, M. J. (2020). Graph neural networks for prevention of leakage of secret data. Proceedings of the 5th International Conference on Communication and Electronics Systems, ICCES 2020, ICCs, 994–999. https://doi.org/10.1109/ICCES48766.2020.09137957

[8] H. R, S. R., B. S, P. A., & Kumar. P, D. R. (2019). Smart Document Analysis Using AI-ML. International Journal of Innovative Research in Computer Science & Technology, 7(3), 54– 70. https://doi.org/10.21276/ijircst.2019.7.3.6

[9] Hart, M., Manadhata, P., & Johnson, R. (2011). Text classification for data loss prevention. HP Laboratories Technical Report, 114, 1–21.

[10] Hassan, M., Jincai, C., Iftekhar, A., Shehzad, A., & Cui, X. (n.d.). Implementation of Security Systems for Detection and Prevention of Data Loss / Leakage at Organization via Traffic Inspection.

[11] Hou, X. Y., Zhao, X. L., Wu, M. J., Ma, R., & Chen, Y. P. (2018). A Dynamic Detection Technique for XSS Vulnerabilities. Proceedings - 2018 4th Annual International Conference on Network and Information Systems for Computers, ICNISC 2018, 34–43. https://doi.org/10.1109/ICNISC.2018.00016

[12] Karamani, B. (2018). Improving data loss prevention using classification. Lecture Notes on Data Engineering and Communications Technologies, 17,183–189. https://doi.org/10.1007/978-3-319-75928-9_16

[13] Kowsari, K., Heidarysafa, M., Brown, D. E., Meimandi, K. J., & Barnes, L. E. (2018). RMDL: Random multimodel deep learning for classification. ACM International Conference Proceeding Series, 19–28. https://doi.org/10.1145/3206098.3206111

[14] Kumar, S., Mahajan, R., Kumar, N., & Khatri, S. K. (2018). A study on web-application security and detecting security vulnerabilities. 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICR ITO 2017, 2018-Janua, 451–455. https://doi.org/10.1109/ICRITO.2017.8342469

[15] Liu, D., Liu, X., Ma, L., Chang, Y., Wang, R., Zhang, H., Yu, H., & Wang, W. (2020). Research on Leakage Prevention Technology of Sensitive Data based on Artificial Intelligence. ICE IEC 2020 - Proceedings of 2020 IEEE 10th International Conference on Electronic Information and Emergency Communication, 142–145.https://doi.org/10.1109/ICEIEC49280.2020.9152286

[16] Mary, D. S. N., & Begum, A. T. (2017). An algorithm for moderating DoS attacks in web-based applications. Proceedings - 2017 International Conference on Technical Advancements in Computers and Communication, ICTACC 2017, 2017-October, 26–31. https://doi.org/10.1109/ICTACC.2017.17

[17] Neerbek, J. (2020). Sensitive information detection: Recursive neural networks for encoding context. ArXiv.

[18] Obaida, M. A., Nelson, E., Ee, R. V., Jahan, I., & Sajal, S. Z. (2017). Interactive sensitive data exposure detection through static analysis. IEEE International Conference on Electro Information Technology, May 2017, 270–275. https://doi.org/10.1109/EIT.2017.8053368

[19] Oliveira, R. A., Raga, M. M., Laranjeiro, N., & Vieira, M. (2020). An approach for benchmarking the security of web service frameworks. Future Generation Computer Systems, 110,833–848. https://doi.org/10.1016/j.future.2019.10 detection. Journal of Systems and Software,113,337–361.