{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 169
-
Number 10

Year of Publication: 2017

Authors:

Jay Kant Pratap Singh Yadav, Devottam Gaurav

10.5120/ijca2017914904

{bibtex}2017914904.bib{/bibtex}

Abstract

In this paper, we propose data mining approach for database intrusion detection. In each database, there are a few attributes or columns or columns that are more important or sensitive to be tracked or sensed for malicious modifications as compared to the other attributes. Our approach concentrates on mining pre-write as well as post-write data dependencies among the important or sensitive data items in relational database. These dependencies are generated in the form of association rules. Any transaction that does not follow these dependency rules are identified as malicious. We also suggest removal of redundant rules in our proposed algorithm to minimize the number of comparisons during detection phase.

References

1. J. Han, M. Kamber. “Data Mining: Concept and Techniques”, 2001, Morgan Kaufmann Publishers.
2. D. Neelapala. “Use of FP growth Algorithm for Database Intrusion Detection”, UMI

dissertation Publishing, 2008, pp. 230-260.

3. W. L. Low, S. Y. Lee, P. Teoh. “DIDAFIT: Detecting Intrusions in Databases Through Fingerprinting Transactions”, In: proceedings of the 4th International Conference on Enterprise Information Systems (ICEIS), 2002, pp. 264-269.

4. U. Fayyad, G.P. Shapiro, P. Smyth. “The KDD Process for Extracting Useful Knowledge from Volumes of Data”, In proceedings of the Communications of the ACM, 1996, pp. 27-34.

5. A.Srivastava, S. Sural, A.K. Majumdar. “Weighted Intra-transactional Rule Mining for Database Intrusion Detection,” Lecture Notes in Artificial Intelligence, Springer Verlag, In proceedings of Pacific-Asia Conference in Knowledge Discovery and Data Mining, 2006, pp. 611-620.

6. Y. Hu, B. Panda. “A Data Mining Approach for Database Intrusion Detection”, In proceedings of the ACM Symposium on Applied Computing, 2004, pp. 711-716.

7. A. Rezk, H. Ali, M. El-Mikkawy, S. Barakat. “Minimize the False Positive Rate in a Database Intrusion Detection System”, International Journal of Computer Science & Information Technology (IJCSIT), 2011, Vol. 3, No 5, pp. 29-38.

8. R. Agrawal, R. Srikant. “Fast algorithms for mining association rules”, In: Proceedings of the 20th International Conference on Very Large Databases, 1994, ACM SIGMOD, pp. 487–499.

9. W. Wang, J. Yang, P. S. Yu. “Efficient Mining of Weighted Association Rules”, In proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2000, pp. 270-274.

10. F. Tao, F. Murtagh, M. Farid. “Weighted Association Rule Mining using Weighted Support and Significance Framework”, 2003, In proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining, pp. 661-666.

11. E. Lundin, E. Jonsson. “Survey of Intrusion Detection Research”, Technical Report, 2002, Chalmers University of Technology.

12. W. Lee, S.J. Stolfo. “Data Mining Approaches for Intrusion Detection”, In proceedings of the USENIX Security Symposium, 1998, pp. 79-94.

13. D. Barbara, J. Couto, S. Jajodia, N. Wu. “ADAM: A Testbed for Exploring the Use of Data Mining in Intrusion Detection”, ACM SIGMOD, 2001, pp. 15-24.

14. C.Y. Chung, M. Gertz, K. Levitt. “DEMIDS: A Misuse Detection System for Database Systems”, In proceedings of the IFIP TC-11 WG 11.5 Working Conference on Integrity and Internal Control in Information System,1999, pp. 159-178.

15. V.C.S. Lee, J.A. Stankovic, S.H. Son. “Intrusion Detection in Real-time Database Systems via Time Signatures”, 2000, In proceedings of the Real Time Technology and Application Symposium, pp. 124.

16. S.Y. Lee, W.L. Low, P.Y. Wong. “Learning Fingerprints for a Database Intrusion Detection System”, 2002, In proceedings of the European Symposium on Research in Computer Security, pp. 264-280.

17. D. Barbara, R.Goel, S. Jajodia. “Mining Malicious Data Corruption with Hidden Markov Models”, 2002, In proceedings of the IFIP WG 11.3 Working Conference on Data and Application Security, pp. 175-189.

18. Y. Zhong, X. Qin. “Research on Algorithm of User Query Frequent Item sets Mining”, 2004, Machine Learning Cybernetics, pp. 1671-1676.

19. A. Srivastava, A. Bhosale, S. Sural. “Speeding up Web Access Using Weighted Association Rules”, Lecture Notes in Computer Science, Springer Verlag, 2005, In proceedings

of International Conference on Pattern Recognition and Machine Intelligence (PReMI'05), 660-665.

20. A. Kundu, S. Sural, A.K. Majumdar. “Database Intrusion Detection using sequence alignment”, 2010, In proceedings of international journal of information security, pp. 179-191.

21. E. Bertino, E. Terzi, A. Kamra, A. Vakali.“Intrusion Detection in RBAC-Administered Databases”, 2005, In: Proceedings of the 21st annual computer security applications conference (ACSAC), pp. 170–182.

22. R. Agrawal, R. Srikant. “Mining Sequential pattern”, In proceedings of the 1995 International Conference on Data Engineering, 1995, Taipei, Taiwan , pp. 203-205.

23. S.Wenhui, T. Tan. “A Novel Intrusion Detection System Model for Securing Web-Based Database Systems”, 2001, In proceedings of the 25th annual international computer software and applications conference (COMPSAC), pp. 249–254.

24. K. Takeda. “The Application of Bioinformatics to Network Intrusion Detection”, 2005, In proceedings of the international carnahan conference on security technology (CCST), pp. 130–132.

25. S. Coull, J. Branch, B. Szymanski, E. Breimer. “Intrusion Detection: A Bioinformatics Approach”, 2003, In: proceedings of the annual computer security applications conference (ACSAC), pp. 24–33.

26. E. Mohammadreza, S. Merar, S. Fatimah, A. Lilly Suraini. “Intrusion detection using Data Mining Techniques”, 2010, In: proceedings of Information retrieval and knowledge management (CAMP), IEEE, pp. 200-203.

27. Yi Hu, C. Campan, J. Walden, I. Vorobyeva, J. Shelton. “An effective log mining approach for database intrusion detection”, 2010, In proceeding of International Conference on Systems Man and Cybernetics (SMC), IEEE , pp. 2299 – 2306.

28. M. Ektefa, S. Memar, F. Sidi, Affendey L. S.. “Intrusion Detection Using Data Mining Techniques”, 2010, In Proceedings of the International Conference on Information Retrieval & Knowledge Management, (CAMP), IEEE, pp.200-203.

29. U.P. Rao, G.J. Sahani, D.R. Patel. “Detection of Malicious Activity in Role Based Access Control (RBAC) Enabled Databases”, 2010, In Proceeding of Journal of Information Assurance and Security 5, pp. 611-617.

30. R. Brace, P. Mell. “Intrusion detection system”, 2001, NIST special publication on Intrusion Detection System.

31. R. Sandhu, D. Ferraiolo, R. Kuhan. “The NIST Model for Role Based Access Control: Towards Unified Standard”, 2000, In Proceedings of the 5th ACM workshop of Role Based Access Control.

32. S.Hashmi, Y. Yang, D. Zabihzadeh, M. Rangavari. “Detecting Intrusion Transaction in Databases Using Data Dependencies and Analysis Expert Systems”, 2008, Vol. 25, pp.460-473S.

Index Terms

Computer Science Security

Keywords

Data Mining, Intrusion Detection System, Data Dependency, Sensitive Attributes.