

{tag}

{/tag}

Technology for Inter-Sectoral Research  
© 2019 by IJCA Journal

IJCA Proceedings on Leveraging Information

ICAIM 2017 - Number 2

Year of Publication: 2019

Authors:

Priyanka Nikalje

Gauresh Lotlikar

Manish Mishra

Shirshendu Maitra

{bibtex}icaim201721.bib{/bibtex}

## Abstract

In today's IT world computer systems are vulnerable by both insiders (i. e. employees) as well as penetration by outsiders (or attackers). Also there are evidences showing the

growing number of incidents reported in the press for such abuse. Closing all security loopholes from today's system is infeasible, whereas no combination of technologies can prevent legitimate users from abusing their authority in a system, auditing is viewed as the last line of defense. But auditing a large amount of data is not a feasible option hence what is needed is automated tools to analyze the vast amount of audit data for suspicious user behavior. This paper presents audit trail analysis technique and intrusion detection systems that have emerged in the past several years.

## References

### ences

- <http://www.academypublisher.com/proc/isnns10/paper/isnns10p275.pdf>
- <http://www.lexjansen.com/pnwsug/2004/ExtractingDatafromOracleintoSAS-LessonsLearned.pdf>
- [https://support.sas.com/training/tutorial/el/libspg3\\_at.pdf](https://support.sas.com/training/tutorial/el/libspg3_at.pdf)
- <http://www.atis.org/glossary/definition.aspx?id=5572>
- <http://www.datamation.com/columns/article.php/3578916/The-Importance-of-Audit-Logs.htm>
- <http://csrc.nist.gov/>

## Index Terms

Computer Science

Information Science

## Keywords

System Log Audit Trail