



Institutional Sign In

All



ADVANCED SEARCH

Conferences > 2023 International Conference...

Cybersecurity Threat Detection in Financial Institution Using AI BasedRisk Assessment

Publisher: IEEE

[Cite This](#)

PDF

Lavanya M ; Mangayarkarasi S [All Authors](#)



94
Full
Text Views

Alerts

[Manage Content Alerts](#)
[Add to Citation Alerts](#)

Abstract



Downl
PDF

Document Sections

- I. Introduction
- II. Related works
- III. PROPOSED METHOD
- IV. RESULTS AND DISCUSSIONS
- V. Conclusions

Abstract:

In recent times, the research looks into the measures taken by financial institutions to secure their systems and reduce the likelihood of attacks. The study results indi... [View more](#)

Metadata

Abstract:

In recent times, the research looks into the measures taken by financial institutions to secure their systems and reduce the likelihood of attacks. The study results indicate that all cultures are undergoing a digital transformation at the present time. The dawn of the Internet ushered in an era of increased sophistication in many fields. There has been a gradual but steady shift in attitude toward digital and networked computers in the business world over the past few years. Financial organizations are increasingly vulnerable to external cyberattacks due to the ease of usage and positive effects. They are also susceptible to attacks from within their own organisation. In this paper, we develop a machine learning based quantitative risk assessment model that effectively assess and minimises this risk. Quantitative risk calculation is used since it is the best way for calculating network risk. According to the study, a network's vulnerability is proportional to the number of times its threats have been exploited and the amount of damage they have caused. The simulation is used to test the model's efficacy, and the results show that the model detects threats more effectively than the other methods.

Published in: 2023 International Conference on Emerging Research in Computational Science (ICERCS)

Date of Conference: 07-09 December 2023

DOI: 10.1109/ICERCS57948.2023.10434030

[Authors](#)

[Figures](#)

[References](#)

[Keywords](#)

[Metrics](#)

[More Like This](#)



Date Added to IEEE Xplore: 21 February 2024

Publisher: IEEE

► ISBN Information:

Conference Location: Coimbatore, India

☰ Contents

I. Introduction

The goal of cyber security is to stop someone from entering in, whether they are insiders or outsiders, and using your network, system without the knowledge or permission of the user. It is crucial to protect one privacy and security when dealing with sensitive information online. A company susceptibility to cyberattacks increases when it lacks the resources to provide its employees with the knowledge, skills, and best practises necessary to safeguard its information technology infrastructure against penetration by malware, ransomware, and other factors. Cybersecurity risk in the financial sector has shifted the paradigm of banking operations over the course of several decades due to the prospect of severe interruption to banking services and the imposition of considerable direct and indirect losses. This is a direct outcome of the substantial disruption that could occur to banking services. Financial institutions are increasingly at risk of cyberattacks because of the growing prevalence of online commerce and service provision [1].

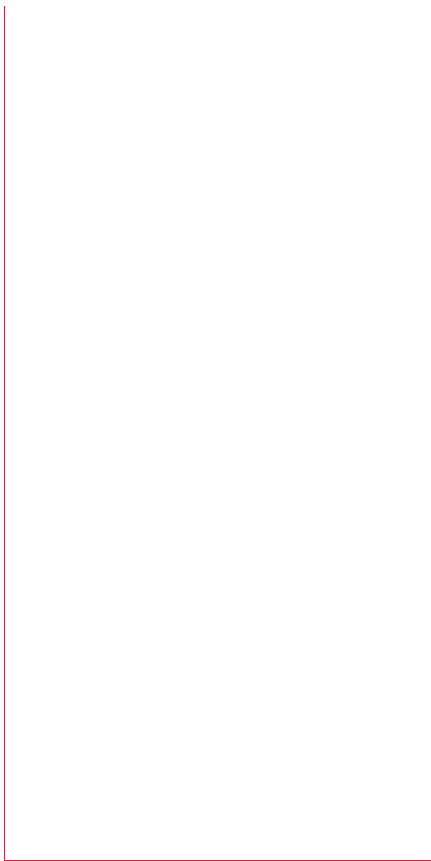
Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

More Like This

Decision Tree: Review of Techniques for Missing Values at Training, Testing and Compatibility
 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)
 Published: 2015

Overcoming Distribution Shifts in Plug-and-Play Methods with Test- Time Training
 2023 IEEE 9th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)
 Published: 2023

Show More



IEEE Personal Account

CHANGE
USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
VIEW PURCHASED
DOCUMENTS

Profile Information

COMMUNICATIONS
PREFERENCES
PROFESSION AND
EDUCATION
TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800
678 4333
WORLDWIDE: +1 732
981 0060
CONTACT & SUPPORT

Follow



About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

- » Communications Preferences
- » Profession and Education

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.