The role of Digital Forensics Incident Response for mitigating insider attacks in the healthcare system

Dr.Mervin Retnadhas Mary[1,2,] [a], *Dr.Pawan Whig*[3,] [b]

[1]Postdoctoral Researcher, Lincoln University College, Petaling Jaya-47301, Selangor, Malaysia.
[2]Assistant Professor, Department of Information Technology, Saudi Electronic University, Saudi Arabia.
[3]Dean Research, Vivekananda Institute of Professional Studies-TC, New Delhi
mervinvijay@gmail.com , pawan.whig@vips.edu

Abstract: The healthcare sector is gradually becoming the most important prime target for cybercriminals due to the nature of data used in the healthcare sector, including patient data, medical records, usernames, passwords, and so on. This reality underscores the need to protect these data from insider attacks and highlights the importance of digital forensics in the health care sector. This research paper explores digital forensic investigation and responses to mitigate insider attacks, supported by the Digital Forensic Incident Response (DFIR) framework. This framework supports identifying the incident across its phases, including Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. The CERT datasets have been taken for the analysis, and they have been pre-processed before applying the algorithm. The different machine learning algorithms are incorporated to gain better results, and it produces 97.7% accuracy with AdaBoost. The research concludes that the insider attack can be eliminated in the health care system using the DFIR investigation process.

Keywords: Cybersecurity, Health Care, Digital Forensics Incident Response, Cyberattacks, Insider Attacks, Health Recommendation Systems, Health Care System, Countermeasures, and Mitigation.

Introduction

Digital crime is becoming a more common issue across all fields of digitalization. Forensic computing is a well-structured field that aims to reduce cybercrime worldwide. There is a good chance that digital evidence will be found in almost every crime. It is possible to extract information from different data sources using digital forensic analysis, which can be used to provide evidence of criminality, exonerate suspects, or aid a larger investigation [4]. Insider threats remain one of the most persistent and damaging challenges in modern cloud-based environments. Organizations rely on cloud services to store sensitive information, deliver business applications, and support distributed workforces, which increases the volume and complexity of digital activity that must be monitored for security and forensic purposes. There is many software tools are used to do the investigation on the digital crime. FTK (Forensics Tool Kit) and EnCase are the most important tools that analyze the feature similarity.[5].

---

a https://orcid.org/0000-0002-8587-0624
b https://orcid.org/0000-0003-1863-1591

In forensics, tools such as FTK Imager are used to create images of data. This is done because it can pull data, which can be converted into important information, so the data can be used as forensic evidence.[8]

Every organisation must investigate security breaches and evaluate cyber incidents to take preventive measures against future attacks. The healthcare IT experts must know the concepts to effectively respond to incidents and protect patient information. The following process must be followed by these experts to protect the data and to navigate the complexities of digital crime.

- Data Recovery: It focuses on restoring the lost data or deleted files of the patient.
- Evidence Preservation: It is an important process to collect the digital evidence and preserve it for any legal proceedings.
- Incident Response: A well-structured approach to handle a cyber attack that supports minimising the damage, also restoring normal operation as quickly as possible, particularly through digital forensics investigation and response.

Related work

Wasyihun et al. [1] wrote the state of the art, challenges, and future directions of cybersecurity. He also mentioned the integration of Artificial Intelligence and Machine Learning techniques that help to mitigate vulnerabilities in the cyber security filed. The paper focused on the various applications of cyber security, including cyber security in smart cities, smart grid, vehicle communication, and eHealth systems. It also discussed many cybersecurity attacks, particularly zero-day attacks. Zero-day attacks have been analysed and divided into five stages zero day attacks, pseudo zero day attacks, potential for zero-day attacks, potential for pseudo-zero-day attacks, and passive. They found a solution with IoT(Internet of Things), AI, ML, and cloud computing techniques to mitigate the cybersecurity vulnerabilities.

Cornelius Itodo et al. [2] described the Digital Forensics and Incident Response (DFIR) Challenges in (Internet of Things) IoT Platforms. The IoT platform collects an enormous amount of data generated by IoT devices. The data will be shared through the network, and due to the huge collection of data, congestion may occur. During the traffic, the attacker will try to modify the data. The digital forensics response plan should be developed to narrow targeted network traffic. Dr. Suneel Pappala et al. [3] discussed the vulnerabilities in the various domains, techniques to resolve those vulnerabilities, and evaluated the risk assessment.

Aditya Choudhary [9] briefed about a comparative analysis of digital forensics tools based on performance parameters. The forensic tools EnCase, FTK, Autopsy, and X-Ways has been analyzed by the performance parameters acquisition/processing speed, accuracy/recovery, usability, platform and file-system support, resource usage, reporting, and cost. He discussed different forensic tools and made a comparative analysis to gain a better understanding of these tools.

Key Contribution

Digital Forensics and Incident Response (DFIR) are like two puzzle pieces that fit together perfectly when it comes to managing cybersecurity threats. While each serves a different purpose, when combined, they make [6]. Digital forensics is all about figuring out the details of the attack—who did it, how they got in, and what they did. Incident response focuses on stopping the attack, fixing the problem, and getting everything back to normal. The integration of information technology into healthcare has revolutionized how medical services are delivered, recorded, and managed [7]. The main steps of the DFIR Process are [9]

1. Preparation: Building policies and tools for handling incidents
2. Identification: Detecting anomalies indicating a security incident.
3. Containment: Limiting the scope of the breach to prevent further damage.
4. Eradication: Removing the root cause and malicious artifacts.
5. Recovery: Restoring systems to normal operations.
6. Lessons Learned: Post-incident review to strengthen future attacks.

Method, Experiments and Results

The CERT has been taken for analysis, including the logon activity of the user. The dataset was preprocessed, and the pattern was analyzed in the logon dataset to check for the vulnerability of insider attacks. The following figures 1a and 1b depict the logon/ log off activity of the users. It helps to analyze the pattern of the user logon/ log off activity. If there is a pattern change, then it can be considered as a vulnerability, and immediately the DFIR process will be executed to fix the issue.

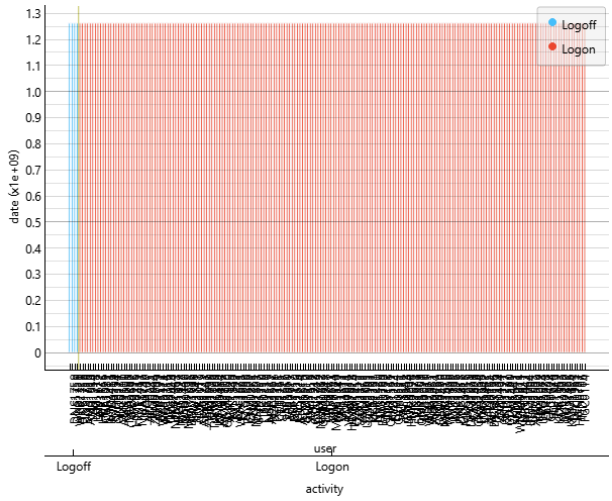

Figure 1a. The user logon/logoff activity

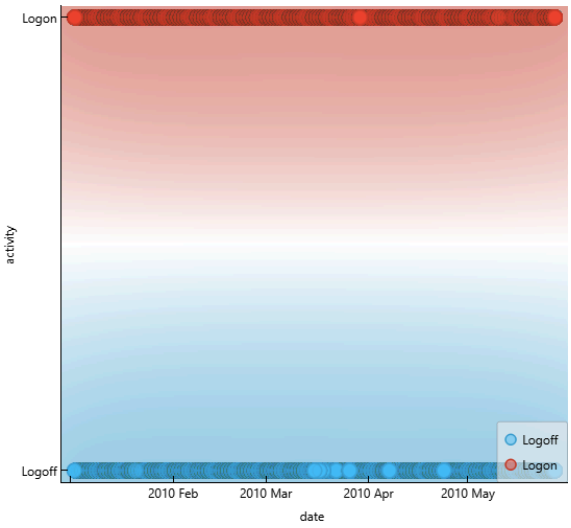

Figure 1b. The user logon/logoff activity based on date

Discussions

The machine learning algorithms Support Vector Machine, KNN, Adaboost, Random Forest, and Navie bayes method are executed to check the best suitable algorithm to understand the concepts. Among the different algorithms, Adaboost produced 97.7% accuracy, and random forest gave 97.5% accuracy. Figure 2 shows up the performance curve and ROC analysis of these algorithms, also it helps to reduce the False Positive in a good way.

Table 1. Evaluation results for the target

Model	AUC	CA	F1	Prec	Recall	MCC
AdaBoost	0.996	0.977	0.977	0.979	0.977	0.971
kNN	0.992	0.973	0.973	0.973	0.973	0.967
Naive Bayes	0.999	0.927	0.951	0.979	0.927	0.912
Random Forest	0.998	0.975	0.975	0.976	0.975	0.969
SVM	0.997	0.963	0.960	0.961	0.963	0.954

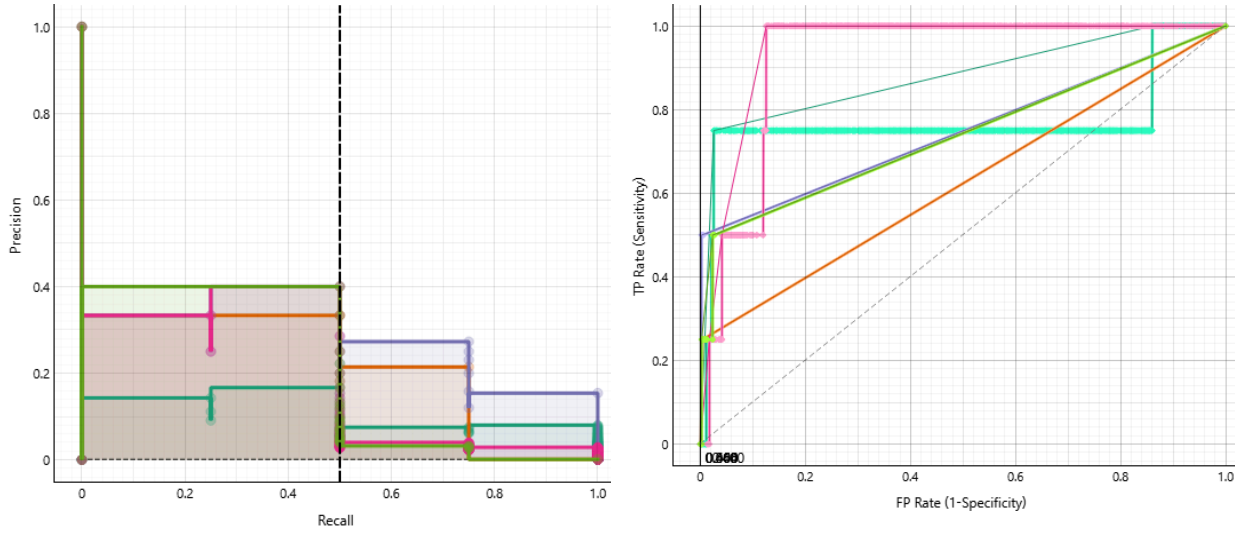

Figure 2. Performance curve and ROC analysis

Conclusions

Mastering digital forensics investigation and response in healthcare is essential for protecting sensitive patient information and ensuring compliance with stringent regulations. This article underscores the importance of grasping digital forensics concepts, addressing healthcare-specific challenges, and implementing effective tools and techniques. By adopting a structured approach to forensic investigations, healthcare organizations can enhance their defenses against cyber threats and improve their overall security posture. Based on the research, the tools and techniques have been identified in the fields of Digital Forensics and Machine Learning.DFIR guidelines have been implemented to reduce insider attacks. The datasets are tested with the Support Vector Machine, KNN, Adaboost, Random

Forest, and Navie bayes method. The results were analysed with the performance metrics. Adaboost is giving 97.7% accuracy. Furthermore, a deep investigation has to be implemented to remove all vulnerabilities in the healthcare system.

References

1. Wasyihun Sema Admass ,Yirga Yayeh Munaye ,Abebe Abeshu Diro, “Cyber Security: State of the art, Challenges and future Directions ”, Cyber Security and Applications, 2024, 10031,pp 1- 9. https://doi.org/10.1016/j.csa.2023.100031.
2. Cornelius Itodo, Said Varlioglu, Nelly Elsayed, "Digital Forensics and Incident Response (DFIR) Challenges in IoT Platforms", 2021 4th International Conference on Information and Computer Technologies (ICICT),978-1-6654-1399-2/21/$31.00 ©2021 IEEE, DOI 10.1109/ICICT52872.2021.00040, pp. 199-203.
3. Dr. Suneel Pappala, Dr. Kanigiri Suresh, "Advancements in Ethical Hacking Techniques and Tools: Strengthening Cybersecurity Resilience", International Journal for Multidisciplinary Research (IJFMR), E-ISSN: 2582-2160, Volume 7, Issue 2, March-April 2025, pp 1-12.
4. Narayan P. Bhosale , " Evidence Recovery using EnCase and FTK in Forensic Computing Investigation ", International Journal of Scientific Research in Computer Science and Engineering, Vol.9, Issue.4, pp.08-13, August 2021, *DOI: https://doi.org/10.26438/ijsrcse/v9i4.813, pp. 8-13.*
5. Abubakar Abdulkadir, Ahmad Ahmad, and Badamasi Jaafar, "The Evaluation of the Encase and FTK Forensic for effective evidence extraction," Global Scientific Journals: Volume 9, Issue 3, March 2021, Online: ISSN 2320-9186, pp. 1825 – 1834.
6. Sakshi Adarkar, "Navigating Cyber Threats: A Comprehensive Study of Digital Forensics and Incident Response", International Journal for Research Trends and Innovation, ISSN: 2456-3315 , 2024, pp. 184-176.
7. Shashi Tharoor, "Applying Digital Forensics Techniques to Secure and Investigate Threats in Healthcare Information Systems and Electronic Medical Records", International Journal of Scientific Research & Engineering Trends Volume 9, Issue 2, Mar-Apr-2023, ISSN (Online): 2395-566X, pp. 1-5.
8. Rachmat Suryadithia1, Witriana Endah Pangesti2, Muhammad Faisal3, Aji Nurrohman4, Wibisono5, Arman Syah Putra6 ,"FTK Image For Forensic Data Processing In Forensic Tools ", International Journal of Information System & Technology , Akreditasi No. 158/E/KPT/2021 | Vol. 5, No. 6, (2022), pp. 726-735.
9. Aditya Choudhary, "A Comparative Analysis of Digital Forensics Tools Based on Performance Parameters", International Research Journal of Engineering and Technology, Volume: 13 Issue: 01 | Jan 2026, pp. 113-117.