Article Review #1: Braktooth Attacks

Student Name: Aaron Fields

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

September 27, 2025

The Article by Kirbubavathi and Nair (2024) examines a growing threat to the healthcare industry: Braktooth attacks on IoT (Internet of Things) devices. Their study introduces a framework that uses multiple layers of machine learning to accurately detect attacks. Healthcare is increasingly dependent on connected devices to accurately monitor patients and provide the best care possible, which makes this a critical topic. This review will provide a summary to aid in understanding the research, data analysis, and broad implications that the healthcare industry faces in this digital age.

Cybersecurity is often seen as being a technical problem, but it is deeply connected to the social sciences, particularly ethics and sociology. As an example, patients are trusting that the personal information that they give will be protected and secure by the systems and IT infrastructure. This article highlights how vulnerabilities in IoT healthcare systems can affect patients and public confidence. There are also ethical considerations, as failure to secure patient information can also harm the elderly and those in rural areas, who already have limited access to healthcare. These are marginalized groups that need to be taken into consideration when discussing the impact of healthcare attacks and vulnerabilities.

The question that the authors raise is: *How can a stacking framework improve detection of Braktooth attacks in IoT healthcare systems?* The research methods used to study this included creating a virtual IoT environment containing common devices used in a hospital like health trackers, wearable monitors for patients, and other connected medical equipment. The stacking framework was tested in this simulated environment and as a result, they concluded that the machine learning method called stacking detection would help improve accuracy and overall detection compared to the existing methods that are available. The simulation allowed for precise control over various factors to test theories while avoiding the risks of testing in a live healthcare setting. The data gathered came from IoT network traffic in both normal and attack conditions. The important things to look at in this data are detection accuracy and false positive rate. The detection framework had a detection accuracy of 96% while reducing false positives by 15%. It essentially shows the effectiveness in the framework to detect attacks without causing false alarms.

This article relates to principles discussed in this class, particularly ransomware attacks. Hackers exploit the vulnerabilities in IoT devices and healthcare systems are a prime target because of the sensitive data that flows through and collects on these networks. Public policy implications also arise, as governments and healthcare organizations have the need to regulate and safeguard data while still ensuring that the proper parties have access.

The authors demonstrate the need for technological innovation to partner with social responsibility in order to support safer healthcare delivery through better cybersecurity practices. This research offers great insight from both technical and ethical standpoints, making it a great source to reference for future studies in healthcare cybersecurity.

References

Kirubavathi, G., & Nair, A. N. K. S. (2024). *Stacking framework for detecting Braktooth attack on IoT healthcare systems* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10581018