Chapter 2
Case-Based Reasoning and Computer Vision for Cybersecurity: A Short Review

Naomi Dassi Tchomte
University of Ngaoundere, Cameroon

Franklin Tchakounte
https://orcid.org/0000-0003-0723-2640
Faculty of Science, University of Ngaoundere, Cameroon

Ismael Abbo
Faculty of Sciences, University of Ngaoundere, Cameroon

ABSTRACT

The integration of case-based reasoning (CBR) and computer vision (CV) holds significant promise for enhancing cybersecurity, enabling the analysis and interpretation of visual data to detect security threats. This study provides an investigation of the synergy between case-based reasoning and computer vision techniques in the context of cybersecurity, aiming to address open challenges and identify opportunities for advancing security operations. Three main steps are realized. First, a taxonomy declining categories and sub-categories of the studied works is designed. Second, the collected literature is analysed in terms of (1) CBR for leveraging past security incidents and patterns in visual data analysis, facilitating threat detection, incident response, and threat intelligence analysis; (2) CV for cybersecurity modelling and to support cybersecurity decision making; (3) association between CBR and CV to design cybersecurity approaches. Third, open issues are discussed. This study exploiting CBR in computing vision for cybersecurity opens doors for further research.

DOI: 10.4018/978-1-6684-8127-1.ch002

1. INTRODUCTION

Cybersecurity is an ever-evolving field faced with the daunting challenge of defending against a myriad of sophisticated and constantly evolving cyber threats (Beghhith 2017). As organizations increasingly rely on digital technologies and data-driven processes, the need for robust and effective cybersecurity measures has never been more critical. Traditional approaches to cybersecurity often rely on signature-based detection systems and rule-based algorithms, which may struggle to keep pace with the rapidly evolving threat landscape (de Sousa, 2018). In recent years, there has been growing interest in exploring innovative approaches that leverage artificial intelligence (AI) and machine learning (ML) techniques to enhance cybersecurity capabilities. Among these approaches, the integration of case-based reasoning (CBR) and computer vision has emerged as a promising paradigm for analysing and interpreting visual data to detect and respond to security threats effectively.

Computer vision (CV), a subfield of AI, focuses on enabling computers to interpret and understand visual information from the world around them (Bachir, 2024). By leveraging advanced algorithms and techniques, computer vision systems can extract meaningful insights from diverse visual sources, including images, videos, network traffic visualizations, and log data. These insights are valuable for identifying anomalous behaviour, detecting suspicious activities, and investigating security incidents in real-time (D. Lopez-Sanchez, 2018) (Adedoyin et al., 2016). More specifically, visualizing binary files or network packets as images and applying convolutional neural networks (CNNs) can help detect malware signatures or anomalies (Yang et al. 2024); Anomaly detection algorithms based on computer vision can identify unusual behavior or suspicious activities in video feeds, alerting security personnel to potential threats (Zhao et al. 2021); Facial recognition and iris scanning, relying on computer vision algorithms provide robust authentication mechanisms difficult to spoof or replicate (Minaee et al. 2023); Analysing video streams in real-time, security personnel can quickly respond to incidents and mitigate potential risks (Wang et al. 2013); In forensics, computer vision techniques are employed in digital forensics to analyze visual evidence collected from crime scenes or digital devices based on image and video analysis tools (Kapoor et al. 2023).

On the other hand, case-based reasoning is a problem-solving methodology that relies on past experiences or cases to guide decision-making in new and similar situations (Nabila, 2013). By storing and retrieving relevant cases from a knowledge base, CBR systems can leverage historical data and patterns to inform security analyses, incident response, and threat intelligence operations. When combined with computer vision techniques, CBR systems can harness the power of visual data to enrich their knowledge base and improve decision-making capabilities (Wang et al. 2023). The association between CBR and CV can also increase reliability and