RADemics

Transformer-Based Threat Intelligence Frameworks Using BERT and GPT for Dark Web Analysis and Cybercrime Prediction

R Boopathi, Indumathi Venkatesan, Briskilal.J

KARPAGA VINAYAGA COLLEGE OF ENGINEERING AND TECHNOLOGY, RVS COLLEGE OF ARTS AND SCIENCE, SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Transformer-Based Threat Intelligence Frameworks Using BERT and GPT for Dark Web Analysis and Cybercrime Prediction

[1]R Boopathi, Assistant Professor, EEE, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu. rboopathiyadav@gmail.com

[2]Indumathi Venkatesan, Assistant Professor, School of Computer Studies- UG (BCA), RVS College of Arts and Science, Sulur. indhumathi@rvsgroup.com

[3]Briskilal.J, Assistant Professor, Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai. briskilj@srmist.edu.in

Abstract

The increasing sophistication of cyber threats originating from the Dark Web has necessitated the development of advanced threat intelligence frameworks capable of detecting and predicting malicious activities in real time. Traditional cybersecurity approaches often struggle to process the vast, unstructured, and linguistically diverse data generated on underground forums and illicit marketplaces. Transformer-based natural language processing (NLP) models, such as Bidirectional Encoder Representations from Transformers (BERT) and Generative Pre-trained Transformers (GPT), have demonstrated exceptional capabilities in understanding and generating contextualized textual representations, making them highly effective for Dark Web analysis and cybercrime prediction. This chapter explores the integration of transformer-based models in cyber threat intelligence workflows, emphasizing their ability to automate the identification of emerging threats, detect cybercriminal activities, and forecast evolving attack patterns. Key challenges, including data scarcity, adversarial linguistic variations, and ethical considerations in Dark Web monitoring, are analyzed alongside potential solutions leveraging AI-driven methodologies. , the chapter discusses the implications of transformer-based threat intelligence frameworks for real-time cybersecurity applications and future research directions aimed at enhancing cyber resilience. The insights presented contribute to the advancement of AI-driven cyber threat intelligence, enabling proactive threat mitigation strategies in an increasingly complex digital threat landscape.

Keywords: Transformer-Based Threat Intelligence, Dark Web Analysis, Cybercrime Prediction, BERT, GPT, AI-Driven Cybersecurity

Introduction

The rapid evolution of cyber threats, particularly those emerging from the Dark Web, has introduced unprecedented challenges in cybersecurity. The Dark Web serves as an unregulated ecosystem where threat actors engage in illicit activities such as data breaches, ransomware distribution, and the sale of exploit kits. Traditional cybersecurity frameworks, which often rely on rule-based detection and signature-based threat identification, struggle to keep pace with the dynamic nature of cyber threats originating from underground forums and marketplaces. the anonymity provided by encryption technologies such as The Onion Router (Tor) and Invisible

Internet Project (I2P) complicates law enforcement efforts, making proactive threat intelligence a necessity. Given the increasing sophistication of cybercriminal tactics, leveraging artificial intelligence (AI)-driven models capable of processing large-scale unstructured data has become an essential strategy for enhancing cyber resilience.

Transformer-based natural language processing (NLP) models, particularly Bidirectional Encoder Representations from Transformers (BERT) and Generative Pre-trained Transformers (GPT), have revolutionized the field of automated text analysis. These models possess the capability to understand contextual relationships, extract actionable intelligence from noisy and adversarial data, and generate coherent textual representations. Unlike conventional machine learning approaches, transformer-based architectures utilize self-attention mechanisms to process large volumes of cyber threat intelligence (CTI) data, enabling deeper insights into cybercriminal discussions and emerging attack vectors. Their ability to adapt to domain-specific linguistic variations makes them particularly effective for monitoring Dark Web communications, where threat actors frequently employ obfuscation techniques to evade detection. By integrating transformers into cybersecurity workflows, organizations can enhance their ability to detect, predict, and mitigate cyber threats in real-time.

Transformer-based models in threat intelligence, several challenges hinder their widespread adoption in Dark Web analysis. One of the primary concerns is data scarcity, as acquiring high-quality labeled datasets for training NLP models remains difficult due to ethical, legal, and technical constraints. Cybercriminal communications often contain adversarial language, encoded terminology, and multilingual content, further complicating automated threat analysis. Moreover, the lack of standardized benchmarking datasets and evaluation metrics makes it difficult to assess the performance of transformer models in real-world cyber threat scenarios. Addressing these challenges requires the development of robust data collection, annotation, and augmentation methodologies, as well as collaboration between academia, industry, and government agencies to facilitate responsible data-sharing practices.