SecureFed: A Decentralized Trust Framework for Privacy-Preserving Collaborative Cyber Threat Detection

Mohd Rijvan Ahmad
Graphic Era University, Uttarakhand, India

Dr. Poonam Verma
Graphic Era University, Uttarakhand, India

Dr. Vikas Tripathi
Graphic Era University, Uttarakhand, India

Abstract

Cyber attacks are increasing at an alarming rate and this requires greater cooperation among the firms in detecting and managing security threats. Sharing information about cybersecurity in different firms usually poses serious issues in terms of privacy, confidentiality, and compliance with laws. Traditional centralized cyber analytics rely on collecting sensitive information of the security logs into one repository.

This paper presents SecureFed, A Blockchain-enabled federated learning framework for collaborative cyber threat detection, which allows a number of organizations to collaborate and learn cyber threat models by utilizing their private data without exposing their raw datasets to each other. This framework uses Federated Learning where the collaborating organizations can learn their models using their cybersecurity datasets where only the model parameters are shared in order to construct a global model. In order to provide trust, transparency, and integrity in the collaboration process, blockchain technology has been utilized.

This framework facilitates cybersecurity analysis at a scale in which a vast amount of security logs, network traffic information, and threat intelligence are produced all the time. SecureFed is able to improve the privacy preservation process, facilitate collaborative threat intelligence, and minimize the use of central infrastructure through the integration of decentralized learning with blockchain-based validation techniques. Experimental evaluation based on standard cybersecurity datasets confirms that the proposed solution is efficient in providing accurate threat detection results.

The suggested model provides a workable approach for enterprises that want to enhance their cyber-defense abilities through collaboration and is hence very applicable to domains like healthcare, finance, education, and government.