Ensemble-Driven Malware Detection with Anomaly Override Capabilities

Viren Passi*, Sudhakar Kumar*, Sunil K. Singh*, Shivam Jindal*, Prince Raj**, Varsha Arya***,
Kwok Tai Chui***, Brij B. Gupta****

**Department of CSE,* Chandigarh *College of Engineering and Technology, Chandigarh, India*

*** Department of CSE, Galgotias University Greater Noida, Uttar Pradesh, India*

**** Hong Kong Metropolitan University, Hong Kong SAR, China*

***** Dept. of CSIE, Asia University, Taichung, Taiwan*

co23369@ccet.ac.in, sudhakar@ccet.ac.in, sksingh@ccet.ac.in, co23360@ccet.ac.in, princeraj15042005@gmail.com, varya@hkmu.edu.hk, jktchui@hkmu.edu.hk, bbgupta@asia.edu.tw

***Abstract*—This paper proposes a hybrid malware detection framework that combines ensemble learning with an anomaly based override mechanism. The ensemble component integrates Random Forest and XGBoost classifiers, while the override mechanism uses Isolation Forest to detect anomalous or uncertain samples. Each model was individually trained and evaluated on a labeled malware dataset, with Random Forest and XGBoost achieving 78.54% and 72.91% accuracy, respectively. Feature selection was performed using mutual information and ANOVA F-score to enhance model performance. In the proposed two-stage decision process, classification outputs from RF and XGBoost are fused through probabilistic averaging, and Isolation Forest acts as an override to flag potential malware. This hybrid strategy effectively reduces false negatives and enhances detection accuracy. The complete framework achieved 91.49% test accuracy and a weighted F1-score of 0.91, demonstrating its strength in detecting diverse malware types with improved reliability and adaptability.**

***Keyword*—Malware Detection, Ensemble Learning, Anomaly Override, Hybrid Classification, Feature Selection, Anomaly Detect**

Mr. Viren Passi was born in Ambala, Haryana, on November 27, 2004. He is currently pursuing the Bachelor of Engineering degree in computer science and engineering from the Chandigarh College of Engineering and Technology, Panjab University, Chandigarh, India. His major field of study includes natural language processing, artificial intelligence, and quantum computing. He is currently an Open Source Contributor with the Oppia Foundation. His work focuses on developing accessible educational software and researching quantum-classical hybrid models for audio classification tasks. Mr. Passi is actively interested in large-scale open-source development and the intersection of quantum mechanics with machine learning.

Dr. Sudhakar Kumar is a Senior Member of the Association for Computing Machinery (ACM) and the IEEE Computer Society. He is presently serving as an Assistant Professor in the Department of Computer Science and Engineering at Chandigarh College of Engineering and Technology, Sector 26, Chandigarh, functioning under the Chandigarh Union Territory Administration. He obtained his Doctor of Philosophy (Ph.D.) in the field of high-performance computing (HPC) with a focus on algorithmic design and compiler optimization from Panjab University, Chandigarh, India. He completed his Master of Technology (M.Tech.) at the Indian Institute of Technology (IIT) Guwahati, India. His scholarly interests encompass HPC, compiler optimization, machine learning (ML), artificial intelligence (AI), and human-computer interaction (HCI). Dr. Kumar has an extensive record of academic contributions, comprising more than one hundred twenty research publications in reputed international and national journals, conferences, and book chapters. In addition, he holds four design patents.

Prof. Sunil K. Singh is Professor and Head of the Computer Science & Engineering Department at Chandigarh College of Engineering and Technology (Degree Wing), a premier Chandigarh (UT) Government institute affiliated with Panjab University, Chandigarh, India. He holds B.E., M.E., and Ph.D. degrees in Computer Science and Engineering and has over 240 publications, 7 granted patents, and extensive reviewing experience for more than 135 international journals. His expertise spans high-performance computing, Linux/Unix, NLP, IoT, machine learning, cyber security, computer architecture, and computer networks, and he has supervised multiple Ph.D. scholars at Panjab University.

Mr. Shivam Jindal received the Bachelor of Engineering degree in computer science from Chandigarh College of Engineering and Technology, Panjab University, Chandigarh, India, where he is currently pursuing his undergraduate studies. His major field of study includes computer systems, backend engineering, and applied artificial intelligence. He is currently a Software Development Intern with the IT Department, Bharti Airtel, Chandigarh, India. Mr. Jindal is actively interested in large-scale software systems, system reliability, and applied AI for real-world engineering problems.

Mr. Prince Raj is a passionate and dedicated B.Tech Computer Science and Engineering student, actively seeking an internship to apply technical knowledge, build practical skills, and gain real-world industry exposure. He has a strong interest in research, product development, and hands-on projects involving web integration, dashboard development, and the implementation of machine learning and deep learning models. With solid problem-solving abilities, excellent communication skills, and the stamina for long, productive working hours, he is committed to continuous learning and innovation.

Mrs. Varsha Arya is a researcher affiliated with Hong Kong Metropolitan University, Hong Kong SAR, China, working in the broad area of computer science and intelligent systems. Her work spans topics such as network fault tolerance, cybersecurity, transfer learning, and deep learning–based models for applications including digital forensics and biomedical signal analysis. She actively collaborates with international teams and contributes to multidisciplinary research at the intersection of artificial intelligence, networking, and data-driven optimization.

Prof. Kwok Tai Chui is a Distinguished is a Professor in the School of Science and Technology at Hong Kong Metropolitan University, Hong Kong SAR, China. He received his B.Eng. in Electronic and Communication Engineering with a Business Intelligence minor and his Ph.D. in Electronic Engineering from City University of Hong Kong, both with first-class honors and multiple international IEEE awards, including the 2014 IEEE Region 10 Student Paper Contest (Postgraduate Category) prize and Best Paper Awards at IEEE International Conference on Consumer Electronics-China in 2014 and 2015. His research interests include computational intelligence, energy monitoring and management, pattern recognition, machine learning algorithms, optimization, smart healthcare, and intelligent transportation systems.

Prof. Brij B. Gupta is a Distinguished Professor in the Department of Computer Science and Information Engineering at Asia University, Taiwan, and Director of the International Center for AI and Cyber Security Research and Innovations. He received his Ph.D. in Information and Cyber Security from the Indian Institute of Technology Roorkee and, over nearly two decades of academic and research experience, has published more than 500–600 research papers, 35–40 books, and around 10–12 patents, with over 30,000–40,000 citations and multiple appearances in Clarivate's Highly Cited Researchers list and Stanford's top 2% scientist rankings. His research focuses on cyber security, cloud computing, artificial intelligence, intrusion detection, blockchain, cyber-physical systems, and Internet of Things security, and he serves on editorial boards and leadership roles in several international journals and IEEE societies, including Member-in-Large on the Board of Governors of the IEEE Consumer Technology Society.