CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

Notice for the PhD Viva Voce Examination

Ms Jinsi Jose (Registration Number: 1942043), PhD scholar at the School of Sciences, CHRIST (Deemed to be University), Bangalore will defend her PhD thesis at the public viva-voce examination on Wednesday, 20 December 2023 at 10.30 am in Room No. 044, Ground Floor, R & D Block, CHRIST (Deemed to be University), Bengaluru - 560029.

Title of the Thesis	:	**Hybrid Intrusion Detection Technique for Internet of Things**
Discipline	:	**Computer Science**
External Examiner (Outside Karnataka)	:	**Dr Muthumanikandan V** Associate Professor Department of CSE VIT Chennai Vandalur – Kelambakkam Road Chennai – 600127 Tamil Nadu
External Examiner (Within Karnataka)	:	**Dr Akhila S** Professor Department of Electronics & communication Engineering B.M.S. College of Engineering III Floor, Platinum Jubilee Block Bengaluru - 560019 Karnataka
Supervisor	:	**Dr Deepa V Jose** Associate Professor Department of Computer Science School of Sciences CHRIST (Deemed to be University) Bengaluru – 560029 Karnataka

The members of the Research Advisory Committee of the Scholar, the faculty members of the Department and the School, interested experts and research scholars of all the branches of research are cordially invited to attend this open viva-voce examination.

Registrar

Place: Bengaluru
Date: 13 December 2023

ABSTRACT

The rapid expansion of extensive IoT (Internet of Things) applications has significantly surprised and impacted modern society. The most crucial keyword concerning these applications is security, specifically in the enormous amount of data generated every second and how it is used. These applications are vulnerable to various attacks, which could result in an unthinkable catastrophe if not managed and controlled with sufficient foresight. Although many conventional methods are still used, there might be superior options for devices with limited resources. Artificial intelligence plays a significant role in this issue.

Using CNN with LSTM, this study suggests a hybrid intrusion detection system for anomaly-based and signature-based intrusions (CNN-LSTM). Anomaly and Signature Signature-based Detection System is the name of the proposed hybrid model (AS-CL IDS). The AS-CL IDS concentrated on two different IoT IDS detection strategies employing a combination of deep learning techniques. The model includes model training and testing as well as data preprocessing. The CIC-IDS 2018, IoT Network Intrusion Dataset, MQTT-IoT-IDS2020, and BoTNeTIoT-L01 datasets were used to train and test the AS-CL IDS. The overall performance of the proposed model was assessed using accepted assessment metrics. Despite reducing the number of characteristics, the model outperformed several other hybrid models.

Keywords: Internet of Things, Intrusion detection systems, machine learning, deep learning, hybrid intrusion detection.

Publications:

1. **Jose, J.** & Jose, D.V., 2019. Impact of Distributed Denial of Service attack in Internet of Things Applications- An Overview. International Journal of Advanced Science and Technology (IJAST), vol. 28, no. 17, pp. 201 – 205.
2. **Jose, J.** & Jose, D.V., 2023. Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset. International Journal of Electrical and Computer Engineering (IJECE), 13(1), pp.1134-1141.
3. **Jose, J.** & Jose, D.V., 2023. AS-CL IDS: Anomaly and signature-based CNN-LSTM intrusion detection system for Internet of Things. International Journal of Advanced Technology and Engineering Exploration (IJATEE).