

# **SIBI CHAKKARAVARTHY S** B.E, M.Tech, Ph.D.,

**Security Researcher - Network Security | Targeted Cyber Attacks | Advanced Persistent Threats | Malware analysis**

62/7a Standard colony, Thiruthangal, Sivakasi, Virudhunagar district, Tamil Nadu, India, pin – 626 130  
+91 9585583918, +91 9381622298, [sb.sibi@gmail.com](mailto:sb.sibi@gmail.com), [sb.sibi@mitindia.edu](mailto:sb.sibi@mitindia.edu)

## **Education**

- **Ph.D (2018): Network and System Security**  
**Anna University (Madras Institute of Technology (MIT) campus), Chennai.**  
**CGPA - 8.4.**  
**JRF - Department of Science and Technology (DST) Fellow**  
**Thesis Title: Targeted Cyber Attacks and their mitigation techniques**
- **Master of Technology (2014): Computer Science and Engineering**  
**VelTech Rangarajan Dr.Sagunthala R&D Institute of Science And Technology, Chennai**  
**CGPA - 8.9.**
- **Bachelor of Engineering (2012): Computer Science Engineering**  
**P.S.R Engineering College, Anna University, Chennai**  
**CGPA - 8.1.**

## **Work Experience**

- **Associate Professor, Vellore Institute of Technology – Andhra Pradesh (VIT-AP), 17.09.2018 - Till date.**
- **Assistant Professor, Vellore Institute of Technology – Andhra Pradesh (VIT-AP), 09.05.2018 - 16.09.2018.**
- **Junior Research Fellow (DST-PURSE II)**  
**Department of Electronics Engineering, Anna University (MIT Campus), (14.03.2015 - 31.12.2017)**
- **Junior Research Fellow (DST-NRDMS)**  
**Project title: “Complex Event Processing for sensor network”**  
**AU-KBC Research Centre, Anna University (MIT Campus), (04.1.2015 - 13.03.2015)**

## Research Grant

**Title** : **GPU accelerated security system**  
**Funding agency** : **NVIDIA**  
**Grant in INR** : **1.7L**  
**Duration** : **01.07.2018 - 01.07.2019**

## Fellowship, Awards and Achievements

- **Global Speaker Grant (2019)** – Sponsored by **University System of New Hampshire, United States of America.**  
**Grant Worth: \$3000 USD.**
- **Junior Research Fellow (2015 – 2017)** – Sponsored by **Department of Science and Technology (DST)** for pursuing **Ph.D.**

## Research Experience

### Remote Health Monitoring System [Award Winner - Hackathon]

- Deployed a cloud infrastructure using OpenNebula.
- Examined the literature on Activity recognition, remote healthcare and vital sign classification algorithms.
- Designed a Machine Learning based remote health monitoring system that performs intelligent diagnosis alerting the most common abnormalities such as fall, ECG, blood pressure and oxygen level - **National Winner in healthcare vertical**, Open Innovation Hackathon for Smart villages, 2017, organized by **Andhra Pradesh** Government.
- Genetic Algorithm is used (Selection, Mutation, Crossover).
- Fitness estimation is performed in each layer in order to estimate the best chromosome to fit.
- Scaled individual data node's disk space usage by setting up an alert threshold.

### Automatic Leaf Vein Feature Extraction (Research Intern at SS & DM group, C-DAC, Pune)

- Automatic Leaf Vein Feature Extraction
- Hough lines are used to extract the first degree veins and Centroid vein angle (medial axis line) is considered to be the primary feature.
- Skeletonization (Thinning) algorithm is applied to extract the possible medial axis from the veins and finally a pruning algorithm is applied to determine the dominant veins.
- A Sequential correlation is applied in order to perform template matching.
- Designed a plugin for leafilia (leaf recognition system developed by C-DAC) to extract first degree vein from leaf images.

### Face spoof attack detection

- A hybrid feature descriptor such as Color Local Binary Pattern (CLBP), Haralick feature, Color moment are used.
- Optimized the feature extraction phase using GPU-based real-time data analyses and speed up more than 5 times.
- NVIDIA Quadro K2000 is used for optimizing computation.
- OpenCV library is used for implementation

### **Automatic Phishing detection using machine learning techniques (algorithms)**

- Hybrid classification model is used to classify the phishing pages
- Ensemble of classifiers are used (Intermediate layer and Decision layer)
- Intermediate layer - Classifiers used: K-NN, RandomForest, Logistic regression, DNN (MLP with 5 neurons for each layer, Maximum epoch = 750)
- Random forest is further used to classify the results of intermediate layer.

### **Trajectory based Abnormal Event Detection in Video Traffic Surveillance**

- General Potential Data field (GPDf) is used along with spectral clustering to detect outliers such as illegal U-Turn, frequent lane changing and overlapping.
- Nvidia Quadro K2000 is used for GPDf estimation (approximately 1000 trajectories)
- Complex Event Processing (rule) Engine is used to make decisions.

### **Intrusion Detection Honeypot**

- Examined the literature on Honeypot, Intrusion Detection System, CEP etc.
- Designed a Hidden Markov Model based Honeypot to detect and prevent ransomware attacks.
- Hidden Markov Model is used as the classifier to classify the ransomware and benign activities.
- Viterbi algorithm is used for training the samples.
- Complex Event Processing (CEP) engine is deployed to aggregate the data from different security systems to confirm the ransomware behavior, attack pattern and respond them in a timely manner.
- Handled nearly 100+GB of logs.

### **CEP based Hybrid Intrusion Detection System**

- Examined the literature on Honeypot, Intrusion Detection System.
- Designed a CEP based Hybrid IDS that integrates the output of the Host IDS and Network IDS into the CEP Module and produces a consolidated output with higher accuracy.
- Multivariate Correlation Analysis (MCA) is used to estimate and characterize the normal behavior of the network.

### **Git**

- <https://github.com/sibichakkaravarthy>

### **Professional Experience**

- Experience with varied forms of practical data, including drone data, healthcare, logs & other high-dimensional data
- Strong expertise in detecting intrusions via network scans and deep packet analysis
- Hands-on experience in deploying cloud servers (OpenNebula, Openstack) and monitoring the Server Health status, backup management, update checklist and reports based on daily, weekly and monthly basis.

- Hands-on experience in deploying Honeypot (Dionaea) and Malware analysis sandboxes (Cuckoo) in production environment.
- Hands-on experience in deploying SIEM (OSSIM) to monitor real time security events (visualization using ELKB) using Elasticsearch, Logstash, Kibana and Beats (ELKB).

## Selective Publications

### Journal

1. **S. Sibi Chakkaravarthy**, V. Vaidehi and Steven Walczak, “Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles”, Journal of Medical Systems, **December 2019, Springer, (SCIE)**.
2. D. Arivudainambi, K.A. Varun Kumar, **S. Sibi Chakkaravarthy**, P. Visu, “Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance”, Computer Communications, **November 2019, Elsevier, (SCIE)**.
3. Akshay T, **S. Sibi Chakkaravarthy**, D. Sangeetha, M. Venkata Rathnam, V. Vaidehi, “Role Based Policy to Maintain Privacy of Patient Health Records in Cloud”, Journal of Super Computing, **June 2019, Springer, (SCIE)**.
4. **S. Sibi Chakkaravarthy**, D. Sangeetha and V. Vaidehi, “Intrusion Detection System to detect Wireless attacks in IEEE 802.11 networks”, IET networks, **July 2019, Volume 8, Issue 4, pp. 219- 232, IET**.
5. **S. Sibi Chakkaravarthy**, D. Sangeetha and V. Vaidehi, “A Survey on malware analysis and mitigation techniques”, Computer Science Review, **May 2019, Elsevier, (SCIE)**.
6. Jerart Julius L, Manimegalai D, **S. Sibi Chakkaravarthy**, “FBMC-Based Dispersion Compensation Using Artificial Neural Network Equalization for Long-Reach Passive Optical Network”, International Journal of Wavelets, Multiresolution and Information Processing, **April 2019, World Scientific Publisher, (SCIE)**.
7. Joshan Athaneious, **S. Sibi Chakkaravarthy**, S. Vasuhi and V. Vaidehi, “Trajectory based Abnormal Event Detection in Video Traffic Surveillance using General Potential Data field with Spectral clustering”, Multimedia Tools and Applications, **February 2019, Springer, (SCIE)**.
8. **S. Sibi Chakkaravarthy**, D. Sangeetha, M. Venkata Rathnam, K. Sri nithi, V. Vaidehi; "Futuristic cyber-attacks", International Journal of Knowledge based and Intelligent System Engineering, Vol.22, no.3, pp. 105- 204, 2018. **IOS press**.

9. **S. Sibi Chakkaravarthy**, P.Rajesh and V. Vaidehi, "Hybrid analysis technique to detect Advanced Persistent Threats", International Journal of Intelligent Information Technologies, 59 -76, Volume 14, Issue Q2, 2018, **IGI Global**.
10. V Mohanraj, **S. Sibi Chakkaravarthy**, I Gogul, V Sathiesh Kumar, Ranajit Kumar, V Vaidehi ; "Hybrid Feature Descriptors to Detect face Spoof Attacks", Journal of Intelligent & Fuzzy Systems, vol. 34, no. 3, pp. 1411-1419, 2018, **IOS press, (SCIE)**.
11. D. Arivudainambi, Varun Kumar K.A and **S. Sibi Chakkaravarthy**; "LION IDS: A meta-heuristic approach to detect DDoS attacks against Software Defined Networks", Neural Computing and Applications, 1-11, 2018, **Springer, (SCIE)**.

### **Monographs/Books/Book Chapters**

12. V Mohanraj, **S. Sibi Chakkaravarthy**, V Vaidehi; Ensemble of Convolutional Neural Networks for Face Recognition, Recent Developments in Machine Learning and Data Analytics, vol 740, 467-477, Springer, Singapore, 2019.
13. V Vaidehi, Ravi Pathak, Renta Chintala Bhargavi, Kirupa Ganapathy, C Sweetlin Hemalatha, A Annis Fathima, PTV Bhuvaneswari, **Sibi Chakkaravarthy S**, Xavier Fernando. Enhanced Complex Event Processing Framework for Geriatric Remote Healthcare, Handbook of Research on Investigations in Artificial Life Research and Development, 348-379, 2018, IGI Global.

### **Conference**

14. Mohan Raj, I Gogul, M Deepan Raj, V Sathiesh Kumar, V Vaidehi, **S Sibi Chakkaravarthy**; Analyzing ConvNet Depth for Deep Face Recognition, Second International Conference on Computer Vision & Image Processing", CVIP'17, IIT Roorkee, September 09 -12, 2017.
15. **Sibi Chakkaravarthy S** and V. Vaidehi; Drone based Targeted Cyber Attacks: A Practical Study, Doctoral colloquium, IDBRT, November 30 - December 1, 2017.
16. **Sibi Chakkaravarthy S** and V. Vaidehi; Deploying Low Interaction Honeypot for Darknet, Security and Privacy Symposium 2016 (SPS'16), IIITDelhi, February 12-13, 2016.
17. **Sibi Chakkaravarthy S** and V. Vaidehi; Hybrid analysis model to detect Advanced Persistent Threats, International Summer School on Information Security and Protection (ISSISP'16), 02-06 August, 2016. **(Best Research Paper award)**.
18. **Sibi Chakkaravarthy S** and V. Vaidehi; Behavior based anomaly detection model for detecting wireless covert attacks in Wi-Fi, Security and Privacy Symposium(SPS'15), IIITDelhi, February 13-14, 2015.

19. Ranjan Mohan, V Vaidehi, Ajay Krishna, M Mahalakshmi, **S Sibi Chakkaravarthy**; Complex Event Processing based Hybrid Intrusion Detection System, ICSCN'15, March 26-28, 1-6, 2015.
20. **S Sibi Chakkaravarthy**, G Sajeewan, E Kamalanaban, KA Varun Kumar; Automatic Leaf Vein Feature Extraction for First Degree Veins, SIRS'15, IIIT Kerala, AISC, 581-592 , Springer.
21. **Sibi Chakkaravarthy S** and V. Vaidehi; Detecting Covert attacks in Wireless networks, International Conference on Cloudification of the Internet of Things, June 10-11, 2015, Paris, France.
22. Kamalanaban Ethala, R Sheshadri, **S Sibi Chakkaravarthy**; WIDS-Real Time Intrusion Detection System using Entropical Approach, ICAEES, Artificial Intelligence and Evolutionary Algorithms, Springer, 73-79, 2014.

## **Magazine**

1. **Sibi Chakkaravarthy S** and Deepsagar Mandal; “Things you should know about Buffer overflow”, eForensics Magazine, March 2019.
2. **Sibi Chakkaravarthy S**; "Dissecting malwares using sandboxing technique", Pawning through Powershell, PentestMag, November 2016.
3. **Sibi Chakkaravarthy S**; “Volatility: The open source framework for memory forensics”, Open Source for you, October 2016, EFY publishers.
4. **Sibi Chakkaravarthy S**; “Introduction to Qubes”, Open Source for you, March 2016, EFY publishers.
5. **Sibi Chakkaravarthy S**; “Exploring processes using Sysinternals”, Open Source for you, January 2016, EFY publishers.
6. **Sibi Chakkaravarthy S**; “Malware analysis using REMnux” – Second series, Open Source for you, November 2015, EFY publishers.
7. **Sibi Chakkaravarthy S**; “Malware analysis using REMnux”, Open Source for you, October 2015, EFY publishers.
8. **Sibi Chakkaravarthy S**; “Things you should know about Advanced Persistent Threats”, Open Source for you, August 2015, EFY publishers.

## **Active Projects**

### **1. AI enabled Chatbot**

- **Chatbot name: VIT Assist, VIT Admissions.**
- **Available live in Google Assistant**

### **2. TARS: The Autonomous Rhapsody spider**

### **3. Humanoid – A physical personal assistant**

## **Student Research (under my guidance)**

1. “Tools that Accelerate a Newbie’s Understanding of Machine Learning”, Open Source for you, October 2019, EFY publishers.
2. “An Introduction to Processing, a Tool for Graphics Designers”, Open Source for you, November 2018, EFY publishers.
3. “Designing a simple 3d block jumper game”, Open Source for you, January 2019, EFY publishers.
4. “Things you should know about Buffer overflow”, eForensics magazine, Volume 08, 2019.

## **Courses Handled**

- Problem Solving using Java, Theory and Lab, Fall 2019.
- Web Technologies, Theory and Lab, Fall 2019.
- Problem solving using CPP, Lab, Summer 2018.
- Computer Graphics, Theory and Lab, Fall 2018.
- Secure Coding, Theory and Lab, Winter 2018.

## **Event Organized**

- One day Hackathon at VIT-AP on 08.10.2018.
- Four days FDP on Python and Java programming, 16.04.2019 – 20.04.2019.
- One day Workshop on Cyber Security, 04.11.2019.

## **Editorship**

- **Associate Editor, International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), IGI Global Publisher.**

## **Reviewer**

- **Computer Networks, Elsevier.**
- **IEEE Consumer Electronics, IEEE.**
- **Journal of Super Computing, Springer.**
- **IEEE Access, IEEE.**
- **International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), IGI Global.**
- **Journal of Organization and End User Computing, IGI Global.**

## **References**

### **Dr. V. Vaidehi**

Vice Chancellor

Mother Teresa Women's University, Kodaikanal

ph. +91 93810 41596, +91 99520 55529

### **G. Sajeevan**

Joint Director

Emerging Solutions and E-Gov Group,

Centre for Development of Advanced Computing (CDAC); Pune.

Ministry of Communication & Information Technology,

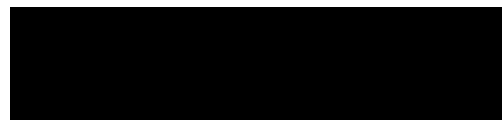
Government of India.

Ph. +91 94223 49936

email - sajeevan@cdac.in

**Place:Chennai**

**Date: 01.11.2019**



**SIBI CHAKKARAVARTHY S**