Deeraj Nagothu, Ph.D.

Research Scientist, Intelligent Fusion Technology Inc.

deerajnagothu10@gmail.com +1(607)-761-3956

Website GitHub LinkedIn Google Scholar

Research Interests

- Digital Multimedia Authentication, Information Assurance, Computer Network Security.
- AI/ML Model Development, Large Language Models (LLMs), Predictive Modeling and Anomaly Detection.
- Blockchain, Network Infrastructure Virtualization, and Software Defined Networking.

Work Experience

2023 – Present

- **Research Scientist.** Intelligent Fusion Technology Inc. (IFT), Germantown, MD, USA.
  - Led the development of a modular, transformer-based system for enhancing YOLOv9 object detection via synthetic image generation using Stable Diffusion XL and VLM-guided prompts, improving recall in low-visibility targets.
  - Designed and deployed ML-based anomaly detection models for time-series data streams with real-time geo-location visualization, using Elastic Stack (Elasticsearch, Kibana) and automated with Apache Airflow. Ensured STIG-based cybersecurity compliance.
  - Designed a secure, blockchain-enabled access control and data integrity framework using containerized ML workflows (Docker/Kubernetes) and Named Data Networking architecture for data exchange.
  - Authored multiple SBIR/STTR Phase I/II proposals on topics including AI model security, deepfake detection, 5G/SDN integration, and synthetic data-based feature engineering.

2018 – 2023

- **Research Assistant** SUNY Research Foundation, Binghamton University, Binghamton, NY, USA.
  - Designed and deployed a novel deepfake detection framework leveraging Electrical Network Frequency (ENF) signatures extracted from audio/video recordings, optimized for heterogeneous and low-power edge devices.
  - Developed pyenf, a Python library for multimodal ENF signal extraction and authentication. The package supports audio/video inputs and modular signal processing pipelines.
  - Built and validated ML pipelines towards media anomaly detection and interpretability.
  - Integrated authentication system into blockchain-enabled smart surveillance platforms, ensuring verifiable data provenance in decentralized public safety infrastructures, and real-time media authentication using ENF as consensus.
  - Developed GAN fingerprinting techniques that leveraged frequency-domain and artifact-based cues to detect AI-generated imagery, contributing to the early identification of synthetic media threats.

Education

2017 – 2023

- **Ph.D, Electrical and Computer Engineering**, Binghamton University-SUNY, Binghamton, NY, USA.
  Dissertation title: *Lightweight Multimedia Authentication at the Edge using Environmental Fingerprint*
  Advisor: Dr. Yu Chen

2015 – 2016

- **MS, Electrical and Computer Engineering**, Binghamton University-SUNY, Binghamton, NY, USA.
  Thesis title: *iCrawl: A high interaction client honeypot system.*
  Advisor: Dr. Andrey Dolgikh

2011 – 2015

- **B.Tech, Electronics and Communications Engineering**, SASTRA University, Tamil Nadu, India.

Skills

Coding	◇ Python, C/C++, C#, Shell, Bash, MATLAB, Powershell, SQL, LaTeX, Neo4j and Cypher.
Network and Security	◇ DHCP, SSH, VPN, DNS, Port-Forwarding, DMZ N/W, NMAP scan, Hyperledger Fabric, Pentesting using Metasploit framework, OpenDaylight for SDN, LibreNMS, Cacti Server, Tenable Nessus Scanner and DISA STIGs.
Deep Learning	◇ Pytorch, Keras, Tensorflow, FastAI, Hugging Face Transformers, Wandb, PEFT, Transformer-lens, NLTK, scikit-learn, Prompt Engineering.
Virtualization	◇ ESXi, Vyos, Cisco Nexus, HyperV, Xen, OpenStack, OpenMano, Docker, Kubernetes, Proxmox, GCP and AWS platforms
Misc.	◇ Grafana, Kibana, Elasticsearch, Logstash, Apache Airflow, Wireshark, Git/GitHub, JIRA, Tablueau, Snowflake.

Teaching Experience

Graduate Instructor	◇ **Network Computer Security (EECE-480F),**
Teaching Assistant	◇ **Cyber Physical Systems (EECE-480A), Cryptography and Information Security (EECE-405/560), Linear Algebra and Engg Programming (EECE-212),**

Research Publications

Journal Articles

1 Ogunbunmi, S., Chen, Y., Zhao, Q., **Nagothu**, **D.**, Wei, S., Chen, G., & Blasch, E. (2025). Interest Flooding Attacks in Named Data Networking and Mitigations: Recent Advances and Challenges. *Future Internet*, *17*(8), 357. Publisher: Multidisciplinary Digital Publishing Institute. doi:10.3390/fi17080357

2 Zhao, Q., **Nagothu**, **D.**, Tian, X., Chen, G., Pham, K. D., & Blasch, E. (2025). Sd-sat: Software-defined multi-constellation satellite communication traffic management framework. *IET Conference Proceedings*, *2024*(31), 71–78. Publisher: The Institution of Engineering and Technology. doi:10.1049/icp.2024.4615

3 Xu, R., **Nagothu**, **D.**, Chen, Y., Aved, A., Ardiles-Cruz, E., & Blasch, E. (2024). A Secure Interconnected Autonomous System Architecture for Multi-Domain IoT Ecosystems. *IEEE Communications Magazine*, *62*(7), 52–57. Conference Name: IEEE Communications Magazine. doi:10.1109/MCOM.001.2300354

4 Qu, Q., Hatami, M., Xu, R., **Nagothu**, **D.**, Chen, Y., Li, X., … Chen, G. (2024). The microverse: A task-oriented edge-scale metaverse. *Future Internet*, *"16"*(2), 60. doi:10.3390/fi16020060

5 **Nagothu**, **D.**, Xu, R., Chen, Y., Blasch, E., & Aved, A. (2022a). Defakepro: Decentralized deepfake attacks detection using enf authentication. *IT Professional*, *24*(5), 46–52. doi:10.1109/MITP.2022.3172653

6 **Nagothu**, **D.**, Xu, R., Chen, Y., Blasch, E., & Aved, A. (2022b). Deterring deepfake attacks with an electrical network frequency fingerprints approach. *Future Internet*, *14*(5), 125. doi:10.3390/fi14050125

7 Xu, R., **Nagothu**, **D.**, & Chen, Y. (2021a). Decentralized video input authentication as an edge service for smart cities. *IEEE Consumer Electronics Magazine*, *10*(6), 76–82. doi:10.1109/MCE.2021.3062564

8 Xu, R., **Nagothu**, **D.**, & Chen, Y. (2021b). Econledger: A proof-of-enf consensus based lightweight distributed ledger for iovt networks. *Future Internet*, *13*(10), 248. doi:10.3390/fi13100248

9 **Nagothu**, **D.**, Chen, Y., Aved, A., & Blasch, E. (2021). Authenticating video feeds using electric network frequency estimation at the edge. *EAI Endorsed Transactions on Security and Safety*, *"7"*(24). doi:10.4108/eai.4-2-2021.168648

10 Xu, R., Nikouei, S. Y., **Nagothu**, **D.**, Fitwi, A., & Chen, Y. (2020). Blendsps: A blockchain-enabled decentralized smart public safety system. *Smart Cities*, *3*(3), 928–951. doi:10.3390/smartcities3030047

°The complete list of publications is available on my Google Scholar page

11 **Nagothu**, **D.**, Chen, Y., Blasch, E., Aved, A., & Zhu, S. (2019). Detecting malicious false frame injection attacks on surveillance systems at the edge using electrical network frequency signals. *Sensors (Basel).*, *19*(11), 1–19. doi:10.3390/s19112424

Conference Proceedings

1 Hatami, M., Qu, Q., **Nagothu**, **D.**, Mohammadi, J., Chen, Y., Ardiles-Cruz, E., & Blasch, E. (2025). Securing Smart Grid Digital Twins via Real-World ENF Anchors Against Deepfake Attacks. (pp. 392–397). doi:10.1109/PerComWorkshops65533.2025.00097

2 Xu, R., Liu, X., **Nagothu**, **D.**, Qu, Q., & Chen, Y. (2025). Detecting Manipulated Digital Entities Through Real-World Anchors. In L. Barolli (Ed.), *Advanced Information Networking and Applications* (pp. 450–461). doi:10.1007/978-3-031-87784-1_41

3 Pazylkarim, A., **Nagothu**, **D.**, & Chen, Y. (2024). A lightweight deep learning model for rapid detection of fabricated ENF signals from audio sources. In *Disruptive Technologies in Information Sciences VIII* (Vol. 13058, pp. 363–375). doi:10.1117/12.3013456

4 Poredi, N., Sudarsan, M., Solomon, E., **Nagothu**, **D.**, & Chen, Y. (2024). Generative adversarial networks-based AI-generated imagery authentication using frequency domain analysis. In *Disruptive Technologies in Information Sciences VIII* (Vol. 13058, pp. 376–390). doi:10.1117/12.3013240

5 Zhao, X., **Nagothu**, **D.**, & Chen, Y. (2024). A homogeneous low-resolution face recognition method using correlation features at the edge. In *Sensors and Systems for Space Applications XVII* (Vol. 13062, pp. 107–123). doi:10.1117/12.3008368

6 Poredi, N., **Nagothu**, **D.**, & Chen, Y. (2024). Authenticating ai-generated social media images using frequency domain analysis. In *2024 ieee 21st consumer communications & networking conference (ccnc)* (pp. 534–539). ISSN: 2331-9860. doi:10.1109/CCNC51664.2024.10454640

7 **Nagothu**, **D.**, Xu, R., Chen, Y., Blasch, E., & Ardiles-Cruz, E. (2023). Application of Electrical Network Frequency as an Entropy Generator in Distributed Systems. In *NAECON 2023 - IEEE National Aerospace and Electronics Conference* (pp. 233–238). ISSN: 2379-2027. doi:10.1109/NAECON58068.2023.10365792

8 Parker, J., **Nagothu**, **D.**, & Chen, Y. (2023). Decentralized Vehicular Identification and Tracking on Lightweight IoT Edge Nodes. In *NAECON 2023 - IEEE National Aerospace and Electronics Conference* (pp. 198–203). ISSN: 2379-2027. doi:10.1109/NAECON58068.2023.10365952

9 **Nagothu**, **D.**, Xu, R., & Chen, Y. (2023). DEMA: Decentralized electrical network frequency map for social media authentication. In *Disruptive Technologies in Information Sciences VII* (Vol. 12542, pp. 57–72). doi:10.1117/12.2663303

10 Poredi, N., **Nagothu**, **D.**, & Chen, Y. (2023). AUSOME: Authenticating social media images using frequency analysis. In *Disruptive Technologies in Information Sciences VII* (Vol. 12542, pp. 44–56). doi:10.1117/12.2663296

11 Poredi, N., **Nagothu**, **D.**, Chen, Y., Li, X., Aved, A., Ardiles-Cruz, E., & Blasch, E. (2022). Robustness of electrical network frequency signals as a fingerprint for digital media authentication. In *2022 ieee 24th international workshop on multimedia signal processing (mmsp)* (pp. 1–6). doi:10.1109/MMSP55362.2022.9949315

12 **Nagothu**, **D.**, Dimock, D., Kulesza, A., Yang, H., & Chen, Y. (2022). A distributed crawler for iovt-based public safety surveillance exploring the spatio-temporal correlation. In *Sensors and systems for space applications xv* (Vol. 12121, pp. 18–28). doi:10.1117/12.2618909

13 **Nagothu**, **D.**, Xu, R., Chen, Y., Blasch, E., & Aved, A. (2021a). Detecting compromised edge smart cameras using lightweight environmental fingerprint consensus. In *Proceedings of the 19th acm conference on embedded networked sensor systems* (pp. 505–510). doi:10.1145/3485730.3493684

14 **Nagothu**, **D.**, Xu, R., Chen, Y., Blasch, E., & Aved, A. (2021b). Defake: Decentralized enf-consensus based deepfake detection in video conferencing. In *Ieee 23rd international workshop on multimedia signal processing*. doi:10.1109/MMSP53017.2021.9733503

15 Quan, W., **Nagothu**, **D.**, Poredi, N., & Chen, Y. (2021). Cripi: An efficient critical pixels identification algorithm for fast one-pixel attacks. In *Sensors and systems for space applications xiv* (Vol. 11755, pp. 83–99). doi:10.1117/12.2581377

16 Rosenberg, M., Burns, J. H., **Nagothu**, **D.**, & Chen, Y. (2020). Enabling continuous operations for uavs with an autonomous service network infrastructure. In *Sensors and systems for space applications xiii* (Vol. 11422, pp. 165–179). doi:10.1117/12.2565866

17 Fitwi, A. H., **Nagothu**, **D.**, Chen, Y., & Blasch, E. (2019). A distributed agent-based framework for a constellation of drones in a military operation. In *Proc. - winter simul. conf.* (Vol. 2019-Decem). doi:10.1109/WSC40007.2019.9004907

18 **Nagothu**, **D.**, Schwell, J., Chen, Y., Blasch, E., & Zhu, S. (2019). A study on smart online frame forging attacks against video surveillance system. In *Proc. spie - int. soc. opt. eng.* (Vol. 11017). doi:10.1117/12.2519005

19 **Nagothu**, **D.**, Xu, R., Nikouei, S. Y., & Chen, Y. (2019). A microservice-enabled architecture for smart surveillance using blockchain technology. In *2018 ieee int. smart cities conf. isc2 2018*. doi:10.1109/ISC2.2018.8656968

20 Nikouei, S. Y., Xu, R., **Nagothu**, **D.**, Chen, Y., Aved, A., & Blasch, E. (2019). Real-time index authentication for event-oriented surveillance video query using blockchain. In *2018 ieee int. smart cities conf. isc2 2018*. doi:10.1109/ISC2.2018.8656668

21 **Nagothu**, **D.**, & Dolgikh, A. (2017). Icrawl: A visual high interaction web crawler. In *Lect. notes comput. sci. (including subser. lect. notes artif. intell. lect. notes bioinformatics)* (Vol. 10446 LNCS). doi:10.1007/978-3-319-65127-9_8

Book Chapters

1 Xu, R., **Nagothu**, **D.**, Chen, Y., Xu, R., **Nagothu**, **D.**, & Chen, Y. (2024). AR-Edge: Autonomous and Resilient Edge Computing Architecture for Smart Cities. doi:10.5772/intechopen.1005876

2 **Nagothu**, **D.**, Poredi, N., & Chen, Y. (2022). Evolution of attacks on intelligent surveillance systems and effective detection techniques. doi:10.5772/intechopen.105958

3 Xu, R., **Nagothu**, **D.**, & Chen, Y. (2022). Ecom: Epoch randomness-based consensus committee configuration for iot blockchains. In K. Daimi, I. Dionysiou, & N. El Madhoun (Eds.), *Principles and practice of blockchains* (pp. 135–154). doi:10.1007/978-3-031-10507-4_7

4 **Nagothu**, **D.**, Xu, R., Nikouei, S. Y., Zhao, X., & Chen, Y. (2020). Smart surveillance for public safety enabled by edge computing. (pp. 409–433). doi:10.1049/PBPC033E_ch19

Books

1 **Nagothu**, **D.**, & Chen, Y. (2023). *Authentication of video feeds in smart edge surveillance networks* (C. Olson, Ed.). Bellingham, Washington 98227-0010: SPIE Press.

Dissertation and Thesis

1 **Nagothu**, **D.** (2023). *Lightweight Multimedia Authentication at the Edge Using Environmental Fingerprint* (Ph.D. State University of New York at Binghamton, United States – New York). ISBN: 9798380566988. Retrieved October 28, 2023, from https://www.proquest.com/docview/2872097834/abstract/A49AAD7CD800446BPQ/1

2 **Nagothu**, **D.** (2016). *Icrawl: A high interaction client honeypot system* (M.S. State University of New York at Binghamton, United States – New York).

Professional Activities

Reviewer for Journals

- IEEE Transactions on Pattern Analysis and Machine Intelligence

Professional Activities (continued)

- IEEE Transactions on Multimedia Computing Communications
- IEEE Transactions on Dependable and Services Computing
- IEEE Transactions on Services Computing
- IEEE Internet of Things Journal
- SPIE Journal of Electronic Imaging (JEI).
- Elsevier Computers and Security
- Expert Systems with Applications
- IEEE Access
- IEEE Transactions on Aerospace and Electronic Systems
- IEEE Transactions on Cloud Computing
- IEEE Computers
- Applied Sciences
- MDPI Sensors

Reviewer for Conferences

- IEEE International Conference on Computer Communications (INFOCOM).
- IEEE Communications Magazine (COMMAG)
- IEEE Global Communications Conference (GLOBECOM) IoT and Sensor Networks (IoTSN).
- IEEE Global Communications Conference (GLOBECOM) Communication and Information Systems Security (CISS).
- IEEE Global Communications Conference (GLOBECOM) Communications Software, Services and Multimedia Apps (CSSMA).
- IEEE International Conference on Wireless and Mobile Computing, Networking And Communications (WiMob).
- ACM International Workshop on Blockchain-enabled Networked Sensor Systems (BlockSys)
- IEEE International Smart Cities Conference (ISC2).
- IEEE International Conference on Cloud Networking (CloudNet)
- IEEE International Conference on Communications (ICC)
- Knowledge based Systems (KNOSYS)
- Scientific Reports

Miscellaneous Experience

Awards and Achievements

2025
- **Best Paper Award**, Best Workshop Paper at IEEE Percom SPT-IoT Conference. (Securing Smart Grid Digital Twins via Real-World ENF Anchors against DeepFake Attacks)
- **Finalist**, xTech AI Competition, for the project "GRADIENT", focused on synthetic data-based feature engineering for robust AI model performance.
- **Winner** IEEE AESS Cybersecurity Challenge: Authored the winning challenge proposal “Federated AI for Resilient Avionics and Drone Operations,” establishing a federated learning benchmark for resilient aerospace and drone cybersecurity research.

2020
- **GSEA**, Graduate Student Award for Excellence in Teaching (**Courses** - Network Computer Security and Cyber Physical Systems).