Munawar Hasan

Contact Information

222/A362, Chemistry Building
National Institute of Standards and Technology (NIST)
Gaithersburg, MD, USA

munawar.hasan@nist.gov
munawar3008@gmail.com

Public Profile Website · LinkedIn · Github

Research Interest Cryptography · Artificial Intelligence · Blockchain · Biometric Security

Executive Summary

I am working as a foreign guest researcher at Computer Security Division of NIST (National Institute of Standards and Technology). I work in the area of Cryptography, Artificial Intelligence and related areas.

Cryptography: My research is centered around design and analysis of cryptographic algorithms that target the design space of lightweight cryptography. I have worked extensively on theoretical and practical aspects of authenticated encryption schemes under various security notions. Lynx: family of lightweight authenticated encryption schemes based on a tweakable blockcipher, and provides birthday bound security for integrity security (nonce misuse and RUP scenarios), and birthday bound security for confidentiality (nonce respecting scenario). I was also involved in validating and benchmarking implementations on various IoT hardware, for the candidates participating in the lightweight cryptography competition (LWC) at NIST.

I have also worked in the area of biometric cryptosystems like cancelable biometrics, fuzzy commitment and fuzzy vault. I have worked in the development of large scale biometric authentication systems. I have worked in the research and development of biometric algorithms for Iris, and implemented them at the kernel level, for low-powered and handheld devices.

AI: I am working in the NIST Automated Vehicle Program in the AV AI team under Strategic and Emerging Research Initiatives (SERI), on various computer vision tasks like classification and detection in the area of autonomous driving. Our research interest include measurement, evaluation and reporting of uncertainty induced in these tasks in driving conditions. We are also working on generating adversarial scenarios on CARLA simulator, and evaluating the performance of models on these adversarial attacks. I have also experience in the area of large language models (LLMs) and have worked on several NLP tasks like sentiment analysis, hate speech detection and meta-learning techniques.

Industry Experience

Foreign Guest Researcher (Research and Science) — January 2020-Present
National Institute of Standards and Technology (NIST)
Computer Security Division
Gaithersburg, Maryland, USA

Senior Researcher — July 2016-June 2022
Irisys Co. Ltd.,
IRISYS-IIITD R&D Lab
New Delhi, India

Software Engineer — Sept 2010-May 2013
DXC Technology (formerly Computer Sciences Corporation)
Noida, India

Education

Master of Technology, CGPA: 8.89/10 — Aug, 2014-Jun 2016
Information Security (Computer Science)
Thesis Title: Cryptanalysis of SHA2 based on Perturbation technique
Advisor: Dr. Somitra Sanadhya
IIIT-Delhi, India

Bachelor of Technology, 84.87% — Aug, 2006-May 2010
Computer Science and Engineering
Dehradun Institute of Technology, Dehradun

Technical Skills

Programming	:	C, Java, Python, Julia, Android, Latex.
Frameworks/Tools	:	PyTorch, PyTorch Lightning, Tensorflow, Keras, CARLA, OpenCV, CUDA, Hyperledger Fabric, Android Kernel(BSP).
IDE	:	Mathematica, MATLAB, Clion, Pycharm, Android Studio, Xcode, VS Code, Eclipse.
Hardware	:	ESP32, LockIT(Rockchip), NVIDIA Jetson TX2, Arduino (Uno, Nano, Due), Nordic nRF52, Movidius, Raspberry Pi, RP2040.

Industrial Projects

- **NIST Autonomous Vehicles Project**
  The goal of the project is to measure of uncertainty in the area of autonomous driving for computer vision related tasks like object classification and object detection. Evaluated state-of-the-art models like YOLOv8, DETR, RT-DETR etc. on custom dataset generated for replicating real world scenarios. Implemented GaussianYOLO and BayesianYOLO and reported localization uncertainty, aleatoric uncertainty and epistemic uncertainty. Implemented Ensemble techniques for reporting uncertainty estimates.
  Developed web application based on Flask with backend as Hugging Face and Ultralytics for evaluating object detection models on finely curated datasets (with corner cases). The web app also displays a leaderboard to showcase best performing models. End users can also upload their dataset for evaluating them against state-of-the-art models.
  Proposed several experiments on CARLA simulator for generating adversarial scenarios for autonomous driving.
- **Context Commitment Security Analysis of AEAD**
  Currently I am working on security analysis for tweakable wide block ciphers like HBSH, HCTR2, double-decker and docked-double-decker under encode-then-encrypt paradigm. Provided CMT-4 attack with time complexity as $O(1)$ on all the four tweakable wide block ciphers under EtE paradigm.
  Evaluating CMT-4 security for various NIST LWC finalists, where the AEAD has sponge function as the underlying primitive.
- **Design and Security Analysis of AEAD based on Tweakable Blockcipher**
  Proposed 72 AEAD constructions based on a tweakable blockcipher and evaluated each of them on various security parameters. After analysis of each of the 72 constructions, proposed lynx (lynx-A and lynx-B). Lynx is a 1-pass and rate-1 family of lightweight authenticated encryption scheme based on a tweakable blockcipher, and has an edge both at the design level and at the implementation level when compared to NIST LWC candidates like Romulus.
- **Meta-Learning Techniques with Language Models**
  1. Meta-Learning technique (MLT) that combines individual models built with different text representations. For the combination so created, we analytically showed that the technique is numerically stable and produces reasonable combining weights. Proposed a threshold-moving (TM) technique over the base

MLT to further enhance the performance. The project involved training of LLMs: BigBird, BERT, BERTweet, Bloom and XLNet on CAD dataset and HateCheck dataset. Some of the major challenges in this project were handling skewness in the dataset and generating performance gain on both multi-label as well as binary label task for both MLT and MLT-TM techniques as compared to performance of individual models.

2. Proposed meta-learning architecture SSNet that is inspired by a specialized neuron formation, called Sagittal Stratum (SS). SSNet consists of three methods for combining language models .i.e, neural network combiner, Bayesian decision rule combiner and heuristic hybrid combiner. Neural network combiner outperformed all the individual participating models.

- **BLE based Doorlock and Smarthub with Amazon IoT integration**: Development of bluetooth based doorlock and smarthub integrated with Amazon IoT cloud. The development involves working on Board support package (BSP) for doorlock and smarthub and an android app for user interaction. Links: demo, doorlock product.
- **FIDO Alliance: IRIS based FIDO2, UAF and U2F Authenticators** Implemented entire line of FIDO protocols (FIDO2, UAF, U2F) for authenticators based on Iris Authentication at the Kernel level for custom board using BSP. All our implementations successfully received certification by FIDO Alliance. FIDO2 Iris Authenticator; LockIT, was the world's first and (currently) only Iris based certified FIDO2 and UAF authenticator in the world. FIDO2 is a standard for Bio-metric Authentication, supported and standardized by W3C under Webauthn. Google Chrome, Microsoft Edge, Apple's Safari etc. have already enabled the use of FIDO2 for authentication.
- **IoT: Smartbulb and Smarthub Integration with Amazon Alexa** Designed complete architecture for Home Automation based on Smartbulb and Smarthub using AVS and AWS. Alexa Skill was implemented on AWS Lambda using NodeJS. This skill used to take voice input from AVS devices like Amazon Echo to command actions for Smartbulb. This lambda function sends AVS parsed content to our JSP Server hosted on a different cloud service platform(Digital Ocean), which stores this parsed content in its Application context. The Smarthub, implemented on Raspberry Pi v3 (using Python) fetches the content from this JSP Server's application context and parses it into a command to send it to Smartbulb for necessary actions (on, off etc.) using BLE. Additionally, I also created Android app for users to connect, name and control their Smartbulb and configure their Smarthub using AP mode.
- **IRIS/PIN Based Access Control System** Designed and implemented Iris and Pin based Access Control System. The Access Control System, ACS consists of 3 modules, Server, Android Client and Windows Admin Software. The Server was based on REST Services and used Public Key Cryptosystem (RSA 2048) for communication with Android Client and the Admin Software. The Iris details is encrypted using AES128 in CBC mode. User can authenticate himself using the Android Client App by scanning his/her Iris or entering the Pin. The product is used by several companies across Korea and the US as an authentication system.
- **Fingerprint Extraction Software** Developed Minutiae Extraction Software from FVC2002 database or from Live Scan for ETRI (Electronics and Telecommunications Research Institute, Korea). The extracted minutiae was then converted to ISO and IST format and stored for future research work. The development included study and analysis of several research papers due to the fact that FVC2002 is one of the poorest dataset. The developed Software was able to extract all the minutiae even in the poorest images.

Publications and Submissions

- Donghoon Chang, **Munawar Hasan:**
  Context-Committing Authenticated Encryptions using Tweakable Stream Cipher, Published in IEEE Access 2024.
- **Munawar Hasan**, Donghoon Chang**:**
  Lynx: Family of Lightweight Authenticated Encryption Schemes based on Tweakable Blockcipher, Published in IEEE Internet of Things Journal 2023.
  Full version: Cryptology ePrint [Link] [Source Code].
- Apostol Vassilev, Honglan Jin, **Munawar Hasan:**
  Meta learning with language models: Challenges and opportunities in the classification of imbalanced text, arXiv 2023 [Link].
- Donghoon Chang, Surabhi Garg, **Munawar Hasan**, Sweata Mishra**:**
  On Security of Fuzzy Commitment Scheme for Biometric Authentication, Published in ACISP 2022.
- Apostol Vassilev, **Munawar Hasan**, Honglan Jin**:**
  Can you tell? SSNet – a Sagittal Stratum-inspired Neural Network Framework for Sentiment Analysis, Published in LOD 2021.
  Full version: [arXiv] [Source Code].
- Donghoon Chang, Surabhi Garg, Mohona Ghosh, **Munawar Hasan:**
  BIOFUSE: A Framework For Multi-Biometric Fusion On Biocryptosystem Level, Published in Elsevier Information Sciences 2021.
- Donghoon Chang, Surabhi Garg, **Munawar Hasan**, Sweata Mishra**:**
  Cancelable Multi-biometric Approach using Fuzzy Extractor and Novel Bit-wise Encryption, Published in IEEE TIFS 2020.
- Donghoon Chang, Vinjohn Chirakkal, Shubham Goswami, **Munawar Hasan**, Taekwon Jung, Jinkeon Kang, Seok-Cheol Kee, Dongkyu Lee, Ajit Pratap Singh**:**
  Multi-lane Detection Using Instance Segmentation and Attentive Voting, Published in ICCAS-2019.
- Donghoon Chang, **Munawar Hasan**, Pranav Jain**:**
  Spy Based Analysis of Selfish Mining Attack on Multi-Stage Blockchain, Cryptology ePrint 2019 [Link].

Lectures, Talks and Participation

- Autonomous Vehicle Training by Dataspeed Inc. for Drive-by-Wire (DBW) kit on Ford Fusion, NIST Campus, Gaithersburg, MD, April 2024.
- VTTI (Virginia Tech Transportation Institute) invited NIST Automated Vehicles Team for discussing research collaboration and providing tour of VTTI Smart Road testing facility, Blacksburg, VA, February 2024. [Newsletter].
- Invited for a talk on Meta-Learning technique for HateSpeech Detection at Artificial Intelligence Community of Interest (AI COI), NIST, Gaithersburg, MD, November 2023.
- CAMLIS 2023: Conference on Applied Machine Learning for Information Security, Arlington, VA, October, 2023.
- Third NIST Workshop on Block Cipher Modes of Operation, National Cybersecurity Center of Excellence (NCCoE), Rockville, MD, October 2023.
- MPTS 2023: NIST Workshop on Multi-party Threshold Schemes, Virtual [link], September 2023.
- Standards and Performance Metrics for On-Road Automated Vehicles Workshop, Virtual [link], September 2023.
- Poster Presentation at ITL Science Day, NIST, October 2022.
- Paper Presentation at Conference on Machine Learning, Optimization, and Data Science (LOD), October 2021 (online participation).
- Poster at ITL Science Day, NIST, October 2020
- Invited for a talk on GPU Cluster at NIST, Gaithersburg, MD, August 2020.
- Invited for a talk on Hyperledger Fabric and Anti-Spoofing using AI at ETRI, Daejeon, South Korea, April 2019

- Invited for a two day lecture on Quantum Computing at IIT Delhi, March 2019.
- FIDO2 Certification for Iris based Authenticator, Seoul, South Korea, October 2018.
- Invited for a three day lecture on Quantum Computing at IIIT Delhi, April 2018.
- Exhibitor at RSA Conference, Moscone Center, San Francisco, CA, February 2017.
- FIDO UAF Certification for Iris based Authenticator, Fremont, CA, December 2016.

Personal R&D

- Searchable Symmetric Encryption Database; SSE-DB (sunset), http://sse-db.com/
- Quantum Algorithm Simulator (sunset). Some algos can be tried at: following link

Personal Details

- Gender: Male
- Hobbies: Astronomy, Browsing about technological research, Watching Cricket/Football
- Languages: English and Hindi

References

Dr. Donghoon Chang
Associate Professor, IIIT-Delhi, India
Email: donghoon@iiitd.ac.in

Dr. Apostol Vassilev (Fed)
Research Team Supervisor, NIST, USA
Email: apostol.vassilev@nist.gov

Dr. Edward Griffor (Fed)
Associate Director for Cyber-Physical Systems (CPS) and Internet of Things (IoT), NIST, USA
Email: edward.griffor@nist.gov

Honglan Jin (Fed)
Computer Scientist, NIST, USA
Email: honglan.jin@nist.gov

Dr. Thoshitha Gamage
Associate Professor, Southern Illinois University Edwardsville (SIUE), USA
Email: tgamage@siue.edu