Munawar Hasan

Contact Information

769 Quince Orchard Blvd
Gaithersburg, MD
USA

+1 202-738-8909
munawar.hasan@nist.gov
munawar3008@gmail.com

Public Profile Website, LinkedIn, Github

Research Interest Cryptography, Artificial Intelligence, Blockchain, IoT, Quantum Computing

Executive Summary

I am working as a guest researcher at Computer Security Division of NIST in the threshold crypto group for the standardization of threshold schemes of the cryptographic primitives. Areas of research includes secret shares, threshold signature, multiparty computation, single and multi core implementations. I am also involved in research based work with multiple firms and have over 6 years of experience in IT industry across various fields including artificial intelligence, IoT, blockchain technology and custom firmware development (bsp) for custom low powered hardware devices. I have also got experience in design and analysis of biometric algorithms (Iris and Face). I have worked on several custom hardware and SoCs like Rockchip, Nordic nRF series etc. Further, I have also got exposure in deploying AI models on embedded devices. I am proficient in ML libraries like tensorflow, keras and pytorch and gpu libraries like cuda.

Recent Work: I am working on certain theoretical and practical aspects of threshold signatures and single/multi core implementations of symmetric cryptosystem. I am also working with the AI group of NIST on NLP. Implemented FIDO2 authenticator protocol at the firmware level. Our hardware (with the developed firmware) successfully passed FIDO2 certification I am also working on development of a product based on hyperledger fabric for automated billing system.

Industry Experience

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

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

Software Engineer — Sept 2010-May 2013
Computer Sciences Corporation (CSC)
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
Framework, Tools and IDE	:	OpenCV, Tensorflow, Keras, CUDA, Hyperledger Fabric, Android Kernel(BSP), Clion, Pycharm, Eclipse, Keil, Android Studio, Xcode, Visual Studio
Hardware	:	NVIDIA Jetson TX2, Movidius, LockIT(Rockchip), Nordic nRF52, Raspberry Pi

Industrial Projects

- **Evaluation of Threshold Crypto Schemes**
  Working towards evaluation and standardization of several algorithms both a public and symmetric. Also working on single and multicore implementations of symmetric ciphers.
- **Evaluation of LWC Candidates**
  Working of evaluation of candidates of lightweight competition. The evaluation is two fold: claimed security bounds and performance on microcontrollers and power constrained SoC
- **Autonomous Driving: Multi-Lane Detection**
  Designed end to end architecture for detecting the lanes of the road for Smart Car Center at Chungbuk National University, Korea. The architecture is divided into several phases and is under development. The first phase was able to achieve very high accuracy and speed. The model ran efficiently on NVIDIA Jetson TX2 and detected lanes even during partial visibility (rain, sunlight) and no-visibility (occluded). The architecture was validated on KITTI dataset and performed better than base implementation
- **Blockchain: Employee Tracking System**
  Proposed a blockchain based project to track employees. The blockchain forms a backbone of proposed system to irradiate refutability and non-trusted or malicious activities. The project is integrated into ERP with services like automated billing, messaging services, leaves management, hierarchical workflow etc. Currently, crash tolerance is used as a means for reaching consensus, later to be replaced by PBFT. The project is currently under development with several POCs completed
- **FIDO Alliance: IRIS based FIDO2, UAF and U2F Authenticators**
  Implemented entire line of FIDO protocols (FIDO2, UAF, U2F) for authenticators on Iris Authentication at the Kernel level for custom board using BSP. All our implementations successfully received certification by FIDO Alliance. Our FIDO2 Iris Authenticator; LockIT, is the world's first and (currently) only Iris based certified 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
- **Automatic Encryption**
  Implemented AES128 bit Encryption and Decryption in CBC mode at the Kernel level for the custom hardware, LockIT device. When user plugs out the USB from the Machine (Desktop + Android), the data on the USB drive get encrypted automatically. Upon successful Iris scan, the data is Decrypted automatically. It provides security against the theft or unwanted access
- **IoT: Smartbulb and Smarthub Integration with Amazon Alexa**
  Designed complete architecture for Home Automation based on Smartbulb and Smarthub using AVS and AWS. The architecture included several components that interacted with each other in real time.
  The implementation included 4 different development platforms. The first "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 Pi3 (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.
This product become one of the main line of business and later the Smarthub functionalities were imbedded into the Smartbulb itself followed by imbedding of AI modules

- **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 User registered using the Windows Admin Software written in C#. The User also register's his/her Iris and Pin from this Software. All the registration details is sent to the Rest Server. The Iris details is encrypted using AES128 in CBC mode. The Server stores the details in MySQL. Once successfully registered, the User can authenticate himself using the Android Client App by scanning his Iris or entering the Pin. The authentication is logged onto Server.
  The product is one of our best seller and is used by several companies across Korea and US as a complete 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. We added a custom layer for image enhancement. Our Software was able to extract all the minutiae even in the poorest images
- **Deep Learning Based Detection System for Harbor**
  Used transfer learning for training ML model based on COCO dataset for automatically detecting whether the crane is detached from the truck correctly or not, through CCTV live stream. The position of the truck was determined using the Object Detection Module in Tensorflow. Once the truck's position was obtained, its motion was tracked using SURF in subsequent frames. If the motion was upward a flag was initiated and the system halted automatically

Publications and Submissions

- Donghoon Chang, Surabhi Garg, Mohona Ghosh, **Munawar Hasan:**
  BIOFUSE: A Framework For Multi-Biometric Fusion On Biocryptosystem Level, Published in Elsevier Information Sciences
- Donghoon Chang, Surabhi Garg, **Munawar Hasan**, Sweata Mishra**:**
  Cancelable Multi-biometric Approach using Fuzzy Extractor and Novel Bit-wise Encryption, Published in IEEE TIFS
- 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
- Apostol Vassilev, **Munawar Hasan:**
  Can you tell? SSNet – a Sagittal Stratum-inspired Neural Network Framework for Sentiment Analysis, Submitted to arXiv [Link]
- Donghoon Chang, **Munawar Hasan**, Pranav Jain**:**
  Spy Based Analysis of Selfish Mining Attack on Multi-Stage Blockchain, Submitted to Cryptology [Link]
- Submitted: Donghoon Chang, Surabhi Garg, **Munawar Hasan**, Sweata Mishra**:**

An Improved Construction of Fuzzy Commitment Scheme for Biometric Authentication, in Elsevier [Result Awaited]

Lectures and Talks

- 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
- Invited for a three day lecture on Quantum Computing at IIIT Delhi, April 2018

Organizational Associations

- IIIT Delhi (New Delhi, India): Cryptographic Research Group (CRG)
- Chungbuk National University (Cheongju, South Korea): Smart Car Center
- Delhi Government: Dept. of Environment of NCT of Delhi (Pollution Control)
- ETRI (Eletronics and Telecommunications Research Institute, Daejeon, South Korea): Dept. of Information Security

Personal R&D

- Creator of Searchable Symmetric Encryption Database; SSE-DB, http://sse-db.com/
- Quantum Algorithm Simulator (sunset)
  Some algos can be tried at: following link
- Alexa Skill: Quantum Computing Guide (Status: Published)

Personal Details

- Gender: Male
- Hobbies: Browsing about technological research
  Writing articles for technical magazines, playing and watching Cricket
- Languages: English and Hindi

References On Request