Himanshu Goyal

Contact Information

MHR, Room B - 150
IIT Bhubaneswar
Orissa, India
Tel: (+91) – 8078698408

Homepage: https://move47.github.io/
Github: https://github.com/move47
✉ E-mail: hg11@iitbbs.ac.in

Research Interests

I am broadly interested in developing practical systems which guarantees – Security, Privacy and Robustness. Special topics of focus include: Multi-party Computation, Homomorphic Encryption, Fault tolerance, Functional Encryption, Zero-Knowledge Proofs, Privacy Preserving Machine Learning, Blockchains.

Education

Indian Institute of Technology, Bhubaneswar, Orissa, India — 2017–2022 (expected)

- *Dual-Degree(B.Tech+M.Tech) in Computer Science and Engineering*
- CGPA: **9.41**[1] – via 209 credits
- Thesis: Practical Byzantine Fault tolerance for WSNs/IoT
- Advisor: Dr. Sudipta Saha

Birla School Pilani, Rajasthan, India — 2014–2016

- Intermediate(+2) , Percentage: **93.00%**

Publications

Practical Byzantine Consensus for Internet of Things
Himanshu Goyal and Sudipta Saha. Under Review. Preprint.

Multi-Party Computation in IoT for Privacy-Preservation (Poster)
Himanshu Goyal and Sudipta Saha. Under Review. Preprint.

Research Experience

- **Decentralised and Smart Systems Research Group** - *Research Assistant* May 2020 –
  Advisor: Prof. Sudipta Saha, Indian Institute of Technology, Bhubaneswar
  - Developed an efficient protocol for achieving Byzantine consensus in IoT/WSNs networks using Synchronous Communication. Our proposed design can work up to 80% faster and consume 82% less energy than a naive implementation in both simulation and emulation.
  - Designed a single round efficient non-interactive protocol using Secret sharing techniques for IoT analytics.

- **Cryptography and Information Security Lab** - *Research Assistant* June 2020 – Dec 2020
  Advisor: Prof. Arpita Patra, Indian Institute of Science, Banglore
  - Implemented Privacy-Preserving algorithms for training and inference for machine learning algorithms using the *ABY3* framework.
  - Developed algorithms used Secret sharing schemes and achieved a reduction in both communication and computation time than existing 3PC approaches for semi-honest settings.

- **TCS Research and Innovation, Kolkata** - *Research Assistant* May 2020 – July 2020
  Advisor: Chayan Sarkar
  - Collaborated with the members of Embedded Systems and Robotics Lab. Build customized language model for cognitive robotics application that can aid *local* speech-to-text recognition.
  - Our optimised language models performed invariably better than the existing state-of-art statistical language models.

- **CNeRG - Complex Networks Research Lab** - *Research Assistant* May 2019 – Aug 2019
  Advisor: Prof. Sandip Chakraborty, Indian Institute of Technology, Kharagpur
  - Design and validated an algorithm for the characterization of workload in Multi-tier Cloud Infrastructure. The work focused on considering the dynamics of multiple servers and multiple users-compared to the single-server approaches.
  - Modeled the influence among servers with the help of Gaussian Mixture Model (GMM), Mixture Density Network (MDN) and Bayesian Belief Network (BBN). In addition to workload characterization, the algorithm was also able to detect malicious users.

[1] As of December 2021

Independent Projects

- **Secure all-to-all data sharing** July 2021 – Dec 2021
  - Developed an end-to-end secure version of the concurrent transmission-based synchronous protocol that allows each party to communicate with each other party in low-power wireless networks.
  - Analysed the performance of designed protocol in physical testbeds available at ETH Zurich and TU Graz.
- **Privacy Preserving Secure Inference** July 2020 – Feb 2021
  - Implemented the state-of-art algorithms for analyzing the performance of end-to-end secure inference tasks in healthcare related machine learning models.
  - Additionally, modified these algorithms incorporating Zero-Knowledge Proofs to achieve partial robustness against malicious adversaries.
  - Tested in 2PC setting using CryptFlow, MOTION, SCALE-MAMBA, and MP-SPDZ frameworks.
- **Blockchain based Network Slice Auctioning in 5G** Jan 2020 – Apr 2020
  - Developed a Hall's matching based auctioning mechanism for network slice auctioning among Mobile Virtual Network Operators (MVNOs).
  - Validated the devised algorithm using Hyperledger-Fabric Blockchain platform.
- **Novel Hybrid Encryption of Digital Image** Oct 2019 – Dec 2019
  - Developed a hybrid encryption algorithm using Arnold's transformation and Decisional Diffie-Hellman (DDH) assumption.
  - Evaluated the robustness performance of the algorithm on multimedia data.

Teaching Positions

ID6L004: *Machine Learning and Data Analytics*: Teaching Assistant Autumn 2021
CS1L001: *Introduction to Programming and Data Structures* : Teaching Assistant Autumn 2021
CS1P001: *Introduction to Programming and Data Structures*: Lab Assistant Autumn 2021

Honors and Awards

- COLT 2021 LeT-All Mentorship Workshop.
- Indian Institute of Technology, Bhubaneswar **Merit-Cum-Means** (MCM) Scholarship for Undergraduate studies.
- Indian Institute of Technology, Bhubaneswar, **Department Change**: Changed the major from Metallurgy to Computer Science at the end of freshman year; **1 out of the entire batch** for CS Dual Degree Program. *iitbbs.com*
- Indian Institute of Technology, Bhubaneswar, **Department Topper** with SGPA - *9.78* in 2^{nd} semester and with SGPA- *10.0* in 8^{th} semester.
- **MHRD, Govt. of India**, Qualified for the finale of prestigious Smart India Hackathon(SIH); Member of one among the three teams from entire country.
- Inter-IIT Tech Meet, IIT Roorkee, **Secured Bronze medal** among 23 IITs by proposing a solution on psycho-graphic profiling of TV Audience.

Extra Curricular activities

- **Event Plannar**
  E-Summit-The Entrepreneurship Fest IIT Bhubaneswar
  Worked in a team to organise various events and workshops for those who have an inbuilt urge to innovate for mankind.
- **Member**
  The Fourth Wall-The Dramatics Society IIT Bhubaneswar
  Involved and acted in many plays held during various institute events.

Technical Skills

- **Programming Languages**: C, C++, Go, Python, Shell Scripting, Verilog, SQL, LaTeX, Assembly(x86)
- **Operating Systems**: Ubuntu, Kali Linux, Windows, Contiki
- **Technical Tools**: Git, Docker, MATLAB, Wireshark, Logisim, Cooja, Tensorflow, Hyperledger Fabric, ABY3, Flocklab, DCube, CrypTFlow, MOTION, SCALE-MAMBA, and MP-SPDZ.

MOOCs

Foundations of Cryptography (NPTEL), Secure Computation (NPTEL), Computational Complexity (TIFR), Computing on Encrypted Data Course (COSIC-KU Leuven), Distributed Systems (UCSC), Advanced topics in Security (UCSB), Cryptography (MIT), Machine Learning (Coursera), Probalistic Graphical Models (Coursera)