Laltu Sardar

Contact Information

Office Address:
412 C. D. Deshmukh Bhavan
Indian Statistical Institute, Kolkata
203 Barrackpore Trunk Road
Kolkata- 700108, India

Residential Address:
A14/102 Nonadanga
Sharat Malancha Abasan
Anandapur
Kolkata- 700105, India

E-mail:
laltuisical@gmail.com
laltu_r@isical.ac.in

Homepage:
http://www.isical.ac.in/∼laltu_r

Date of Birth

4th October, 1991

Research Interests

Cryptography, Security and Privacy, Encrypted Graph Analytics, Searchable Encryption

Current Affiliation

Senior Research Fellow (2016 – present)
Cryptology and Security Research Unit,
Indian Statistical Institute, Kolkata
Ph. D. Supervisor: Dr. Sushmita Ruj

Education

Master of Technology (M. Tech.) (2014 – 2016),
In Computer Science,
Indian Statistical Institute, Kolkata

Master of Science (M. Sc.) (2012 – 2014)
In Pure Mathematics,
Department of Pure Mathematics,
University of Calcutta, Kolkata, India

Bachelor of Science(B. Sc.) (2009 – 2012)
With Honours in Mathematics,
University of Calcutta, Kolkata, India

Higher Secondary (H. S.) (2007 – 2009)
West Bengal Council of Higher Secondary Education
Kasba Chittaranjan High School, Kasba, Kolkata

Secondary (2005 – 2007)
West Bengal Board of Secondary Education
Kasba Chittaranjan High School, Kasba, Kolkata

Work in Progress

Verifiable Conjunctive keyword search on Dynamic Sensitive cloud data

Abstract: Symmetric Searchable Encryption (SSE) schemes enable clients to encrypt their database while still performing queries for retrieving documents matching some keyword. Verifiable Dynamic SSE deals with the problems when the servers are malicious on dynamic database. Presently, we are studying exiting conjunctive keyword search on dynamic sensitive cloud data.

Publications

- Laltu Sardar, Sushmita Ruj, *FSPVDsse: A Forward Secure Publicly Verifiable Dynamic SSE scheme*, (Accepted in ProvSec 2019, in July 2019)

Abstract: Due to recent attacks on dynamic SSE, forward secrecy has become a crucial property it. However, the existing schemes considers the cloud service provider honest-but-curious. In this work, we present how to keep the dynamic SSE scheme secure even if the cloud server become malicious. However, we don't want to lose forward secrecy while enabling verifiability. In this work, we present challenges towards the problem of verifiability and propose generic solutions of them.

- Laltu Sardar, Sushmita Ruj, *The Secure Link Prediction Problem*, Advances in Mathematics of Communications, AIMS (Published, in June 2019)

Abstract: The link prediction problem states that given a snapshot of a graph, whether we can predict which new interactions between members are most likely to occur in the near future. In this paper we study the secure link prediction problem and use the number of neighbors for prediction. We present three efficient and practical schemes for the secure link prediction problem and prove that the schemes are secure with the real-ideal paradigm in an adaptive adversary model.

- Laltu Sardar, Binanda Sengupta, Sushmita Ruj, *An Efficient Dynamic Searchable Symmetric Encryption Scheme*, (Submitted to a Journal)

Abstract: Keyword searching is a quite challenging problem in dynamically changing set of encrypted files. In this paper, we have proposed an efficient single-keyword search algorithm in dynamically changing dataset that achieves better security guarantees and improved efficiency compared to popular similar schemes.

- Laltu Sardar, Sushmita Ruj, *Security in Unattended WSN- Confidentiality, Authenticity and Survivability*, (Submitted to a Journal)

Abstract: Here, we have proposed an efficient scheme that provides confidentiality, authenticity and survivability of sensed data. All these issues were not addressed together in any of the previous schemes for securing UWSNs and its performance is better than or comparable to existing schemes that do not enjoy all these features.

Academic Projects

- *Bitcoin Transaction Graph Analysis*
Laltu Sardar, Animesh Basak Chowdhury, Ayan Das,
Supervisor: Sushmita Ruj, Indian Statistical Institute, Kolkata

- *Application of Coding Theory in Real Life*
Supervisor: Avishek Adhikari, University of Calcutta, Kolkata

Programming Projects

- Implementation of cigarette-smoker synchronization problem, Language Used: C

- Implementation of movie rating recommendation system using collaborative filtering, Language Used: Python

- Creating a directed weighted graph API, Language Used: Python

- Computing convex hull and its area of a given set of points and detecting position of a point with respect to that convex hull, Language Used: JAVA

- Implementation of Simplex optimization Method, Language Used: C

Technical Skills

- C/C++
- Python
- Java
- R Programming
- Matlab
- HTML
- Javascript
- MySQL
- Bootstrap

Major Subjects Studied

- Advanced Cryptology
- Information Security and Assurance
- Data Mining
- Data Base Management Systems
- Information and Coding Theory
- Optimization Techniques
- Design and Analysis of Algorithms
- Mobile Computing
- Automata, Languages and Computation
- Cryptology
- Discrete Mathematics
- Data and File Structure
- Computer Networks
- Mobile Computing
- Operating Systems
- Abstract Algebra
- Linear Algebra
- Classical Number Theory

Teaching

- Teaching Assistantship (ISI Kolkata): Data and File structure Laboratory, 2017

Internship

- Summer internship to Professor Kouichi Sakurai "Sakurai Lab, Department of Informatics, Graduate School of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan", in May, 2019

Awards/ Achievements

- Qualified in best 37 in JEST-2016 in 'Computer Science'.
- Qualified GATE in 'Computer Science', 2016
- Secured 93rd position UGC-JRF for 'Mathematical Science' in December 2013
- Qualified for NBHM M.A. /M. Sc. Scholarship for 'Mathematics' (2013-2014)
- Placed 3rd position in 'West Bengal Joint Entrance for admission in Masters of Computer Applications (JECA)' 2012
- West Bengal Merit-cum-Means Scholarship for outstanding result in Madhyamik, 2007

Languages

- Bengali- Native, Mother Tongue
- English- Fluent
- Hindi- Fluent

References

Dr. Sushmita Ruj
Associate Professor
Cryptology and Security Research Unit,
Indian Statistical Institute, Kolkata
E-mail: sush@isical.ac.in

Dr. Avishek Adhikari
Professor
Department of Mathematics,
Presidency University, Kolkata
E-mail: avishek.adh@gmail.com