Laltu Sardar

Post-doctoral Research Fellow,
Institute of Advancing Intelligence,
TCG Centres for Research and Education in Science and Technology (TCG CREST), Kolkata, India

E-mail: laltu.sardar@tcgcrest.org, laltuisical@gmail.com
Homepage: https://laltu-sardar.github.io

Contact Information

Office Address:
First Floor, Tower 1, Bengal Eco Intelligent Park
IAI, TCG CREST
Block EM, Plot No 3, Sector V, Salt lake,
Kolkata- 700091, India

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

Research Interests

Searchable Encryption, Secure Cloud Computing, Data Privacy, Encrypted Graph Analytics, Security and Privacy, Blockchain.

Current Affiliation

Post-doctoral Research Fellow (2022– present)
Institute of Advancing Intelligence, TCG CREST, Kolkata, India

Education

- Doctor of Philosophy (Ph. D.) (2016 – 2021), in Computer Science,
Indian Statistical Institute, Kolkata, India
Thesis Title: Queryable Encryption for Outsourced Dynamic Data
Thesis Supervisor: Assoc. Prof. Sushmita Ruj & Prof. Bimal Kumar Roy

- Master of Technology (M. Tech.) (2014 – 2016), in Computer Science,
Indian Statistical Institute, Kolkata, India
Thesis Supervisor: Assoc. Prof. Sushmita Ruj

- 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

- Secondary (2005 – 2007)
West Bengal Board of Secondary Education

Work in Progress

[2] *Fair keyword search on encrypted dynamic database*

Abstract: In a searchable encryption scheme, when the server becomes malicious, it can send incorrect results. So, the client needs to verify the result. However, the cloud may not trust the client as it can incorrectly claim of getting the wrong result. In one of our previous works, we presented an efficient solution for static database. In this work, we are trying to find an efficient solution to provide dynamic SSE scheme with keyword-search functionality, that is verifiable by both parties, in such a way that no one can cheat other parties. We may use blockchain-based smart contracts for fair payment to ensure trust in each other.

[1] *Deletion on dynamic searchable encryption*

Abstract: The updates in existing dynamic searchable encryption (DSE) schemes deal only with a single keyword-document pair. However, in practice when we delete a file we delete it as a whole not a single keyword from that file. Assuming this we can find that existing schemes are vulnerable to real search scenarios. In this work, we are trying to conduct an extensive study on deletion in DSE. We first give some attacks, then we will find some possible fixes for them. Our scheme will include experimental analysis with real-life data as well.

Publications

[5] **Laltu Sardar**, Subhra Majumder, *Fidelis: Verifiable Keyword Search with No Trust Assumption*, In Proceedings of the 20th International Conference on Security and Cryptography (SeCRYPT 2023), ISBN 978-989-758-666-8, ISSN 2184-7711, pages 698-703. DOI:10.5220/0012082700003555

[4] **Laltu Sardar**, Binanda Sengupta, Sushmita Ruj, *Efficient keyword search on encrypted dynamic cloud data*, Advances in Mathematics of Communications, AIMS, 2022. (Published)

Prototype repository (Language used– C):
https://www.dropbox.com/sh/7i0jjcnb5ysolex/AACD3lKO1sNDopzoyorPx59La?dl=0.

[3] **Laltu Sardar**, Gaurav Bansal, Sushmita Ruj, Kouichi Sakurai, *"Securely Computing Clustering Coefficient for Outsourced Dynamic Encrypted Graph Data"*, In *13th International Conference on COMmunication Systems & NETworkS, (COMSNETS 2021), Bangalore, India, January 5-9, 2021*, IEEE, pages 465–473. 2021.

Prototype repository (Language used– C++):
https://www.dropbox.com/sh/pzyakffcq75zlxb/AAAW5jGtl23HlF384Qz-BWBxa?dl=0.

[2] **Laltu Sardar**, Sushmita Ruj, *"FSPVDsse: A forward secure publicly verifiable dynamic SSE scheme"*, In *Provable Security - 13th International Conference, (ProvSec 2019), Cairns, QLD, Australia, October 1-4, 2019, Proceedings*, LNCS, volume 11821, pages 355–371, 2019.

[1] **Laltu Sardar**, Sushmita Ruj, *"The Secure Link Prediction Problem"*, Advances in Mathematics of Communications, AIMS, volume 13(4): pages 733–757, 2019.

Prototype repository (Language used– C and Python):
https://www.dropbox.com/sh/y2obrkefvbrqt05/AAA-nzr1tmK8uJPfVWtXxJFba?dl=0.

[0] **Laltu Sardar**, Sushmita Ruj, *Security in Unattended WSN- Confidentiality, Authenticity and Survivability*, DSPACE, Institutional Repository, Indian Statistical Institute, Series: Dissertation;16-339, 2016

Prototype repository (Language used: Python):
https://github.com/sardarlaltu/UnattendedWSN.git

Manuscripts

[2] **Laltu Sardar**, *Fake me if you can: Unforgeable digital certificate with instant verifiability*,

Abstract: Here, we address the problem of certificate forgery impacting illegal immigration and job markets. It introduces FastVer, a secure certificate verification scheme, aiming to provide instant and cost-free verification globally. The system is designed to integrate seamlessly, preventing the submission of counterfeit certificates. Experimental results show it is fast, scalable, and efficient, with verification completed within seconds.

[1] **Laltu Sardar**, Sushmita Ruj *DIA Tree and its application to conjunctive and verifiable Searchable Encryption scheme with forward privacy*,

Abstract: Here, we design a forward private DSE scheme that supports conjunctive keyword search. At the heart of the construction is our proposed data structure called dynamic interval accumulation tree (DIA tree). It is an accumulator based authentication tree that efficiently returns both membership and non-membership proofs. Using the DIA tree, we can convert any single keyword forward private DSE scheme to a verifiable forward private DSE scheme that can support conjunctive query as well. We have shown the efficiency of our design by comparing it with existing conjunctive DSE schemes.

[3] Bibhas Chandra Das, Nilanjan Datta, Avijit Dutta, Avishek Majumder, **Laltu Sardar**, *ODXT+: An Efficient Dynamic SSE Scheme for Conjunctive Queries*

Abstract: Here, we propose a new dynamic SSE scheme for conjunctive queries based on the OXT framework, dubbed ODXT+, which achieves forward privacy and C2 backward privacy. ODXT+ can be seen as an improved version of ODXT that resolves the correctness and forward privacy issues. To the best of our knowledge, it is the most efficient forward and backward private DSSE construction for conjunctive queries with low client-side computation and communication overhead.

Reviewing

Regular reviewer of the followings.

- IEEE Transactions on Dependable and Secure Computing (**TDSC**)
- IEEE Transactions on Information Forensics and Security (**TIFS**)
- Journal of Information Security and Applications (**JISA**)
- Australasian Conference on Information Security and Privacy (**ACISP**)
- International Conference on Cryptology in India (**INDOCRYPT**)

Technical Skills

- C/C++
- Solidity
- Python
- SageMath
- Matlab
-

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

1. Introduction to Programming and Data Structures, 2024-25, Sem-I
   – Offered for: Ph.D. students in Computer Science at IAI, TCG Crest, India
2. Design and Analysis of Algorithms, 2023-24, Sem-II
   – Offered for: Ph.D. students in Computer Science at IAI, TCG Crest, India
3. Introduction to Programming and Data Structures, 2023-24, Sem-I
   – Offered for: Ph.D. students in Computer Science at IAI, TCG Crest, India
4. Introduction to Programming and Data Structures, 2022-23, Sem-II
   – Offered for: Ph.D. students in Computer Science at IAI, TCG Crest, India
5. Design and Analysis of Combinatorial Algorithms, 2022-23, Sem-II
   – Offered for: Ph.D. students in Computer Science at IAI, TCG Crest, India
6. Introduction to Programming and Data Structures, 2022-23, Sem-I
   – Offered for: Ph.D. students in Computer Science at IAI, TCG Crest, India
7. Data and File structure Laboratory, 2017 (Teaching Assistantship)
   Offered to: M.Tech. students in Computer Science at ISI, Kolkata, India

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
- 93rd position **UGC-NET-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 Secondary, 2007

Languages

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

References

1. Dr. Sushmita Ruj
   Associate Professor
   School of Computer Science and Engineering
   University of New South Wales, Sydney
   E-mail: sushmita.ruj@unsw.edu.au

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

2. Prof. Bimal Kumar Roy
   Professor
   Applied Statistics Unit,
   Indian Statistical Institute, Kolkata
   E-mail: bimal@isical.ac.in