Praveensankar Manimaran

PhD Research Fellow

- ➤ praveema@ifi.uio.no
- Oslo, Norway
- github.com/praveensankar/
- +4796741397
- https://praveen.xyz/
- in linkedin.com/in/praveen000/



Bio

Praveensankar Manimaran is a PhD Research Fellow at the University of Oslo, Norway working on privacy issues in the revocation and verification of VCs. Praveen's PhD gave him expertise in identifying and solving non-trivial research problems that have direct impact on the industry use cases. In addition, Praveen's PhD gave him 4 years of experience in project management, dealing with planning, coordinating and communicating tasks effectively among team members, and time management.

Education

Ph.D. - Informatics, University of Oslo

- Research in Verifiable Credentials and Blockchain Technologies
- Identified novel and non-trivial privacy problems in VCs's revocation and verification, and developed novel solutions using techniques such as Merkle Tree Accumulators, BBS Signatures, and Zero-Knowledge Proofs.
- Implemented prototypes to showcase the practicality of the solutions.
- Published research papers in top venues.
- Worked as a Teaching Assistant for the following courses: IN5020-Distributed Systems (2022, 2023), IN5420-Distributed Blockchain Technologies (2022, 2023)
- Installed and maintained Norway's EBSI pilot node
- Supervisors: Roman Vitenberg, Leander Jehl
- Collaborators: Thiago Garrett, Mayank Raikwar, Arlindo F. Conceição

M.Tech. - Computer Science and Engineering,

National Institute of Technology Puducherry

• CGPA: 9.82, Gold Medalist

Karaikal, India

B.E. - Computer Science and Engineering, PSG College of Technology

2012 Jul - 2016 May

2018 Jul - 2020 Jun

2020 Oct - 2024 Oct

Oslo, Norway

Publications

Prevoke: Privacy-Preserving Configurable Method for Revoking Verifiable

Credentials, 2024 IEEE International Conference on Blockchain (Blockchain).

- Prevoke presents privacy issues in revoking VCs and presents a solution based on Bloom Filters, Merkle Tree Accumulators, and Smart Contracts.
- Prevoke also proposes a novel two-phase verification technique to optimize the efficiency of VCs' verification. Most of the valid VCs would go through efficient and fast verification. Only revoked VCs and a handful of valid VCs would go through expensive verification.

2024 Oct

praveema@ifi.uio.no 1/2

Identity Management Systems, ACM Computing Surveys (Under Review)

- Provides a generic model to analyse the architecture of IMSs
- Using the generic model, analyze a) IOTA Id, b) Indy, and c) eIDAS.
- Discusses the differences between these IMSs using a novel taxonomy

Addressing traceability of revocation status of Verifiable Credentials,

(Work in Progress)

• Utilises Zero-Knowlege Proofs to address traceability problem

Projects

Prevoke, Proof of Concept implementation □

- This POC implements Prevoke, a technique to address privacy issues in revoking and verifying VCs.
- **Components**: 1) Issuer, 2) Holder, 3) Verifier, 4) Smart Contract, 5) Golang and Smart Contract interactions, and 6) mock VC data model based on W3C Specifications.
- Workflows: 1) issuance, 2) revocation, 3) VP construction and sharing, and 4) VP verification
- Languages: Golang, Solidity

Professional Experience

Software Engineer, Accolite Software India Pvt Ltd ♂

2016 Jul - 2017 Mar

• Worked on web development using technologies associated with .NET frameworks and angularjs.

| Skills | | | |
|------------------------|-----------|--------------------|-----------|
| Verifiable Credentials | • • • • | Blockchain | • • • • |
| Research | • • • • | Golang | • • • • • |
| Privacy | • • • • • | Project Management | • • • • |

References

Dr. Roman Vitenberg, *Professor*, University of Oslo, Norway romanvi@ifi.uio.no

Dr. Leander Nikolaus Jehl, Associate Professor, University of Stavanger, Norway leander.jehl@uis.no

Dr. Thiago Garrett, Postdoctoral Fellow, University of Oslo, Norway thiagoga@ifi.uio.no

Dr. Mayank Raikwar, Postdoctoral Fellow, University of Oslo, Norway mayankr@ifi.uio.no

praveema@ifi.uio.no 2 / 2