Venkkatesh Sekar

Date of Birth	14^{th} February 1997	**Home Phone**	+44 7935168549
Nationality	Indian	**Email**	venkkatesh.sekar@gmail.com
Website	vsekar.me	**LinkedIn**	linkedin.com/in/venkkateshsekar

Education

2014-2018 B.Tech in Computer Science & Engineering - National Institute of Technology, Tiruchirappalli

First Class with Distinction - 8.5/10 CGPA

2012-2014 Class XII (Senior Secondary Examination), CBSE - Shrishti Vidyashram

First Class with Distinction - 95% Aggregate
Awarded Overall 3rd place at District Level.

Research/Work Experience

Oct 2019 - Present University of Surrey, United Kingdom
Researcher in Security

- Part of the **ASTRID (Addressing Threats in Virtualized Devices)** team, an EU funded platform for the secure development and deployment of micro-services in emerging software-defined and virtualized infrastructure.
- Developed a **vulnerability assessment framework** to vet cloud applications for secure orchestration. This is executed by building a **hybrid fuzzing and concolic execution model** coupled with **control flow attestation** to discover bugs in pre-deployment and run-time phase.

Jun 2018 - Aug 2019 Oracle India Pvt. Ltd.
Applications Developer

- Part of **Oracle's Human Capital Management (HCM)** software development team.
- Developed an **automated I 9 Employment Verification System**, Faceted Search, Calendar Export functionality and Hash-based user privilege application for the application.

May 2017 - Aug 2017 University of Surrey, United Kingdom
Cyber Security Research Intern

- Developed a **distributed password authenticated searchable encryption** scheme which allows data to be outsourced and retrieved using encrypted keywords without compromising the confidentiality of the data and the security parameters.
- The work was mainly motivated to provide a device agnostic system as the previous approaches stored high entropy keys on the device making them device specific.
- The demonstrator was built using the **NISTP384 Elliptic Curve group for Public Key Infrastructure**, PBKDF2 for key derivation, HMAC for message authentication code and **Stanford Javascript Crypto Library (SJCL)** for implementing the protocol.

Dec 2016 - Aug 2019 Exelerating B.V, Netherlands
Lead Developer and Advisor

- Developed **Pension Funds Network Graphs**, a product that helps clients obtain smarter insights in the data that Exelerating gathers. It's a dynamic map that shows how all relevant players in the Dutch pension sector (companies, fiduciary managers, pension funds, consultants) are connected to one another. The tool gives unique insights of the data and is now broadly used in the sector.
- Currently advising Exelerating on various IT projects where deeper knowledge about programming is needed.

Nov 2016 - Nov 2017 Mozilla Winter of Security
Developer

Developed the fast hash algorithm **BLAKE2** and it's key derivation counterpart **ARGON2** for **Network Security Services (NSS)**, a set of libraries designed to support cross-platform development of security-enabled client and server applications.

July 2015 - May 2018 Festember
Head, Web Operations

- Responsible for building and maintaining the entire computing infrastructure that powers Festember (Int'l Cultural Festival).
- Complete API for web and mobile platform. Included Admin Panel for monitoring of participants, event statistics and sales of tickets.
- Recorded an unprecedented number of site hits (over 300,000) and app downloads (over 6000). Used by more than 13,000 students from various colleges

Nov 2015 - Dec 2015 Dipper Technologies
Software Development Intern
Developed a truck navigation system with real-time pit stops and route optimization to minimize operational cost for freight trucks.

Projects

Jan 2018 - May 2018 Land Records on Blockchain
Cryptography, Blockchain, Python, Flask
A Proof of Work and Proof of Stake based hybrid blockchain web application designed to facilitate a secure Land Records system

Nov 2015 - Dec 2015 PAKS
Cryptography, NodeJS, SJCL
Secure Multi-Server Web application to distribute and retrieve files based on encrypted keywords. The proposed framework is currently being extended for encrypted files.

July 2016 Voice Tutor
NodeJS, Google Cloud Services, Exotel API
Call based automated tutor capable of delivering audio lessons, progress tracking and clarifying doubts . Provides support for English and Hindi.

Dec 2015 Blockhash
Python, Mutli-threading
Multi-threaded SHA2 for large files optimizing the speed by over 50% and has been downloaded over 3000 times. Support to SHA3 was later added at github.com/Spockuto/sha3-parallel.

Publications

Sep 2019 Password-Authenticated Searchable Encryption
Liqun Chen, Kaibin Huang, Mark Manulis, and Venkkatesh Sekar. 2019.
To be submitted in IJIS- PDF

Awards

Runner Up InOut, India's largest student based Hackathon, NIT Surat, 2016
Finalist Capture the Flag, Microsoft Build the Shield, 2016 - **1000+ teams**
Top 200 Google Capture the Flag, 2016 - **3000+ teams**
1st Mathematical Quiz, State Level, VIT, 2014
4th 6th National Interactive Maths Olympiad, 2011