

# Venkkatesh Sekar

vsekar.me | venkkatesh.sekar@gmail.com | +44 7935168549

## EDUCATION

### UNIVERSITY COLLEGE LONDON (UCL)

MSC IN INFORMATION SECURITY  
Exp. Sep 2021 | London, UK

### NIT, TRICHY (NITT)

B. TECH IN COMPUTER  
SCIENCE AND ENGINEERING  
Grad. May 2018 | Trichy, India  
Cum. GPA: 8.5 / 10

### SHRISHTI VIDYASHRAM

Grad. May 2014 | Vellore, India  
Graduating Percentage: 95%

## LINKS

GitHub:// [Spockuto](#)  
Medium:// [@venkkateshsekar](#)  
LinkedIn:// [venkkateshsekar](#)

## COURSEWORK

### POSTGRADUATE

Cryptography  
Computer Security I II  
Malware  
Cryptocurrencies  
Distributed Systems and Security

### UNDERGRADUATE

Operating System  
Network Security  
Database Management  
Compilers  
Algorithms  
Data Structures  
Artificial Intelligence

## SKILLS

### PROGRAMMING

Over 10000 lines  
• C/C++ • Python • PHP

Over 5000 lines

• Java • JavaScript

Familiar

• HTML/CSS • Shell • Node  
• Git • MySQL • MongoDB  
• Docker • TeX

## INTERESTS

Cryptographic Protocols  
Binary Analysis  
Privacy Preserving ML  
Post Quantum Algorithms

## EXPERIENCE

### UNIVERSITY OF SURREY | SECURITY RESEARCHER

Oct 2020 - Present (PT) | Oct 2019 – Sep 2020 (FT) | Guildford, United Kingdom

- Developed a real-time vulnerability detection framework for **ASTRID**, an EU funded platform for the secure orchestration of micro-services in virtualized infrastructure.
- In-depth analysis of virtualized functions through inter-working of **fuzzing**, **concolic execution** and **remote attestation** algorithms, integrated by eBPF hooks.
- Published two papers in IJIS on concurrent work in cryptography and cybersecurity as part of **Surrey Centre for Cyber Security (SCCS)**

### ORACLE | APPLICATIONS ENGINEER

June 2018 – August 2019 | Hyderabad, India

- Worked on **Oracle's HCM** enterprise software, primarily in **Java** and **Oracle ADF**.
- Designed an fully automated **I-9 Employment Verification System** for HCM using a custom XML parser and SOAP requests. Brought down workflow time by 2 weeks.
- As part of Fusion HCM Checklists team, built faceted search, calendar exporter and hash-based access control for the HCM Onboarding component.

### MOZILLA | SOFTWARE DEVELOPER

September 2016 – April 2017 | [github.com/Sachin-A/Blake2](#)

- Implemented **BLAKE2 & ARGON2** from scratch, a set of **fast hashing** libraries in **C** for **Network Security Services (NSS)** as part of **Mozilla's Winter of Security**

## PROJECTS

### PASE June 2017 - July 2017 | [github.com/Spockuto/surrey-paks](#) | **NodeJS**

- Encrypted file storage web application** to store, search and retrieve encrypted files based on encrypted keywords or tags.
- Authentication of users occur using high entropy keys derived from passwords using a custom two-server based secret-sharing cryptographic protocol.
- SJCL** and **WebCrypto API** was used to implement the underlying cryptographic infrastructure and achieve native encryption speeds in JavaScript

### VOICE-TUTOR July 2016 | [github.com/thakkarparth007/voice\\_tutor](#) | **JS**

- Multilingual Call based automated tutor** capable of delivering **audio lessons**, **progress tracking** and **clarifying doubts**.
- Built using **Google Cloud Services** for real-time translation, **Exotel API** for call routing and **Wolfram Alpha** for custom queries.

### BLOCKHASH Dec 2015 | [pypi.python.org/pypi/blockhash](#) | **Python**

- Parallelized SHA2** for large files using multi-threading and custom Merkle trees.
- Achieved **50%** performance boost and **3000** package downloads.
- Support for **SHA3** was added later at [github.com/Spockuto/sha3-parallel](#).

## AWARDS

2016	2 <sup>nd</sup>	<b>InOut</b> , India's largest student based Hackathon, NIT Surat.
2016	Finalist	Capture the Flag, <b>Microsoft Build the Shield</b>
2016	Top 200	<b>Google Capture the Flag</b> worldwide
2014	1 <sup>st</sup>	Mathematical Quiz, State Level, <b>VIT</b>
2006	1 <sup>st</sup>	Japanese Soroban Mental Maths National Competition

## PUBLICATIONS

- Manulis, M., C. P. Bridges, R. Harrison, V. Sekar, and A. Davis. "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges." International Journal of Information Security (2020): 1-25. **DOI**
- Chen, L., K. Huang, M. Manulis and V. Sekar. "Password-Authenticated Searchable Encryption." International Journal of Information Security (Accepted). **Preprint**