

Statement of Purpose

A sense of security is often considered to be the driving force which governs most of our decisions. Coming from a middle-class family, this value of safety and security is deeply inculcated into my being and subconsciously guides my moves. When presented with this opportunity to contribute my limited understanding of the subject in making a more secure transmission, I was motivated enough to apply to this program. According to my understanding, this program deals with cryptography and blockchains to provide a secured distributed ledger technology similar to the popular cryptocurrencies like bitcoin. I have a bachelor's degree in Computer Science Engineering and I think that it is one of the best fits for pursuing research towards the addressed problem and help in finding a solution. I have the subject knowledge of cryptography, computer networking and others which are like stepping stones towards having an understanding of the subject.

The basic inspiration behind my opting this particular field will be my interest in the huge amount of research that I would be exposed to while finding my way out of various tricky problems. According to statistics, the attempts to breach servers or steal digitally stored data have increased almost exponentially. This has in turn caused major problems; for instance, in the year 2021, the average damage caused by data breaching has exceeded the amount USD 3.86 million and reached USD 4.24 million. Such heavy expenses are likely to expose the loopholes of a seemingly tech-safe country. Moreover, after the worldwide attack of the Covid-19 pandemic, the usage of internet and web-based services has increased manifolds and such technical glitches prove immensely detracting in the smooth progression of a nation. Keeping in mind the recent scenario of the breaking out of dispute among countries, it is hardly

necessary to state the ill effects of data loss or data breach to the future of a given country.

These instances have motivated me towards the prospects of the concerned project.

I aspire to pursue my research in the domain of cryptography and secure multi-party computation (MPC). With the advancement of technology in this digital age, issues like security vulnerability pose a huge threat. One way to curb those problems is to incorporate cryptography in the design of those systems, making it possible to formally argue about security guarantees. However, building such cryptographic protocols for complex systems turns out to be a non-trivial task. In fact, in many scenarios it is not even possible to achieve certain security guarantees using traditional cryptographic techniques. I have always been enticed by the concept of impossibilities and taken an unimagined pleasure at negating such views employing the sheer hard work and motivation of an individual. Since the aim of the project is to target such ‘impossible missions’, I think I fit perfectly under the requirements. My knowledge about the blockchain and cryptography will be extremely beneficial if provided with the chance to explore and research them further.

My abilities to cooperate with my colleagues and coordinate my skills with the attributes of others is necessarily portrayed through my being an active member of the Computer Society of India (CSI). In the past I have also been a part of an organized group known as The Bharat Scouts and Guides which is the proof of my leadership and organizational skills.

Through this project I hope to get enough exposure towards this usage of cryptography and blockchain which will prepare me to handle more such complex issues. In future I see myself as a research scholar who works towards answering the numerous questions yet unanswered in the fields of technology and use my knowledge in providing mankind with better and greatly

improved technology which will be free of any discrepancies. Lastly, I would like to present myself as an aspiring candidate for this program since I am truly convinced that the academic knowledge that I will acquire here will increase opportunities for me and I shall be honoured if I am considered for admission in the PhD program at your prestigious institution.