STATEMENT OF OBJECTIVE

(2 pages for Statement and 1 page for References)

Shailesh Mishra (shailesh.mishra0511@gmail.com) PhD Applicant, EDIC, EPFL

1 Motivation

Recently, cryptocurrencies have seen wide adoption because of blockchain[1, 2], its underlying technology, and blockchain's unique features - *decentralization*, *immutability*, *auditability* and *anonymity*. These features make systems scalable, secure and privacy-preserving. Despite their success in cryptocurrencies, conventional blockchains haven't received the similar level of adoption in other computing systems due to a few roadblocks. Conventional blockchains require verification of transactions by all nodes for transaction validation and a resource-intensive algorithm for reaching consensus. These factors increase overheads and latency in blockchains which can adversely affect a network. Adversaries have used anonymity and absence of a central entity in blockchains to execute Sybil attacks. With the number of computing devices and amount of privacy-sensitive data growing at a tremendous rate, the above-mentioned unique features of blockchain can prove to be the panacea for handling and safeguarding large systems. This makes resolution of the above-mentioned issues in blockchain a compelling research direction. **Therefore, during my PhD, I wish to build systems and algorithms to improve the scalability and security of blockchains so that blockchain can be integrated with existing frameworks.** I hope to achieve this goal at the doctoral program of EDIC, EPFL by *designing better consensus algorithms*, *developing packet-optimized architectures* and *connecting real-world identities with digital identities*, without compromising security and privacy of systems. With the experience gained from EPFL, I aspire to become a professor.

2 Research

My first experience with blockchain was during my first research internship where I **developed the prototype of a decentralized marketplace based on blockchain and IPFS**. During this internship, I studied the security and privacy issues in the web and tried to address them in this prototype by incorporating features of blockchain. After realizing the benefits of blockchain, I wanted to use blockchain for improving the performance of systems. Therefore, next, I **designed a decentralized framework based on blockchain and IPFS to monitor voltage for fault and theft detection**[3]. We had worked on a client-server based voltage monitoring system. After identifying the scalability and security issues that can arise with the increase in sensors and the centralization of data, we decentralized the model and enhanced the security by integrating blockchain and IPFS. After this work, I realized that blockchain can help extenuate privacy and security issues in systems. At the same time, I also understood that there are significant roadblocks that prevent the adoption of blockchains. Henceforth, I have worked towards understanding and solving: (i) scalability issues in blockchain; (ii) security issues that can be solved using decentralization; (iii) usability issues in blockchain; and (iv) privacy issues in web.

2.1 Blockchain Scalability

I have been working with **Prof. Raja Jurdak** for more than two years, where I have been primarily involved in projects related to integration of IoT and blockchain.

1) BlockTorrent: I worked on **BlockTorrent**[4], where we integrated BitTorrent algorithms (which includes splitting, distributing and regenerating of files) with blockchain to create a privacy-preserving framework for solving the issue of information sharing between industries without involving a third party. I learnt the idea of using an overlay to prevent a blockchain network from getting bloated in frameworks that generate data at an extremely quick rate. By going through related works while working on BlockTorrent, I learnt more about the issues that prevent integration of blockchain with IoT and I was interested in working towards solving them.

2) Vericom: The first issue that we solved was reducing the large overheads introduced by the requirement of verification of transactions by all nodes for transaction validation. We developed **Vericom**[5] which incorporates dedicated nodes (called backbone nodes) that relay transactions to certain nodes responsible for transaction, instead of a broadcast. I learnt about designing techniques to improve scalability of systems and handling the trade-off between scalability and security that arises when we attempt to make an algorithm lightweight.

3) Treechain: The second issue in integration of blockchain and IoT that I dealt with was consensus algorithms. Conventional blockchains use Proof-of-Work (PoW) for reaching consensus. PoW is resource intensive and induces huge latency. We designed **Treechain**, a non-deterministic lightweight consensus algorithm, which selected validators (equivalent to miners in PoW) using only public-keys of the nodes. I acquired the concept of distribution of computation burden among nodes to improve efficiency and devising methods to prevent energy wastage.

4) Improving Vericom and Treechain: I am developing a light-weight blockchain, aiming to perform better than Vericom and Treechain. Vericom and Treechain had a certain degree of centralization due to the inclusion of backbone nodes and Certificate Authorities (CAs) respectively. **This framework incorporates trust between devices for verification of transactions and reaching consensus in a completely decentralized manner.**

5) Blockchain-based DVPP: I am also working on developing a blockchain-based dynamic virtual power plant (DVPP) network for improving data privacy and trust in smart grids. **I am attempting to design the framework in a way that there is no dependency on CAs without compromising the defence against Sybil attacks.**

2.2 Security

1) Distributed IDS: I started collaborating with **Prof. Sathya Peri** after my fourth year where I have been working on **designing a blockchain-based intrusion detection system (IDS) for IoT networks**. The standard

architecture of IDS involves a single central entity monitoring network traffic for the detection of malicious activity. This architecture is unscalable and vulnerable to single point of failure. Thus, we designed a blockchain-based IDS to improve the scalability of IDS and reach better decisions via collaboration.
2) Distributed Image Reconstruction: In my master's thesis, **I am designing a distributed framework for reconstructing accurate images in CyberPhysical systems (CPSs), even in the case of adversarial activities**. Like classical IoT networks, the CPSs that process images, have a centralized architecture and are vulnerable to attacks. Images carry essential privacy-sensitive information, which if tampered with, can prove to be detrimental to various processes. Therefore, I am designing a distributed framework for image reconstruction that mitigates the effects of False Data Injection and Denial-of-Service attacks, and improves privacy of data by data-splitting.

2.3 Blockchain usability

During the internship where I had developed a decentralized marketplace, I had to write multiple smart contracts. I faced numerous issues while writing them due to lack of documentation and regularly-changing syntax. Therefore, I wanted to build a framework to enhance writing of smart contracts. Thus, I started collaborating with **Prof. Mohammad Hamdaqa**. We developed a **chatbot**[6] **that helps users to generate smart contracts with no prior knowledge**. I learnt the application of Model Driven Engineering for textual modelling to generate codes. I included Levenshtein's edit distance and DialogFlow intent recognition for improving robustness of the chatbot. I designed a comprehensive survey to understand possible improvements in the chatbot (specifically in the intent detection and reduction in efforts from the users'end) which we will be pursuing in the future.

2.4 Privacy issues in web

After working on the decentralized marketplace, I was eager to learn the gravity of privacy issues in web to understand the impact of the solution. Hence, I took the courses - *Social Computing* and *Usable Security and Privacy*, where I learnt about the scenarios of privacy leakage in social media and the methods used in analyzing privacy concerns. Since my previous work was on a marketplace, I was interested in studying the issue of privacy leakage in e-commerce. Firstly, we studied the cases of and reasons behind leakage of personally identifiable information (PII) in Amazon reviews. Since the results were not satisfactory, we are working on **designing and analyzing cross-platform reidentification attack from e-commerce reviews, and redefining a better PSI detection strategy.**
All the above-mentioned projects have enhanced my skills in various domains of systems and security. The feeling of jubilation after achieving research goals and the urge to gain more knowledge has solidified my desire to pursue a PhD.

3 Conclusion

To summarize my research interests and goals, *I would like to work on building systems for increasing the throughput, reducing the overheads and improving the security of the blockchain-based IoT networks.*
About me and why I am a good fit for the programme?: Hailing from a small town in Odisha, India, I have faced multiple ideological, social and technological issues while pursuing research as my career. Nonetheless, **by virtue of resilience and patience**, I have been able to overcome all the barriers and always tried to become a better researcher. I have also often found myself on the receiving end of some harsh setbacks. However, with time, I have grown to **understand the significance of these setbacks**. For instance, when I explored research for the first time, I spent a lot of time for getting a grasp of research papers. I was not able to devote ample time to academics and thus, my performance in fifth semester wasn't good enough. At first, I was dejected but eventually, this process proved to be fruitful. From there on, I have managed research and academics efficiently, and maintained my GPA on the higher side and worked on multiple research projects simultaneously. This experience always helps me reconcile myself everytime a paper gets rejected and work towards improving it from the reviews received. In addition, by working with various teams from different locations, I have realized the value of **teamwork** and learnt to work in a collaborative environment, where people push each other to their limits while amplifying the total output instead of mere addition. These traits have greatly enhanced my ability to conduct research.
Why EDIC?: EPFL, with its stronghold in systems and security, would provide me with the perfect opportunity to achieve my ultimate research goal. Alignment of my research interests with that of the interests of the professors at EDIC, EPFL, makes EDIC the perfect platform for my growth as a doctoral student.

Prof. Bryan Ford has multiple publications in the field of blockchain and security. His work on **Protean**[7] puts forth the ideas of *workflows* and *functional units*, which can enhance the performance of decentralized applications. One interesting scenario for which I would like to design defense mechanism is when the *functional units* act maliciously. One possible solution is by assigning tasks to two past functional units and two future functional units for monitoring.

Prof. Rachid Guerraoui has numerous publications in the field of blockchain and distributed computing. For instance, his recent work on **consensus number**[8] provides a shared memory model and the studies the asset transfer problem in shared memory. Another intriguing part of the work is how the results of shared memory have been translated to message passing.

I would like to work on similar research works during my PhD where I aim to build more efficient and secure systems. My research background in **blockchain**, **distributed systems**, **security** and **privacy** as well as the **technical skills, that I have acquired by working on research projects**, make me a strong candidate for pursuing a PhD at EDIC EPFL to build scalable, secure and privacy-preserving systems.

Thanks a lot for going through my Statement of Purpose!

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[2] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[3] S. Mishra and S. Kumar, "Smart voltage monitoring: Centralised and blockchain-based decentralised approach," in *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, pp. 49–55, 2021.

[4] A. Hill, S. Mishra, A. Dorri, V. Dedeoglu, R. Jurdak, and S. S. Kanhere, "Blocktorrent: A privacy-preserving data availability protocol for multiple stakeholder scenarios," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–3, IEEE, 2021.

[5] A. Dorri, S. Mishra, and R. Jurdak, "Vericom: A verification and communication architecture for iot-based blockchain," *arXiv preprint arXiv:2105.12279*, 2021.

[6] I. Qasse, S. Mishra, and M. Hamdaqa, "icontractbot: A chatbot for smart contracts' specification and code generation," in *2021 IEEE/ACM Third International Workshop on Bots in Software Engineering (BotSE)*, pp. 35–38, 2021.

[7] E. C. Alp, E. Kokoris-Kogias, G. Fragkouli, and B. Ford, "Rethinking general-purpose decentralized computing," in *Proceedings of the Workshop on Hot Topics in Operating Systems*, pp. 105–112, 2019.

[8] R. Guerraoui, P. Kuznetsov, M. Monti, M. Pavlovic, and D.-A. Seredinschi, "The consensus number of a cryptocurrency (extended version)," *Distributed Computing*, pp. 1–15, 2021.