

**CHENNAI – PONDICHERRY**

**SPA: A SECURE AND PRIVATE AUCTION FRAMEWORK FOR DECENTRALIZED ONLINE SOCIAL NETWORKS**

**ABSTRACT**

The security and privacy threats on e-commerce have attracted intensive attention recently. The explosive growth of online social networks (OSNs) has made them potential new great marketplaces for e-commerce, which, however, raise serious security and privacyconcerns. This is mainly due to the centralized system architecture where the service provider knows all users’ private data and becomes the single point of failure. To this end, we propose a secure and private auction framework, called SPA, for decentralized online social networks (DOSNs). SPA consists of three phases: identity initiation, buyer-seller matching, and private auction. It requires no trust among the participants but can provide security, privacy, authenticity, non-repudiation, and correctness for the auctions. We analyze the computation and communication complexities of the proposed private auction scheme, which are O(n+K) for each node where n is the number of bidders and K is the number of pricing points. In contrast, those of previous auction schemes are O(nK) at best. The storage complexity is significantly lower than before as well. Security and privacy of SPA are also analyzed. Extensive experiments are conducted to validate the efficiency of SPA.