1. **INTRODUCTION**

In the meantime, e-auctions have emerged as one of the most widely used tool to harness the true value of an item in the market. Online platforms such as [] [] are one of the popular examples in today’s time which do so. E-Auctions platforms require a seller which is willing to sell an item, an auctioneer which can be an intermediate party or may be the seller itself or the platform owner itself can play the role of auctioneer. Online auction platforms provide accessibility and hassle-free environment to conduct auctions but suffer from privacy issues, privacy issues such as privacy of losing bidder data which can be valuable for the auctioneer or seller. They can use this data to maliciously win the future auctions or make malicious incentives for them. They can know the valuation of a particular bidder and next time never sell that item to bidder lower than that price. This losing bidder’s data can also be used to set reserve prices as the losing bidders data revels valuable insights of the previous auction about a particular good.

Privacy preserving auction such as [reference] are the early examples of work done in the domain and later various application-based works have been performed in the domain of privacy-preserving. Domains such as data-trading, cloud computing use privacy-preserving auction which enables these domains to perform auction in privacy-preserving manner and maintaining trust in the auction participants. Even though various application has been developed but there are various assumptions that are considered while designing these privacy-preserving applications. Assumption such as a central authority which performs much of the computation on original data is honest[reference] or an auctioneer who can collude with the bidders and gain all the true bid values [reference] or the auctioneer and seller will never collude [reference] does not hold in real life scenarios. Various other works such as [][][][][] also lie on such assumptions. Another approach is taken to use zero knowledge proofs too hide real information but with these approaches comes a huge computation cost and works such as [][][][][] applied such approaches but cannot be applied in real life situation following computational constraints.

In this paper we present a privacy preserving auction model based on secure two-party comparison and homomorphic encryption which concludes auction in privacy preserving manner and the protocol does not require any of the participants to reveal the true bid values to the auctioneer. We also prevent the case where the auctioneer can collude with the bidders and try to reveal bids of another bidder. In this model we don’t trust blindly on any of the auction participants and no participants can gather the data of any other participants in plain format.

The contributions of our work are summarized below.

* We propose a publicly verifiable, secure two-party comparison-based privacy-preserving auction protocol, which does not require any of the bid to be disclosed to the auctioneer or other bidders.
* The proposed auction method is collusion proof to auctioneer to bidder collusion can hamper the privacy of the bid values of bidders.
* The proof for correctness and privacy aspects and simulation study of the performance analysis has been presented.

1. **LITERATURE REVIEWS**
2. **PRELIMANARIES**
3. **OUR MAIN PROTOCOL**
4. *Requirements*

Our main protocol enables bidders to submit their padded bid values to auctioneer. These bid values are generated via secure two-party comparison and encrypted via homomorphic encryption. Design of the protocol has been completed considering following requirements.

1. *Public Verifiability* It refers to the authenticity of the shared message during the auction process and declaration of the winner and in our proposed work these both things can be verified with the help of bulletin board[reference].
2. *Correctness.* The proposed protocol ensures that the highest bidder and bid are legitimate and are verifiable to each of the participant of the auction.
3. *Bid Privacy* the protocol is capable to ensure that the privacy of the bids submitted by the bidders is preserved during and after the completion of the auction.

*ADD ANY Other properties too if required*

1. *Entities involved*
2. *Auctioneer.* The auctioneer is the owner of the auction platform and an intermediatory between the seller and bidders.
3. *Certifier* It enables the auction to run by providing necessary information to the auction participants. It generates the id, key values pairs for the auction participants. Certifier is considered to make scheme work or the participants themselves can generate the information themselves.
4. *Bidders. Interested in buying sellers good they apply for the auction and take part in it.*
5. *Seller. It is the participants of the auction which is interested in selling the auctioned product at best rate possible.*