

Towards Trustworthy Procurement: A Lightweight and Secure Bidding System

Swaroop R. Manerikar¹ and Amol D. Vibhute^{2*}

¹ Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, 411016, India; swaroopmanerikar@gmail.com

² School of Cyber Security and Digital Forensics, National Forensic Sciences University, Nagpur, Maharashtra, 440022, India

* Correspondence author: amolvibhute2011@gmail.com

Abstract: A fair tendering system is essential in public administration to ensure the proper use of taxpayers' money. The sealed-bid quotation method remains preferred for minor purchases due to its simplicity. However, it has more geographical restrictions and is more vulnerable to fraud than the e-tendering system. E-tendering methods are more technology-dependent and are used for major purchases. However, both approaches require quotation submission to the procurement host. Therefore, this research proposes a lightweight and secure bidding system that requires no quotation submission at the time of participation. Quotation disclosure is required at the time of bid opening. Until the bid opening event, the quotation remains in the respective bidder's possession, and there is no risk of data leakage. Therefore, this system can be used to secure bidding in real-time.

Keywords: E-Procurement System, Sealed envelope bidding, Pre-disclosure claims, post-disclosure verification.

1 Introduction

Public procurement must be fair and safe. Governing bodies set rules for their procurement process [1]. The public procurement system not only prevents direct purchase-related malpractices but also enables organizations to access a broader pool of suppliers and obtain competitive prices. In addition, malpractices are also possible in direct purchase due to collusion between the supplier and the procurer. The graph presented by the researcher [2] shows that the bidding process benefits the procurer by securing the desired goods and services at a price below the market price. Purchasing by sealed quotation involves submitting the bid while maintaining its confidentiality [3].

Several studies focused on bidding systems with some limits. For instance, the study provided insights about auction types and various bidding strategies [4]. The research explained the advantages of Vickery auctions [5]. This auction benefits both the bidder and the auctioneer. The highest bidder must be declared a winner, but he offered the second-highest bid. In a reverse auction, suppliers get a lower price [4].

1.1 Problems with Sealed Bid Offline

The major problems associated with purchasing sealed quotations are security, privacy, and potential collusion. These challenges can undermine the integrity of the bidding process and affect the outcomes for all participants. Wei & Dang provided limitations on the offline bidding or sealed quotation method [6]. A sealed quotation method requires a trusted third party. However, this approach has limitations of space and time. Moreover, staff involvement might lead to the disclosure of the bidder's identity.

In the sealed-bid method, submitted bids are submitted in sealed envelopes to the procurer. In this case, the submitted bids could remain under the procurer's protection. The sealed bids must be opened in the presence of the bidders or their representatives on the day of opening. Moreover, a comparison chart must be prepared for convenience and to determine the winner. Possible collusion or coercion might lead one bidder to obtain information about other bidders and engage in unfair practices to win the bid. However, conveying useful information to other bidders is a fraud [7]. The scammer may submit multiple bids and decide which bid to open based on previously opened bids. These challenges can harm the integrity of the bidding process and affect the outcomes for all participants. It also creates

a trust issue in the system, leading vendors to show less interest in participating. Similarly, coercion causes bid rigging [8]. Thus, the sealed bidding is always vulnerable to malpractices such as illegal acquisition and manipulation. Hence, the bidding process needs to be digitalized [6].

1.2 Introduction to the E-Procurement System

E-auctions are introduced and adopted to address the problems in bidding systems. E-tendering in public procurement represents a significant shift towards transparency, efficiency, and accessibility. By leveraging technology, e-tendering enhances the traditional tendering system, ensuring fair competition and reducing opportunities for corruption [9]. It also introduces convenience and reduces the cost through healthy competition. It provides a bigger pool of bidders.

The authors discussed types of e-procurement systems [10]. In a principle-based system, the procurer makes the system available to bidders for registration, bid submission, and outcome checking. The procurer approaches a third-party platform to avail themselves of these facilities.

The authors in [11] wrote about the possible risks and disadvantages of a centralized system [11]. Since the centralized systems are connected to the internet, they are also prone to attacks. An unreliable or compromised third party can introduce malpractices such as bid repudiation, bid rigging, and data leakage. Since bidders cannot see each other's bids or others' submission processes, there is a risk of post-submission bid manipulation and related disputes. Many electronic sealed-bid systems are susceptible to third-party interference, in which auction hosts may conspire with bidders to manipulate outcomes [12]. Previous protocols have been found to leak sensitive bidder information, such as bank account details, compromising bidder privacy [12]. Cheating, its possibility, or fear of it creates psychological barriers for bidders [5].

In this case, E-Tendering systems are contributing to securing information and maintaining privacy. In addition, this system has increased transparency, efficiency and enhanced accessibility. E-Tendering can be customized to be more user-friendly, fair, and competitive [13, 14]. However, E-Tendering also requires robust cybersecurity measures to protect sensitive data [15]. Moreover, E-Tendering also requires technical knowledge to execute complex operations, such as online registration and obtaining a digital signature. Hence, small and non-technical companies are reluctant to participate in e-tendering.

1.3 Existing Work

Paillier (1999) proposed the use of homomorphic encryption [16]. Homomorphic encryption supports operations on data without decryption but consumes more resources. In this approach, only encrypted bids could be submitted. This approach benefits voting and other areas where privacy is essential. However, the technique is prone to 'Chosen Plaintext Attack' and 'Chosen Cyphertext Attack' where attackers select arbitrary plaintext and cyphertext to gain access [16].

The study in [17] separates the bid collection and processing activity. Bidder submits the bid in encrypted form. The auctioneer is responsible only for collecting bids. The auctioneer does not know how to process the collected bids. The auction issuer, another player in the process, uses circuit-based logic to process the bids and determine the outcome.

The research in [18] provided a universally verifiable auction protocol that hides losing bids. They published the price list or price range, along with the corresponding public key, and asked bidders to encrypt their bids with the relevant public key. However, decryption starts with the private key of the highest-priced band. If no bid opens, we can use the private key of the next bid (lower than the current price range). Once the highest bids open, opening remaining bids is optional. It hides the identity of losing bidders. However, a bidder can only choose a bid value from the list; they cannot choose a value outside the basket. This mechanism requires multiple public-private keys. Also, key leakage is possible.

The study [19] suggested that using public key infrastructure (PKI) for bidding is a secure option, but it limits participation due to the requirement for PKI [19]. Abe & Suzuki proposed using a physical booth [20]. Depositing the bid generates no receipt; hence, no tracking is possible, and there is no coercion or collusion. The bidder has no proof of the submitted bid value. Only the higher bid value remains open, and the rest remain unopened to preserve the privacy of other bidders. However, physical presence does not seem relevant and feasible in this era. It puts geographical restrictions on participation.

The author proposed a distributed calculation task, assuming that at least a few parties would be honest [21]. This method accommodates three types of players, Auction Authority (A), Seller (S) and Bidders (B) and uses homomorphic encryption. Initially, the bidders prepare their bids and encrypt them with A's public key; S collects all encrypted bids. After shuffling, they handed over to A. Since the homomorphic encryption is used, A can find the first and second winning bids. The winner can then

be awarded the second opportunity. It serves the purpose of fault tolerance and of avoiding possible collusion. The communication mechanism and scaling are complex and costly. It also requires the bidder to submit the bids.

The approach described by the authors provides verifiable bid secrecy [7]. The bidder must submit a bid in an encrypted form, and decryption can be performed in front of all players. No complex multiparty interactive protocols are used. It requires another mechanism, ‘Notary’, as a witness to the bidding process. It also requires trusted servers to prevent manipulation.

The research in [22] proposed a multi-attribute bidding system where each attribute has its own weight set during the Request for Quotation (RFQ) preparation phase [22]. A calculation is required to determine the score for each bid and the winner.

Similarly, the authors [23] proposed a new method based on the zero-knowledge proof and distributed ledger to avoid manipulation [23]. This approach provides verifiable secrecy to the submitted bid. Each party selects a seed from the pool, attaches a random key to it, and forwards it to another party. Another party repeats the same and uses the final key as a token. The bidder must deposit the token amount. The token amount will be refunded only to the honest bidders at the end of the process. The proposed mechanism uses cryptocurrencies as incentives for participants.

The study proposes an upgraded version of the binary veto system [3], in which bids are submitted as binary values. Bid opening has the highest significant bit first, then the next lowest, and so on. It protects the identity of losing bidders.

Markle’s tree-based mechanism [11] requires iterative computation and consumes more time and computational resources than hashing the entire file. The bid amount and password are both used to generate the hash.

The study proposed a method based on Pederson commitment and homomorphic encryption [24]. Data operations were performed without decryption. But submission of the bid in encrypted form is compulsory. Bid value secrecy was maintained through homomorphic encryption.

Another study proposed a different approach to generating a key [25]. The key is used to encrypt the bid. After encryption, the bid must be submitted.

The study applied a method using blockchain and Designated Verifier Ring Signatures (DVRS) [26]. Auctioneer’s public key is used to encrypt bids before submission. Bidders may participate without revealing their identities. However, a bid must be submitted.

The authors proposed a blockchain-based, contract-based solution [27] to store bitwise bid values. Bids are evaluated from the most significant bit to the least significant bit. The highest bid price is identified after comparison. More computational power is required than for non-binary bids and compulsory bid submissions.

The ring signature technology was used to help bidders hide their identity [6]. It also used PKI to maintain secrecy. Blockchain technology is used to avoid single-point failure, providing verifiable secrecy for identity but requiring bid submissions.

The latest research in this domain is more focused on blockchain usage to support transparency and scalability. Bidders can submit bids in the form of smart contracts or other forms [28–33]. However, a larger blockchain network consumes more energy. Also, the full node has to maintain a copy of the entire ledger.

1.4 Limitations of the Existing System

The key components from the literature and their limitations are given Table 1.

Table 1. Existing methodology and limitations

Sr	Existing methodology	Limitations
1	Bid submission on the distributed ledger	Requires special and extensive setup. Need reasonable number of nodes to maintain the copies of ledger [29, 30]
2	Submitting the bid in the encrypted form by using PKI	The risk with this approach is possibility of key access by the vendor [34, 35]
3	Submitting the bid in any form	Possibility of data leakage while transmission. If a host is vulnerable and compromised then adversary can access the bids.
4	Possible chip level manipulation	Possible data leakage by the hardware; difficult to detect and prevent [36, 37]

1.5 Research Objectives

- To propose a procurement system that does not require the deposition of bid information in any form during registration, but requires bid information only at the time of bid opening.
- To provide a mechanism where the host and other bidders can validate the disclosed bid information for post-registration manipulation.

1.6 Structure of this Research Paper

Section II describes the design of the proposed system and algorithms. Section III focuses on results from a simulated real-time example. The results are discussed in Section IV. Section V shows the limitations of the proposed study. The last section concluded the proposed approach and provided insights into the future work.

1.7 Innovation Metrics

Innovation Metrics is shown in Table 2.

2 Methods

This study proposed a mechanism that allows the Bidder to register for the bidding process without initially submitting the quotation document. The proposed system depends on Hashing and random number generation. Hashing consistently produces a fixed-length output independent of the input length [38]. However, hash calculations are reverse, but straightforward calculation (obtaining a preimage) is challenging. Therefore, this study used the SHA256 algorithm to generate the hash value. A hashing function takes any data (say D) as input and produces a string output, also known as the Hash (H(D)).

The proposed auction system has two types of players: Bidders (or participants) and the Procurement Host (PH). The Procurement host platform is used for interaction. When there is a requirement for goods or services, the authority concerned prepares the ‘Request for Quotation’ (RFQ) document with all requirements, terms and conditions, and publishes it on the host platform (see ‘1 RFQ Published’ in Figure 1).

Table 2. Innovation Metrics

Sr	Contribution	Novelty	Section
1	Submission less bid registration	Bidder does not have to submit the bid before bid opening day	II
2	Tamper-evident audit enable system	After getting the bid document the procurement host and other bidders can verify if the bid document is altered or genuine	II
3	Peer participation for better governance	Bidders are enabled to not only observe the process but also participate by sending queries.	II
4	No need of secure storage	Since the bid submission is required only at bid opening day. And data is open to all; there is no need to purchase and maintain online secure storage to store the bids.	II

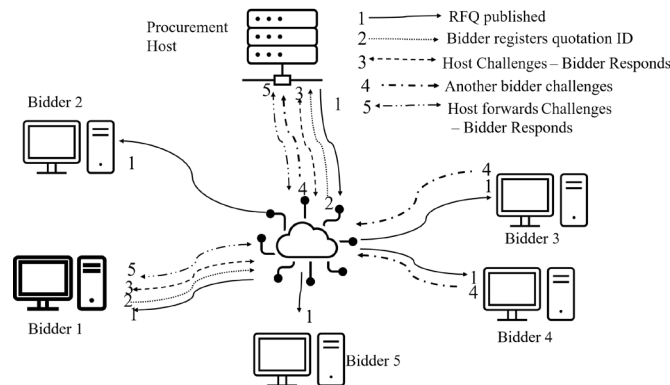


Figure 1. Layout of the proposed system

The RFQ has been kept in the public domain (see ‘1 RFQ published’ in Figure 1). Bidders who wish to participate can register on the platform. After registration, a bidder can submit a quotation and calculate its hash value. It can be considered a quotation identifier. The Bidder submits the quotation identifier to host against the published RFQ (see ‘2 Bidder Registers Quotation ID’ in Figure 1). After receiving the Quotation Identifier, the host logs it and publishes it in the open domain for transparency. The PH sends challenges to the Bidder to increase accountability. The PH specifies random fragments and asks the Bidder to send the hash of those fragments. Since the Bidder does not share the actual length of the quotation document, a fragment has to be specified in the form of a percentage, e.g. beginning at 10% and ending at 29%. Two random numbers, say A and B, can be generated where $0 \leq A < B \leq 100$ and used as relative specifications of a random fragment. This will allow the Bidder to keep the document’s length private. After receiving the challenge (A, B), the Bidder converts them into an absolute specification using the calculations (Equations (1) and (2)).

$$A_{\text{Absolute}} = A * (\text{Length of Quotation Document}) / 100 \quad (1)$$

And

$$B_{\text{Absolute}} = B * (\text{Length of Quotation Document}) / 100 \quad (2)$$

The replying Bidder fetches the exact fragment, calculates the hash, and submits the same as a reply. The host logs and publishes the response for greater transparency (see ‘3 Host challenges- Bidder Responds’ in Figure 1). The proposed bidder registration process is shown in Algorithm 1.

Algorithm 1: Bidder Registration Process

Input:

RFQ identifier $\rightarrow R_j$

Quotation Document Prepared by the Bidder $B_i \rightarrow R_j B_i$

Output:

Public logs for verification of the quotation document ($R_j B_i$)

Begin:

B_i Authenticates with the PH

B_i retrieves the RFQ information with identifier R_j .

B_i registers on the host procurement platform for participation in tendering processing.

B_i prepares the quotation document for $R_j \rightarrow R_j B_i$

B_i computes hash of the prepared document $R_j B_i \rightarrow H(R_j B_i)$

B_i registers for procurement by sharing its identity B_i , R_j , $H(R_j B_i)$ to the Procurement Host (PH)

PH generates challenges (A_c, B_c) for $H(R_j B_i)$, where $0 \leq A_c < B_c \leq 100$

B_i fetches the specified fragment of $R_j B_i \rightarrow R_j B_i[A_c, B_c]$

B_i calculates hash value for $R_j B_i[A_c, B_c] \rightarrow H(R_j B_i[A_c, B_c])$

B_i shares response to PH ($H(R_j B_i), [A_c, B_c], H(R_j B_i[A_c, B_c])$)
 $\rightarrow$ Response

PH publishes the Response in public domain

End:

The RFQ and relevant quotation ID received are available on the hosting platform, making all bidders aware of the responses to the specific RFQ. To increase transparency and the sense of participation, any bidder can challenge another bidder through the host by specifying a random segment and quotation ID (See ‘4 Another Bidder challenges’ in Figure 1). Hosts forward the challenge to the bidder. After receiving the response, the host will log it and forward it to the bidder who issued the challenge (see ‘5 Host forwards Challenges – Bidder Responds’ in Figure 1).

Algorithm 2 specifies the process to issue challenges. The concerned bidder could fetch the challenge and a response submitted to the PH for keeping in the public domain.

Algorithm 2: Bidder queries another bidder through Host

Input:

RFQ identifier $\rightarrow R_j$
Quotation Document Identifiers $\rightarrow H(R_j B_i)$
Total number of bidders participated in $R_j \rightarrow NB$
Maximum challenges allowed $\rightarrow C$

Output:

Challenge issued against $H(R_j B_i) \rightarrow [A_c, B_c]$

Begin:

Other Bidder B_o fetches ongoing procurement from the Procurement Host (PH) $\rightarrow R_j$
 B_o fetches all quotations id received against $R_j \rightarrow H(R_j B_i)$, where $0 < i \leq NB$
For each nb in NB
For each c in C
Generate A_c, B_c such that $0 \leq A_c < B_c \leq 100$
Issue challenge $[A_c, B_c]$ against $H(R_j B_{nb})$

End:

At the time of bid opening, all bidders disclose their quotation file. The proposed bid opening process is shown in Algorithm 3. The registration and challenge-response data are already available with the host. After receiving the original quotation file, the host validates it to ensure the data received has not been altered. The host then shares the same file with the remaining bidders so they can verify it as well. Only valid quotations are considered for comparison, and the content will determine the winner. If the bidder shares the altered file, the Absolute specifications will differ, resulting in a different file fragment. A distinct file fragment will generate distinct hash values, allowing tampering to be detected.

Algorithm 3: Bid Opening Process

Input:

Ongoing Procurement $\rightarrow R_j$
No of bidders participated in $R_j \rightarrow NB$
Quotation document submitted by bidders $B_i \rightarrow R_j B_i$
No of challenges received against quotation id $H(R_j B_i) \rightarrow C$
Challenges received against $H(R_j B_i) \rightarrow [A_c, B_c]$

Output:

Qualified and disqualified list of bidders

Begin:

For each B_n where $0 < n \leq NB$
PH fetches document $R_j B_n$ from B_n
PH fetches challenges and responses about $R_j B_n$
for each $[A_c, B_c]$ where $0 < c \leq C$
Calculate hash of the fragment $\rightarrow H(R_j B_n [A_c, B_c])$
If $H(R_j B_n [A_c, B_c])$ is not matching with $R(R_j B_n [A_c, B_c])$:
Disqualify the bid document and related bidder
Break and go to next bidder
Publish qualified and disqualified list of bidders

End:

For N bidders, if all are permitted to send total C_B challenges to remaining bidders, and PH is supposed to send C_{PH} challenges to each bidder, then the total number of hash operations required is given as $N \cdot C_B + N \cdot (C_{PH})$.

Threat Model

- 1) Bid manipulation by the bidder:
A bidder uses a bid document (say B) for the registration, but while disclosing the bid, it shares B' , where B and B' are not the same.
- 2) data manipulation by the host:
A procurement Host receives bid ID (say B), response (Say R), and actual bid (Say B) from the bidder. But it publishes H' , R' , B' in the responses to any enquiry. OR, despite receiving a bid ID, a response, and the actual bid, it does not acknowledge them.
- 3) Corrupt Host:
A procurement Host not acknowledging receipt of the data or propagating a falsified version of it after an enquiry.
- 4) Corrupt bidder:
A bidder that uses identical versions of data for registration and bids opening.

3 Results

We have implemented Python scripts to simulate the experiments and provided them here [39]. One script simulates the PH, and another script simulates bidders. The simulation supports 100 bidders, and each bidder has TWO copies of quotations (a genuine and an altered one). The nature of the bidders (honest, dishonest, etc.) was selected randomly. Both scripts communicate through the network socket. For ease of communication, we have created a JavaScript Object Notation (JSON) based communication protocol shown in Table 3. By using the standard messages, bidders communicated with the procurement host. In our experiment, we observed that the bidders could pull data, such as ongoing procurements, received bids for a particular procurement, and received challenges/responses for a specific bid. Also, the bidder was able to push data in PH, such as bid registration details, challenges to

Table 3. JSON based messages for communication

Sr	Message	From	To	Details
1	ONGOING_PROCURUREMENTS_RESUEST	Bidder	PH	A bidder send enquiry about ongoing procurements
2	ONGOING_PROCURUREMENTS	PH	Bidder	PH sends list of ongoing procurements
3	REGISTER_BID	Bidder	PH	The bidder is willing to participate in procurement process. Makes the bid file and submit its hash.
3	PROCUREMENT_INFO_REQUEST	Bidder	PH	A bidder requests list of bids received for the particular procurement
4	PROCUREMENT_INFO	PH	Bidder	Procurement Host shares the details
6	PUSH_RESPONSES	Bidder	PH	Bidder pushes calculated responses for each challenge
7	PULL_CHALLENGES	Bidder	PH	Bidder enquires about challenges related submitted bid.
8	CHALLENGES	PH	Bidder	Procurement host sends the list of challenges available for particular bid of the requesting bidder.
9	BID_INFO_REQUEST	Bidder	PH	A bidder requests list of bids received and related challenges and responses.
10	BID_INFO	PH	Bidder	Procurement Host sends data of all the bids received under a specified procurement along with challenges and responses
11	PUSH_CHALLENGES	Bidder	PH	A bidder issues challenges against a specific bid registered with respect to the particular procurement.
12	DISCLOSE_BID	Bidder	PH	A bidder discloses bid document. Can either share the path or submit the file

Table 4. Payload generated with 5 bidders in bytes

Sr	Message Type	Payload size
1	ONGOING_PROCUREMENTS_RESUEST	41
2	ONGOING_PROCUREMENTS	90
3	REGISTER_BID	166
4	PROCUREMENT_INFO_REQUEST	82
5	PROCUREMENT_INFO	433
6	PUSH_CHALLENGES	995
7	PULL_CHALLENGES	169
8	CHALLENGES	212
9	PUSH_RESPONSES	580
10	BID_INFO_REQUEST	74
11	BID_INFO	2396
12	DISCLOSE_BID	213
Total		5451

Table 5. Simulation outcome with 5 bidders

Sr	Bidder	Activity	Specifica- tions	Details
1	1	Registration	0–100*	d6f435b77ed2545dfa7ba496e246ea51a6c3931c3f2a813f63830209c6abd755
2	2	Registration	0–100	41487307562274ea9081df3a6b1dfefa32d49fdfa19736460e24ba8b76e3c5b0
3	3	Registration	0–100	0db5126c7488330795bd31d346b8237c9b02655f7c0942991ad2b50488cb4fac
4	4	Registration	0–100	d3c0a4807b780d43fbc240e325992b6173c8e0b1f1112ac88d258b721d821975
5	5	Registration	0–100	15cc5d4f2cb7be054a46bf0a61ec93c0d9282e8dfbfe74c04f26d02e62f75b28
6	1	Challenge & Response	22–97	a9308f146199b7ca7b2a1a1171b88e6ed445a1cbb1779fb2d561161119b57cdc
7	1	Challenge & Response	77–96	f5023e83191250752a9d49da8a2bd46656d751b42f2fc867dcabfcadd815af86
8	1	Challenge & Response	84–90	68cb6480628178c33ad4fd170c63df5cf36f547dc28dbbc5361f3f8326225877
9	1	Challenge & Response	27–93	26ec16d4bf603c147074c4e33e7862f212b9569edb617eb30c984fd47ff4eb61

* 0–100 represent hashing of the entire file.

other bidders regarding their bids, and responses to related challenges received about the bid. The PH successfully discovered various categories of the bidders.

We implemented the experiment with 5 bidders to measure the payload. The findings are shown in Table 4. The data generated at the PH is dumped into a JSON file, and its simplified tabular version is provided as an Annexure (Table 5).

4 Discussion

4.1 Hashing and Related Computational Load

An experiment was performed on the system with an Intel Core i5-12400 processor, 8 GB of RAM, and an NVMe SSD. Where a relatively large file of size 4.4 GB was considered [40]. First, we calculated the hash of the whole file (from 0% to 100%), then decreased it by 1% at each step. To demonstrate the worst-case scenario, the program always skips the first n% and calculates the hash of the remaining (100-n)%. The proposed approach took less than 4 seconds to process a 1 GB file (Figure 2).

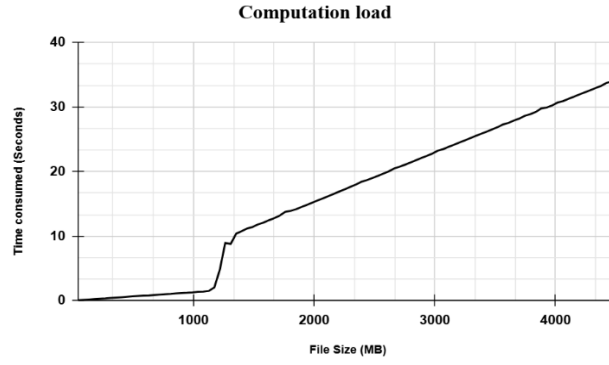


Figure 2. Size of the fragment (MB) vs Time required (Sec) to calculate SHA-256

Table 6. Brute force possibility check

Sr	Attribute	Blank .docx	Blank .pdf
1	Size in bytes	13,536	24,827
2	1% of size in bytes	135	248
3	1% of size in bits ('2' × 8)	1080	1984
4	Possible combinations	2^{1080}	2^{1984}
5	Changing the base to 10	1.29×10^{325}	1.75×10^{597}

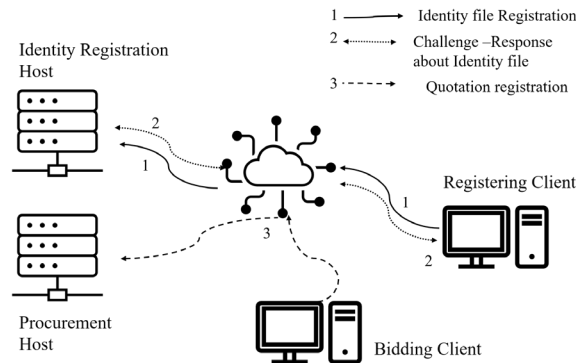


Figure 3. Separate identity and quotation registration

Another experiment was conducted to randomly select a fragment of the same file and calculate its SHA-256 value. The experiment was run 1000 times, and the average data volume processed per second for SHA-256 was 281 MB.

The implemented case study shows that the proposed system does not cause any inconvenience.

4.2 Possibility of Brute-Force Attack

We have checked the feasibility of a brute-force attack using blank files (MS Word and PDF). It was observed that issuing a challenge for 1% of the fragment makes it difficult to obtain a preimage of the hash. The possibility of a brute-force attack with several attributes is demonstrated in Table 6.

Even a password of more than 15 characters can take a relatively long time to crack [41]. And the attacker needs to repeat the procedure for the remaining 99 blocks. The experiment was conducted on blank files, and it was observed that the real quotation document occupies more disk space, making a brute-force attack impossible.

4.3 Separating Identity and Bid

The identity and quotation registration are handled by separate servers, as shown in Figure 3. In this regard, the bidder used a separate channel to identify and register bids. Thus, anonymity can be

provided to bidders. However, the opening quotation does not disclose the bidder's identity. To claim the quotation, the respective bidder must share the identity file registered earlier. However, others can validate it using the logs from the identity registration host. The proposed method is platform-independent and can be applied via social media or an email system.

4.4 The Case of a Compromised Host

In the proposed system, PH keeps all communication logs available in an open domain. To add a layer of accountability, this system can be integrated with email. Where a bidder can communicate with the PH through email APIs such as Gmail, Microsoft Graph, Nylas, and others [42, 43]. Email communication is admissible as valid legal evidence in Indian courts under the Information Technology Act, 2000, and the Bharatiya Saksha Adhinyam, 2023. This can be used to detect a manipulated host.

4.5 The Possible Malpractices and the Results

4.5.1 Bidder Does Not Reply to Challenges

Such a bidder can be identified and blocked by the PH.

4.5.2 Bidder Discloses Quotation with Different Length

Absolute specifications calculated by the PH or others may differ, leading to different fragments. The same input fragment produces the same SHA-256 value. In this case, the bidder can be identified and blocked. In the current scenario, there is a provision to seize Earnest Money Deposit(EMD) in case of malpractice and dishonouring the contract after winning the bid. Generally, EMD is charged 5% of the total value.

4.5.3 The Bidder Discloses Different Quotation

Unidentical quotations produce different SHA-256 values, enabling the detection and blocking of bidders. Manipulation detection is independent of the size of the manipulation. The manipulation detection rate can always be 100%. The time required to detect depends on the size of the quotation document and the computer's capacity.

4.5.4 Compromised Network

In this case, existing error-detection and correction technologies (like SSH or SSL) can handle accidental manipulation and protect communications.

4.6 Real-Time Latency Check

As per the experiments [39,40], processing a 100 MB quotation document takes 0.35 seconds. Also, the communication payload would be less than 1922 bytes, requiring less than 0.5 seconds for transmission. Overall, the activity will take less than 0.85 seconds.

4.7 Legal Consideration

In India, 'Category A' documents have to be preserved forever (perpetuity) by the government, public sector undertakings (PSUs) as a "Permanent" record. For transparency in financial statements, the meeting minutes must be preserved permanently. After receiving the bids, they are open to the technical committee and the purchase committee. Competitors can also attend the meeting to ensure transparency. Bids are awarded, and the procedure is minimised. Bid participants cannot request the erasure of their data, regardless of the bid outcome. Hence, the bidder cannot exercise the 'right to be forgotten'.

5 Limitations of the Study

Timely registration, responding to challenges and disclosing the document are key phases of the proposed system. The existing systems require that the document be deposited before the deadline.

There is no need for iterative communication, i.e., challenge-and-response. Since the proposed system requires only registration, not document deposition, it may lead to a scenario in which participants register the claims but do not participate in the challenge-response. There might also be a scenario in which participant(s) can join the challenge-response but could not disclose their document after the given date. Both scenarios can be addressed by charging the security deposit or participation deposit at the registration phase and freezing the deposit AND/OR blocking the bidder from future bidding processes in case of non-compliance. Moreover, these two provisions are already practiced in the existing system.

6 Conclusion and Future Scope

In this paper, we have proposed a novel approach for e-tendering systems that comply with existing requirements and regulations while providing greater transparency. The proposed system is based on a ‘verifiable claim without disclosure’ and ‘post-disclosure verification’. The proposed system does not require the document deposition. Therefore, the data leakage problem has been eliminated in the proposed system. Participation in the challenge-response and post-disclosure verification approach ensures the transparency and integrity of the document claimed during registration. Registration without document submission eliminates the requirement of secure storage. A bidder can keep their quotation on one isolated computer and use a network computer to interact with the host. It is concluded that run calculations only on isolated computers to obtain the quotation and the responses to the challenges received, and enter the output on a networked computer. This can provide additional confidence in the bidder’s data safety for the proposed system. In the future, we will present a separate identity host alongside the procurement host, allowing participants to remain anonymous.

Author Contributions

S. M.: Conceptualization, methodology, software, writing—original draft preparation.

A. D. V: supervision, validation, writing—review and final editing.

Funding

There is no Funding for this paper.

Conflict of Interest Statement

Author declares no conflict of interest.

Data Availability Statement

No data is collected from any participants. The data generated during the experiment is listed under reference section along with the repository links.

Acknowledgment

Author has no information to declares under this section. .

References

- [1] Government of Maharashtra, *Revised Manual of Office Procedures for Procurement by the Government Departments*. 2016. Accessed: Jun. 22, 2024. [Online]. Available: <https://maitri.mahaonline.gov.in/PDF/GR%2001.12.2016%20Procurement%20Policy%20In%20English.pdf>
- [2] M. L. Emiliani, “Business-to-business online auctions: key issues for purchasing process improvement,” *Supply Chain Management: An International Journal*, vol. 5, no. 4, pp. 176–186, Oct. 2000, doi: 10.1108/13598540010347299.
- [3] S. Bag, F. Hao, S. F. Shahandashti, and I. G. Ray, “SEAL: Sealed-Bid Auction Without Auctioneers,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2042–2052, 2020, doi: 10.1109/TIFS.2019.2955793.
- [4] T. S. Chandrashekar, Y. Narahari, C. H. Rosa, D. M. Kulkarni, J. D. Tew, and P. Dayama, “Auction-Based Mechanisms for Electronic Procurement,” *IEEE Transactions on Automation Science and Engineering*, vol. 4, no. 3, pp. 297–321, Jul. 2007, doi: 10.1109/TASE.2006.885126.
- [5] M. H. Rothkopf, T. J. Teisberg, and E. P. Kahn, “Why Are Vickrey Auctions Rare?,” *Journal of Political Economy*, vol. 98, no. 1, pp. 94–109, Feb. 1990, doi: 10.1086/261670.

- [6] K. Wei and Y. Dang, "Anonymous Verifiable Sealed Quotation Auction Based on Blockchain," in *Proceedings of the 2nd International Conference on Bigdata Blockchain and Economy Management, ICBEM 2023, May 19–21, 2023, Hangzhou, China*, EAI, 2023. doi: 10.4108/eai.19-5-2023.2334348.
- [7] D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. A. Thorpe, "Practical secrecy-preserving, verifiably correct and trustworthy auctions," in *Proceedings of the 8th international conference on Electronic commerce The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet - ICEC '06*, New York, New York, USA: ACM Press, 2006, p. 70. doi: 10.1145/1151454.1151478.
- [8] M. Abe and K. Suzuki, "Receipt-Free Sealed-Bid Auction," 2002, pp. 191–199. doi: 10.1007/3-540-45811-5_14.
- [9] A. Neupane, "The potential of public e-procurement technology to reduce corruption in public procurement," University of Southern Queensland, 2014.
- [10] S. Mohammadi and H. Jahanshahi, "A secure E-tendering system," in *2009 IEEE International Conference on Electro/Information Technology*, IEEE, Jun. 2009, pp. 62–67. doi: 10.1109/EIT.2009.5189585.
- [11] C. Pop, M. Prata, M. Antal, T. Cioara, I. Anghel, and I. Salomie, "An Ethereum-based implementation of English, Dutch and First-price sealed-bid auctions," in *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*, IEEE, Sep. 2020, pp. 491–497. doi: 10.1109/ICCP51029.2020.9266180.
- [12] C.-C. Wu, C.-C. Chang, and I.-C. Lin, "New Sealed-Bid Electronic Auction with Fairness, Security and Efficiency," *J. Comput. Sci. Technol.*, vol. 23, no. 2, pp. 253–264, Mar. 2008, doi: 10.1007/s11390-008-9127-x.
- [13] H. Hasran, A. Indrasakti, and A. S. Wicaksono, "Characteristics of Tenders As A Pre-Contract Stage for the Procurement of Goods and Services," *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 2, pp. 437–444, Feb. 2024, doi: 10.59141/jist.v5i2.904.
- [14] S. Mackie, L. Azzopardi, and Y. Moshfeghi, "An Initial Analysis of E-Procurement Search Behaviour," 2022, pp. 3–12. doi: 10.1007/978-3-030-96960-8_1.
- [15] A. Mavidis and D. Folinas, "From Public E-Procurement 3.0 to E-Procurement 4.0; A Critical Literature Review," *Sustainability*, vol. 14, no. 18, p. 11252, Sep. 2022, doi: 10.3390/su141811252.
- [16] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology — EUROCRYPT '99*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 223–238. doi: 10.1007/3-540-48910-X_16.
- [17] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proceedings of the 1st ACM conference on Electronic commerce*, New York, NY, USA: ACM, Nov. 1999, pp. 129–139. doi: 10.1145/336992.337028.
- [18] Sako Kazue, "Universally verifiable auction protocol which hides losing bids," in *Proc. of Public Key Cryptography*, 2000, pp. 35–39.
- [19] K. Suzuki, K. Kobayashi, and H. Morita, "Efficient Sealed-bid Auction using Hash Chain," 2001, pp. 183–191. doi: 10.1007/3-540-45247-8_15.
- [20] M. Abe and K. Suzuki, "Receipt-Free Sealed-Bid Auction," 2002, pp. 191–199. doi: 10.1007/3-540-45811-5_14.
- [21] H. Lipmaa, N. Asokan, and V. Niemi, "Secure Vickrey Auctions without Threshold Trust," 2003, pp. 87–101. doi: 10.1007/3-540-36504-4_7.
- [22] R. K. Singh and L. Benyoucef, "A fuzzy TOPSIS based approach for e-sourcing," *Eng. Appl. Artif. Intell.*, vol. 24, no. 3, pp. 437–448, Apr. 2011, doi: 10.1016/j.engappai.2010.09.006.
- [23] H. S. Galal and A. M. Youssef, "Verifiable Sealed-Bid Auction on the Ethereum Blockchain," 2019, pp. 265–278. doi: 10.1007/978-3-662-58820-8_18.
- [24] Q. Feng, D. He, H. Wang, D. Wang, and X. Huang, "Multi-party key generation protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IET Inf. Secur.*, vol. 14, no. 6, pp. 724–732, Nov. 2020, doi: 10.1049/iet-ifs.2020.0096.
- [25] H. Abulkasim, A. Mashatan, and S. Ghose, "Quantum-based privacy-preserving sealed-bid auction on the blockchain," *Optik (Stuttg.)*, vol. 242, p. 167039, Sep. 2021, doi: 10.1016/j.ijleo.2021.167039.
- [26] G. Sharma, D. Verstraeten, V. Saraswat, J.-M. Dricot, and O. Markowitch, "Anonymous Sealed-Bid Auction on Ethereum," *Electronics (Basel)*, vol. 10, no. 19, p. 2340, Sep. 2021, doi: 10.3390/electronics10192340.

- [27] B. Chen, X. Li, T. Xiang, and P. Wang, "SBRAC: Blockchain-based sealed-bid auction with bidding price privacy and public verifiability," *Journal of Information Security and Applications*, vol. 65, p. 103082, Mar. 2022, doi: 10.1016/j.jisa.2021.103082.
- [28] D. Mali, D. Mogaveera, P. Kitawat, and Mohd. Jawwad, "Blockchain-based e-Tendering System," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, IEEE, May 2020, pp. 357–362. doi: 10.1109/ICICCS48265.2020.9120890.
- [29] H. P. A, M. Latha, Ashwin. M. S, and R. Chinnaiyan, "BlockchainAs a Service (BaaS) Framework for Government Funded Projects e-Tendering Process Administration and Quality Assurance using Smart Contracts," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, Jan. 2021, pp. 1–4. doi: 10.1109/ICCCI50826.2021.9402348.
- [30] K. Ananthajothi, P. K. Jaisuriya, and S. Haribala, "Ethereum Powered E-Tendering System," in *2024 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, IEEE, Apr. 2024, pp. 1–5. doi: 10.1109/IC3IoT60841.2024.10550251.
- [31] F. Bruschi, T. Paulon, V. Rana, and D. Sciuto, "A Protocol for On-Chain Tenders," in *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE, Mar. 2022, pp. 273–278. doi: 10.1109/PerComWorkshops53856.2022.9767325.
- [32] R. Fangki, "Tender Auction System: Secure Transactions for Goods and Services," *Jurnal Sistem Informasi dan Teknik Informatika (JAFOTIK)*, vol. 2, no. 1, pp. 13–17, Feb. 2024, doi: 10.70356/jafotik.v2i1.28.
- [33] L. K, H. B, M. Deepika, M. T. Badal, and K. K R, "Smart Tender Contract Management System," in *2024 Second International Conference on Inventive Computing and Informatics (ICICI)*, IEEE, Jun. 2024, pp. 497–501. doi: 10.1109/ICICI62254.2024.00086.
- [34] B. Schneier, *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C*. 2014.
- [35] W. Stallings, *Cryptography and Network Security: Principles and Practices*. 2005.
- [36] C. Dong, Y. Xu, X. Liu, F. Zhang, G. He, and Y. Chen, "Hardware Trojans in Chips: A Survey for Detection and Prevention," *Sensors*, vol. 20, no. 18, p. 5165, Sep. 2020, doi: 10.3390/s20185165.
- [37] H. Chunduri, P. M. Anand, S. K. Shukla, and P. V. Sai Charan, "Trusted Yet Disguised: Analysing the Subversive Role of LOLBins in Contemporary Cyber Threats," in *2024 IEEE International Conference on Big Data (BigData)*, IEEE, Dec. 2024, pp. 2596–2605. doi: 10.1109/BigData62323.2024.10825239.
- [38] M. Coluzzi, A. Brocco, P. Contu, and T. Leidi, "A survey and comparison of consistent hashing algorithms," in *2023 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS)*, IEEE, Apr. 2023, pp. 346–348. doi: 10.1109/ISPASS57527.2023.00048.
- [39] S. Manerikar and A. Vibhute, "Simulation of E-Procurement System with delayed bid document submission," 2026, *Zenodo*. doi: 10.5281/zenodo.18430311.
- [40] S. Manerikar and A. Vibhute, "File Fragment Hash Calculator," 2026, *Zenodo*. doi: 10.5281/zenodo.18360121.
- [41] J. Tan, L. Bauer, N. Christin, and L. F. Cranor, "Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2020, pp. 1407–1426. doi: 10.1145/3372297.3417882.
- [42] A. Mishra, "Sending Emails Using Graph API," in *Microsoft Azure for Java Developers*, Berkeley, CA: Apress, 2022, pp. 197–220. doi: 10.1007/978-1-4842-8251-9_10.
- [43] Z. Chen and G. Washburn, "A Robust Set of Emailing Applications that Allow an effective Solution for Bulk Email Sending and receiving," in *Security, Privacy and Trust Management*, Academy & Industry Research Collaboration Center, Jun. 2024, pp. 127–137. doi: 10.5121/csit.2024.141111.

Author Biographies



Swaroop R. Manerikar is from Sindhudura, Maharashtra and has completed his Graduation and postgraduation in Computer Science from Ratnagiri, Maharashtra. He qualified for the National Eligibility Test conducted by UGC in 2012. He is working as a PhD scholar at Symbiosis International University, Pune, India on the domain of security and privacy for the online data. He is currently working in the Institute of Forensic Science, Mumbai.



Dr. Amol D. Vibhute is an Assistant Professor, Associate Dean, and Program Head of MSc (Cybersecurity) at the School of Cyber Security and Digital Forensics, National Forensic Sciences University, Nagpur Campus (An Institution of National Importance), Ministry of Home Affairs (MHA), Government of India. He has over 11 years of experience in research, innovation, and undergraduate and postgraduate teaching. His four (04) Indian and two (02) International patents have been granted and four (04) Indian patents are under the granting stage. He authored/coauthored over 40+ refereed journal papers, seven book chapters, and more than 55 reputed conference papers indexed by SCIE/Scopus/WoS/UGC. The current citations of his research exceed 1,850, 1,000, and 500, with an h-index of 20, 16, and 10, as per Google Scholar, Scopus, and Web of Science, respectively. His two books have been published, and one has been accepted by a reputed publisher and indexed in Scopus. His specialisation is in Hyperspectral-Multispectral Remote Sensing, GIS, Remote Sensing of Soil, Crops, Urban areas, and other areas. His research interests include Geospatial Technology, Digital Image Processing, Computer Vision, Pattern Recognition, Artificial Intelligence, Machine Learning, and Pattern Recognition. He is an IEEE senior member as well as a member of ACM, ISPRS, IAEng, CSTA, IACSIT, and ISCA. He is an editorial board member of Scientific Reports (Sci Rep) published by “Nature Portfolio”, ISSN: 2045-2322 (online). Also, he is an active reviewer of the IEEE Transactions journals like GRASS, Pattern Recognition, Sensors journal, AgriFood Electronics, Image Processing, IEEE Access, and Elsevier (Remote Sensing of Environment, Computer Science Review, Computers and Electronics in Agriculture), Taylor and Francis journals, Wiley Online journals, and Springer Journals indexed by SCI/SCIE/Scopus/WoS..