

## E-Tendering system using Blockchain Technology

Shashank Gowda B B<sup>1</sup>, Brunda C K<sup>1</sup>, Sumanth L Reddy<sup>1</sup>, Rahul V<sup>1</sup>, Chandru A S<sup>2</sup>

<sup>1</sup>UG Student, Dept. of Information Science and Engineering, NIE Institute of Technology, Mysuru, Karnataka, India.

<sup>2</sup>Associate Professor, Dept. of Information Science and Engineering, NIE Institute of Technology, Mysuru, Karnataka, India.

\*\*\*

**Abstract** - The offering interaction is a key business measure that assists organizations with tracking down an appropriate worker for hire. In the structure and development enterprises, customers welcome givers to present a gauge of costs, enumerating the expenses related with finishing a structure. Thusly, the customer can put together their choice with respect to the consequence of the tenders to choose the most reasonable project worker. The givers need to gather the delicate's booklet, value it, and take it back to the customer's office before the cut-off time. In this paper, we present a plan and execution of an e-offering framework by utilizing Web administrations for the mechanization of such offering measures. In this paper, we utilized the blockchain innovation in advanced e-offering framework to tackle the security issues and satisfy the framework necessities. We use SHA for hashing and AES rijndael calculations to scramble the information. It offers new freedoms to convey a safe e-offering framework in any association or country. The arrangement is far superior when contrasted with other arrangement since, it is a decentralized framework, contain the outcomes as spot coins, having various areas. We will likewise break down the security of our proposed offering framework, which shows our convention is safer when contrasted with different arrangements.

**Key Words:** E-tendering system, Block-chain, SHA, AES rijndael, security.

### 1. INTRODUCTION

Current E-Tendering systems are not 'fair and open' meaning that the information is not shared with all stakeholders (Right to Information). The information is released on 'as they please' basis for example - when a company is selected as a winner of a contract, other companies that bid on the same tender are not notified of why their bid was rejected and why a particular company was selected as a winner. A company can request this information but it is a tedious process of getting this data. Even though auditing these documents is possible, evaluating the documents needs time. Aside from not being straightforward, security is additionally a significant issue for these entryways prompting misrepresentation and control of information put away in a brought together data set. If the hacker gets hold of this centralized database, bids can be leaked to competitors leading to major financial and strategic losses for a business.

Blockchain innovation can be utilized to settle these security suggestions as it vigorously around the decentralization of

data and is gotten by encryption coordinated with irrefutable square based engineering for exchange the executives.

Hence, Blockchain can be used as a transparent, decentralized and secured tendering framework that will facilitate bidders' oversight on portal functions and observe all the activities carried out by the tender portal.

### 2. MODULS

We have four modules:

1. Authentication
2. Apply tender
3. Manage client company & client feedback
4. Tender manage & approval

#### Authentication.

Tender Company, Bidder Company & Client company login authentication done in order to verify.

SMTP protocol is used.

#### Apply Tender.

- Bidder Company apply to the Tender based conditions
- **Bid Open Date** - Apply after Bid open date
- **Bid Close Date** - Apply before Bid close date
- **Status-Not Complete** - Apply tender not complete
- **Check Tender already apply** - Only once tender apply based on Blockchain, SHA algorithm & AES rijndael algorithm tender quotation details store in database.

#### Manage client company & client feedback.

- Bidder Company add client company details & provide login Id & password. Bidder company, manage company profile i.e., previous project work details to client.

- Above details maintain, due client feedback/rating based on Tender approval process done.
- Client Company post feedback comments related to project work by bidder company.
- The feedback comment process to NLP concept & rating done.

### Tender manage & approval.

- Tender Company based on category, create new tender with tender details (Tender description, Bid Open date, Bid Close date, Status).
- Tender Company view Tender quotation details Based on Blockchain, SHA algorithm & AES rijndael algorithm tender quotation details from database.
- Check Company Profile (Previous work - feedback comment related to Project & rating's) Tender Company Approve Tender & specify reason

## 3. TECHNOLOGIES AND CONCEPTS

### 3.1 Blockchain Explained

Blockchain is based on the concept of decentralization. Hence, it can be viewed as a distributed database. In this case, the distributed database employs the concept of full replication i.e. each node has a full copy of a blockchain. Whenever the blockchain needs to be updated because of a transaction, a process called mining takes place. A block consists of many transactions. A consensus protocol is used and the mined block is broadcasted to all other nodes. These blocks will have a cryptographic hash in the header that relates to the previous block in the chain. In the event that a square is controlled the hash related with this changes and therefore, all the procedure squares ought to be re-mined which is unimaginable. As such, blockchain utilizes the property of permanence. How the blockchain is implemented and what consensus protocol is the core of blockchain.

### 3.2 SHA-256

SHA-256 is quite possibly the most secure hashing capacities available. The US government requires its offices to secure certain touchy data utilizing SHA-256. While the specific subtleties of how SHA-256 functions are arranged, we realize that it is worked with a Merkle structure got from a single direction pressure work itself made with the Davies-Meyer structure from a particular square code.

Three properties make SHA-256 this protected. To start with, it is practically difficult to reproduce the underlying information from the hash esteem. An animal power assault would have to make 2256 endeavour to create the underlying information. Second, having two messages with a

similar hash esteem (called a crash) is incredibly improbable. With 2256 potential hash esteems (more than the quantity of molecules in the known universe), the probability of two being the equivalent is imperceptibly tiny. At long last, a minor change to the first information modifies the hash esteem such a lot of that it's not evident the new hash esteem is gotten from comparative information; this is known as the torrential slide impact.

### 3.3 AES RIJNDAEL

The square code is intended to utilize just straightforward entire byte activities. Likewise, it gives additional adaptability over that expected of an AES competitor, in that both the key size and the square size might be picked to be any of 128, 192, or 256 pieces. (During a beginning phase of the AES cycle, a draft form of the prerequisites would have required every calculation to have three variants, with both the key and square sizes equivalent to each of 128, 192, and 256 pieces. This was subsequently changed to cause the three expected adaptations to have those three key sizes, however just a square size of 128 pieces, which is all the more effortlessly obliged by numerous kinds of square code plan.)

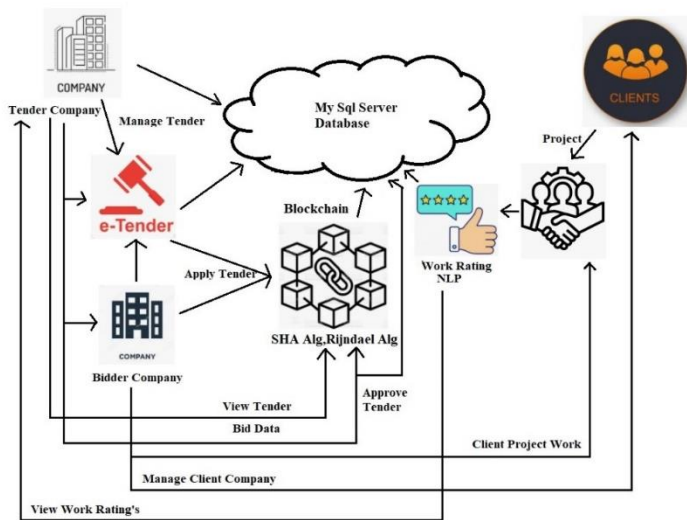
### 3.4 SMTP PROTOCOL

The **Simple Mail Transfer Protocol (SMTP)** is an internet standard communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages. User-level email clients typically use SMTP only for sending messages to a mail server for relaying, and typically submit outgoing email to the mail server on port 587 or 465 per RFC 8314. For retrieving messages, IMAP and POP3 are standard, but proprietary servers also often implement proprietary protocols.

### 3.5 NATURAL LANGUAGE PROCESSING.

NLP empowers PCs to comprehend regular language as people do. Regardless of whether the language is spoken or composed, normal language preparing utilizes man-made brainpower to take genuine information, measure it, and sort out it in a way a PC can comprehend. Similarly as people have various sensors - like ears to hear and eyes to see - PCs have projects to peruse and mouthpieces to gather sound. And just as humans have a brain to process that input, computers have a program to process their respective inputs. At some point in processing, the input is converted to code that the computer can understand. There are two main phases to natural language processing: data pre-processing and algorithm development. Data pre-processing involves preparing and "cleaning" text data for machines to be able to analyze it. Pre-processing puts data in workable form and highlights features in the text that an algorithm can work with.

#### 4. SYSTEM DESIGN



1. A tender is created by the tendering organization by specifying the details such as description, bidding period, etc.
  - a. The stipulation of tender takes place i.e. the tendering company states its demands and the evaluation criteria on which a bid will be evaluated.
  - b. Once the tender details are finalized and the documents are provided, the tender is then

sent to the blockchain in the form of a smart contract. The documents are stored in an encrypted form in a database and are only available to companies that are willing to bid.

2. The bidder registers asynchronously with the system. The bidder is then shown all the tenders available for bid with tender details.
  - a. The bidder then searches for appropriate tender for bidding.
  - b. The tender requirements are sent to the bidder along with the tendering organization details.

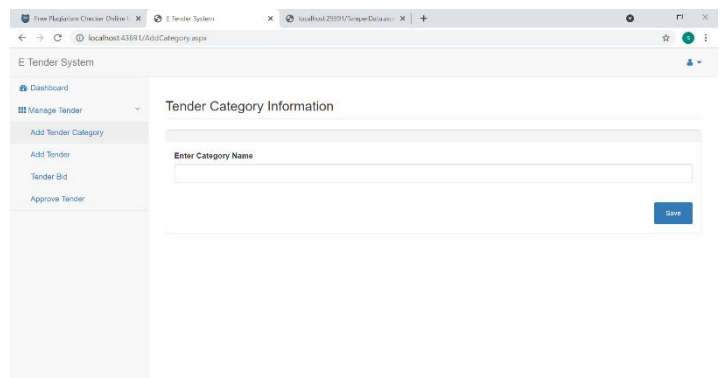
3. The bidder then places a bid on the tender by providing a quote, quotation clauses. The bids are encrypted twice. With bidder's symmetric key and ii. Tender's public key (address of tender on the blockchain). The bidder also shows its credibility by providing its balance sheet, a license from RoC (Registrar of Companies) which are encrypted with

the same key as discussed earlier. The bidder can only bid during the bidding period and once the deadline is reached, no further bids will be accepted.

4. Once the deadline is passed the bids are open to the tendering organization for evaluation.
  - a. The tendering organization gets the details of all the bids and decrypts the bid using the key provided by the bidder.
  - b. Then the bid is evaluated and the credibility and capability of the bidding company are checked using the documents provided in the bid. The tendering organization can approve or reject the bid.
5. The tendering organization then selects the best bid as the winner. All the bidding and negotiation information is released to all the bidders. Thus, ensuring transparency.

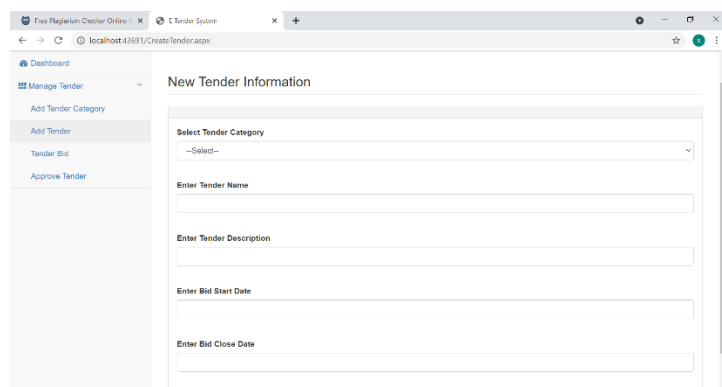
#### 5. RESULTS

##### 5.1 Create Tender Category



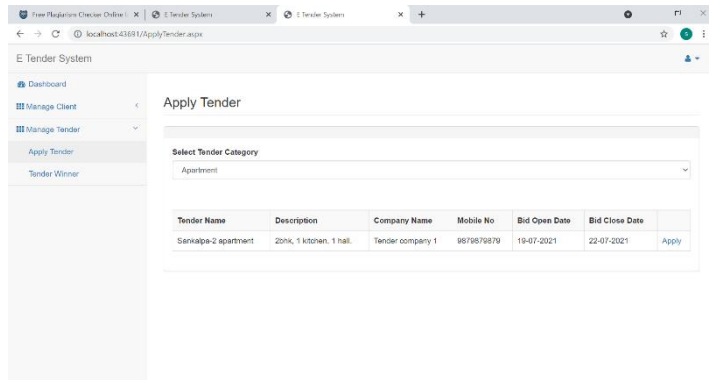
The above table represents how to create a tender category.

##### 5.2 Create Tender



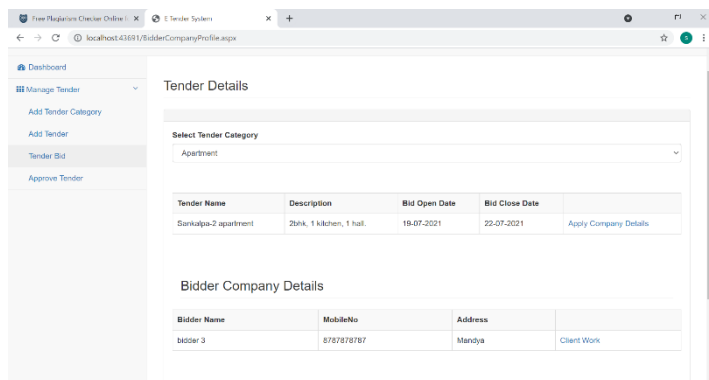
The above table represents how to create a tender. After creating a tender category, the tender company will add a tender based on that category. Here, tender name, description, start date/ close dates are required.

### 5.3 Apply Tender



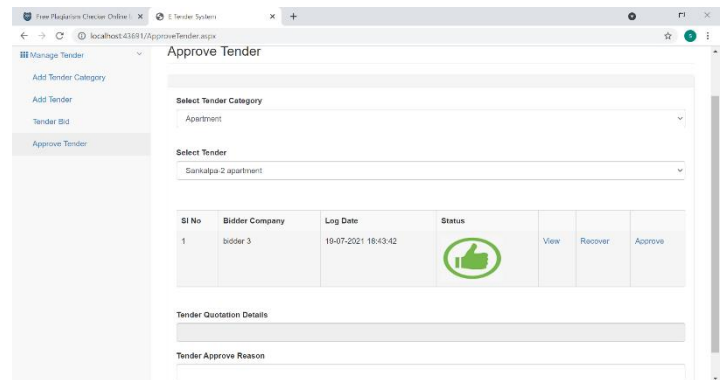
The above figure represents how to apply a tender. Once the tender is created by the tender company that will be published and it can be viewed by the bidder company. There the tender details i.e., tender name, description, start/close date will be displayed.

### 5.4 View bidder profile.

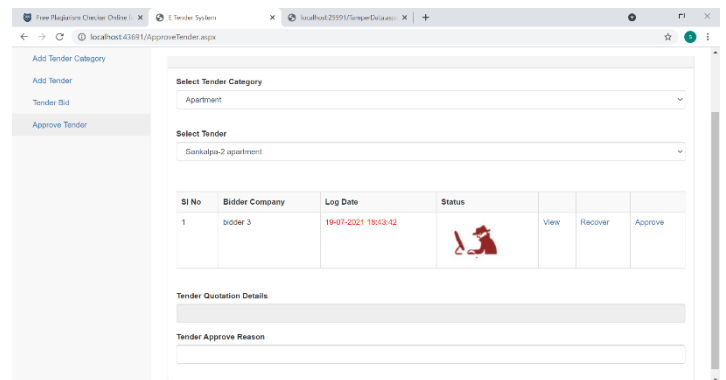


The above figure represents how the bidder profile is viewed by the tender company. Once the bidder apply for the tender, the applied list will be viewed by the tender company.

### 5.5 Check if the data is tampered or not.

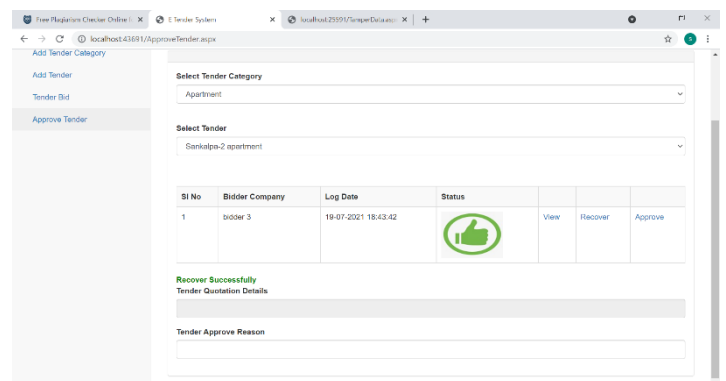


The above figure shows that the data is not tampered.



The above figure shows that the data is modified/tampered.

### 5.6 Recovering the modified data.



If the data is tampered or modified it can be easily recovered by using “recover” option. The above figures show how the data is recovered.

After this, the tender company will select the best bit based on their bid amount and their previous work feed back, which is calculated using NLP concept.

## 6. SECURITY ANALYSIS.

The security provided by a Blockchain based tendering system.

- The company that placed bids are not viewable to other bidders until the tender applied results are revealed.
- The blockchain network must be secure such that bidder company cannot change the bid of another bidder company.
- The tendering company cannot change the tender details once the tender is placed as they may change the requirements to help a particular group.
- The tender company can see the bids only when the date for applying tender is closed.
- Here, bids are encrypted. Hence, block cannot put a security implication on the system by miners.

## 3. Online Tendering and Evaluation for Public Procurement in Tanzania

978-1-5090-5504-3/17/\$31.00 ©2017 IEEE SNPD 2017, June 26-28, 2017, Kanazawa, Japan.

## 7. CONCLUSIONS

When it comes to applications like tender management, where security and transparency is important and traditional technologies and old design patterns cannot be used as they might cause a risk of tampering data. As we know, there are many security requirements for a tendering system that cannot be solved just by using a centralized database for creating and bidding the contracts.

As we are using SHA and AES algorithm for encrypting the data and NLP concept for rating the client feedback, it helps the tender company for selecting the best bid among the list. Using technology like blockchain i.e., decentralized database, the security and openness required for this type of applications can be solved.

In this paper, how such a system can be designed by mentioning various processes involved and their basic implementation are discussed.

## References

1. **e-Tendering with Web Services: A Case Study on the Tendering Process.**  
Lai Sau Chan<sup>1</sup>, Dickson K.W. Chiu<sup>2</sup> and Patrick C.K.Hung<sup>3</sup> Department of Computer Science and Engineering, 2007
2. **Sec-EVS: Secure Electronic Voting System Using Blockchain Technology**  
2018 International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018