A Secure Framework for Government Tender Allocation Based On AWS Service

Likitha M P [1], Dr. Prasanna B T [2]

[1] Student, Compute science and engineering, JSSSTU
[2] Associate professor, Computer science and engineering, JSSSTU

Abstract

Tendering is a lengthy and complex business process that results in several legal obligations associated with corporate contracts. Several governments used an e-tendering system to carry out the tender procedure. Government agencies and private organizations are continuously working to bring fairness in this process. The e-tendering process brings efficiency and convenience in the overall practices which has been seen recently. By facilitating the procurement process with linked parties, e-tendering attempts to promote productivity, effectiveness, and transparency in the tender process. Problems with the e-tendering system remain centralized, giving local groups complete control over the database and system, increasing the risk of fraud, collusion, and manipulation. To avoid bidder fraud and suspicion, the highly competitive contract selection process must be supported by effective and transparent technology. AWS S3 cloud service, AES encryption technology and QR code technique will allow integrated systems to function without any third party involvement. By adopting this technology, e-tendering can reduce the source of fraud, namely database manipulation.

Keywords: Encryption, AES, NLP, e-tendering, QR code.

1. Introduction

- E-tendering is a network platform that is built based on bidding in new ways, which can release information, submit tenders, evaluate bids and so on. The e-tendering system has also developed progressively over the years. In the 1980s it was the beginning of the implementation of e-tendering that was pioneered in the formof one-way information, meaning that communication was not continuous through the same media, i.e., the website was only used as an alternative form of notification to display information other than the traditional method of publishing in sheets. If the tender or related public who wishes to participate in the tender must follow up through contacts such as telephone calls and direct interviews. All subsequent processes must be done manually and inthe paper.

- Then in following years, e-tendering began to develop i.e the web system Expanded to allow files, digitized from paper documents to be downloaded and online forms tobe filled out and submitted online and progressed until the e-tendering system was fully integrated. E-tendering systems can strategically integrate appropriate security mechanisms toprovide the desired security and efficiency services, whereas

traditional tendering systems relyon transparency to achieve equality. With the continued development of technology,the application of e-tendering also has challenges in its implementation.

- Here we implement the project by making it more secure and transparent by the bidders/supplier of goods and services who provide quotation details that will be encrypted with AES encryption algorithm [3] & written to QR code image, store in AWS S3 service. The government officer will download the QR code image from AWS S3 service, decrypt data and evaluate the process who is best based onbidder company profile, based on client rating's on previous project works and will announce the tender winner. Here NLP concept is used [7] to measure client feedback for bidder project work. The centralized database management on the e-tender system has several negative sides that can becaused by being not transparent which will make it vulnerable to collusion with third parties, that the content of bidding quotation details can be leaked/spread to other bidders. [8] Therefore, technology solutions are needed that can be used to protect auction offers, giving rise to trust without the need for third parties according to the principle of procurement of goods/services.[The AES encryption, AWS S3 service & QR code techniques is one solution that can be used to reduce the problems that occur in the current e-tender system.

2. Objectives
- To secure the transaction of e-tendering data using AES and Shamir's algorithm.
- To select the winner of the bid by their rating through NLP.
- To provide an automated experience through network application.

3. Literatute survey
1. "Online Tendering and Evaluation for Public Procurement in Tanzania" Amani Dello and Dr. Chika Yoshida IEEE, June 2017.

This paper analyses how Innovation can be used in Public Procurement to ensure true fairness, competitiveness, transparency and value for money in public projects.

This paper describes the overall Procurement Management practices used in Tanzania how e-evaluation as a component of e-procurement can reduce Time and Cost of Public Projects.

2. "A Secret Sharing Scheme Based on AES", Zhiqiang Xie and Hong Zhong , International Journal of Security and Its Applications, 2017

This paper combines AES algorithms, dynamic key generation mechanisms, Shamir's threshold secret sharing scheme. And sets up the file encryption key for distributed storage to ensure the security of the key and resolve the issues of key complexity, key management and file security.

3. "Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography" Musa. M. Yahaya, Aminat Ajibola IJSRCSEIT , May 2019.

Here authors have made an attempt to identify the key elements or requirements for data security technique in which secure data transmission can take place over open channels without the fear of data breach or interference by third party. Recently, the rate of data transfer over the internet globally has increased and this called for more data security . Cryptography is used to perform encryption on the secrete message while steganography hides the secrete message in digital media, image in this regards.

4. "Qr Code Based Cloud Data Protection Using Rsa Algorithm" Vipin Rawat Km Divya Deena Nath Devki Nandan Shukla, IJCRT, April 2018.

In this paper main goal is public cloud data protection using the asymmetric key encryption algorithm . The main concept of this algorithm encryption technique done by the public key and QR Code. After encryption the file is mostly secure and encrypted file is encrypted in QR code format. Decryption is done by the different key means private key and scan the QR code if QR code is correct the decrypted file is automatically downloaded, is depicted in this paper.

5.   "Review of NLP-based Sytems in Digital Forensics and Cybersecurity", Murat Karabata and Ukwen David, IEEE, January 2021.

This research paper focuses on a literature review of NLP-based systems in and cyber security: role, applications and future directions. This article serves as a guide for researchers and practitioners on the current state of cyber security and provides a roadmap for the future.

NLP-based systems are very powerful systems that can automate tasks and extract information from unstructured sources

4. Proposed System and Methodology

We propose a system to develop an application which will help to secure the tender data. The tender details & quotation details are stored in the AWS S3 services. Each tender quotation details are encrypted by using AES encryption algorithm, then write to QR code image & store in AWS S3 service.

The project is divided into sections, 1. Government department creation tenders, 2. Bidding process on the tender, 3. Government evaluation, and review Bidder Company project works & ratings. 4. Client company post review comment on project works& by using NLP concepts, comments are converted to rating points. To view tender quotation details,OTP is generated and notification is sent to respective person email id. Once OTP is verified, the tender quotation details can beviewed by decrypting data.

This enables privacy and security and prevents from third- party access.

For A Secure Framework for Government TenderAllocation through encryption Algorithms like AES, Shamir's algorithms and using NLP for sorting the reliable and efficient quotation.

Encryption Algorithms are used to secure transaction and to have less human intervention and interaction with efficient price than other secure data transaction technology.

AES

AES is essential for government computer security, cyber security and electronic data protection. Here AES is selected for the secure framework for government tender as allocation RSA algorithm is essentially for small amount of data and slower, DES algorithm is very likely to get attacked.

As shown in Fig 2.1 and 2.2 Input data that is applied by the Bidder about the Quotation is sent to AES encryption algorithm. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data
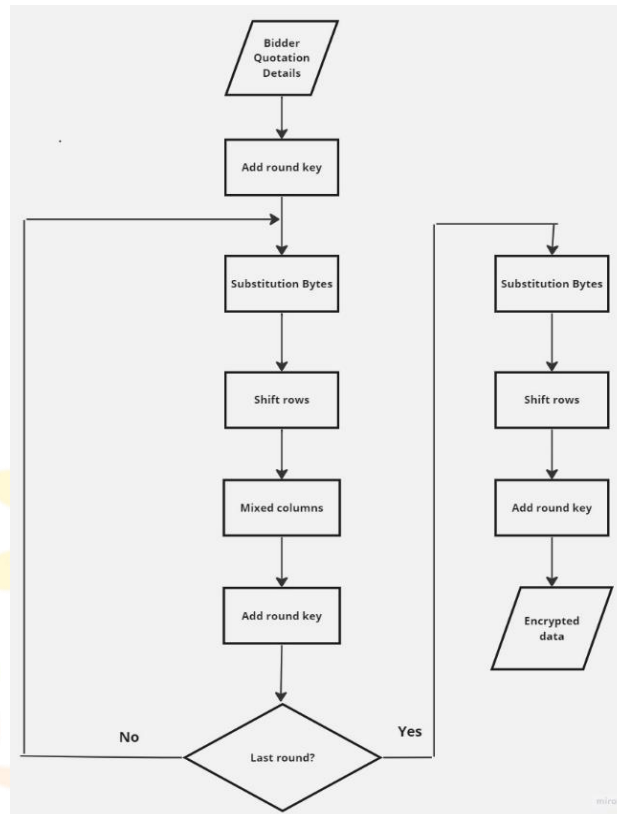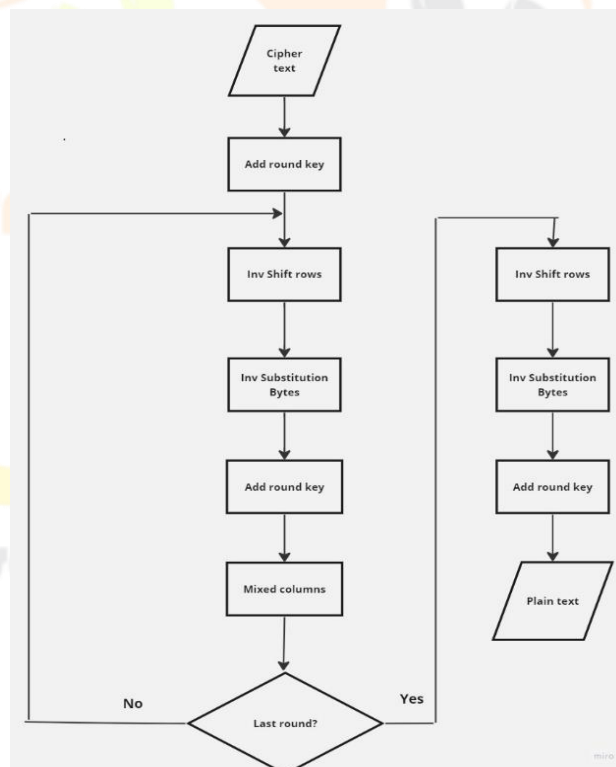
Fig 4.1: Flow diagram of AES encryption

Fig 4.2: Flow Diagram AES Decryption

Shamir's secret sharing

Shamir's secret sharing is used to secure a secret in a distributed form, as in Fig 2.3 most often to secure encryption keys. The secret is split into multiple shares, which individually do not give any information about the secret. To reconstruct a secret secured by SSS in Fig 2.4, a number of shares is needed, called the threshold. No information about the secret can be gained from any number of shares below the threshold

The Random the key generated is passed as input to Shamir's Algorithm for split up and encryption. QR codes are two-dimensional barcodes that are used to store data. Large data's are stored in QR code image.

Any kind of illegal intruder try's to fetch or tamper data that is stored, cannot be achieved as the stored data will be in encrypted format. If any tampering happens, the Hash value that is generated for the encrypted data using SHA algorithm will change. By the change in Hash value one can evaluate that the data is not in original format.

NLP
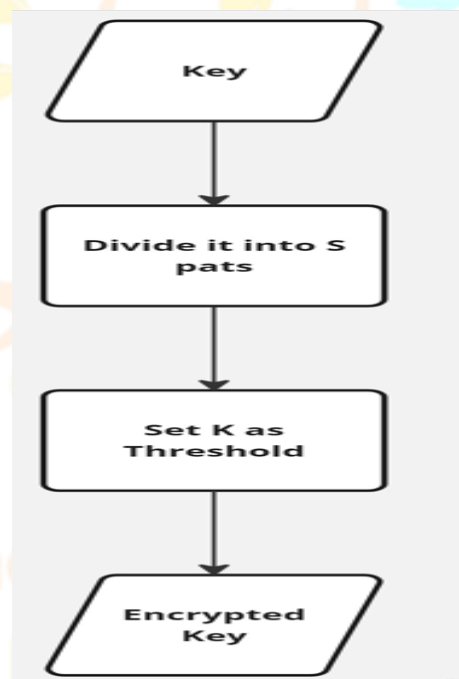
NLP feedback is the automated analysis of text-based   customer responses in order to gather actionable insight. Natural language processing (NLP) programs allow businesses to analyse large amounts of data at scale, saving time and manpower. By using NLP fraudulent and unreliable bidder organisation can be crossed out and it save's time by making it easier for Tender owner to shortlist the reliable bidders.

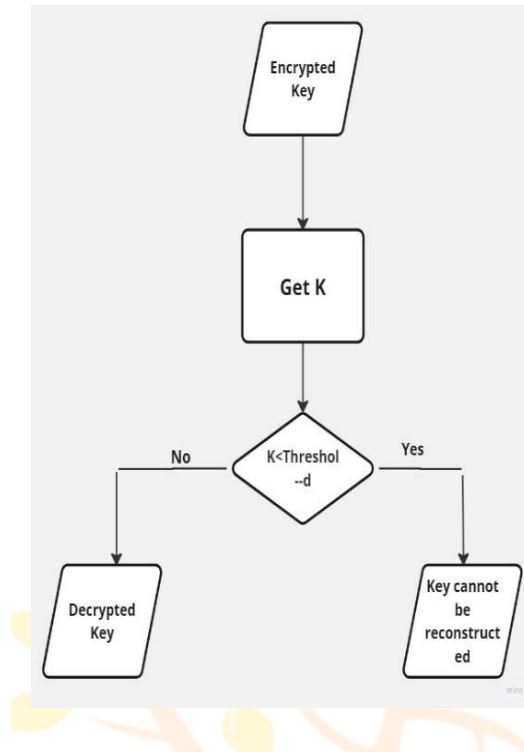Fig 4.3 : Flow working Encryption of Key

Fig 4.4 : Flow working Reconstructing key

5. Implementation

The network application is developed, in which all actors such as Admin, staff, bidder have the interface that is dedicated for accessing the application with convenience. Is depicted in Fig 2.5.

Admin

The functionalities of admin is to add the authorized department's details and their staff member. After adding the staff details a randomly generated user-id and password are sent to their respective mail address.

Staff

After receiving credentials, the application can be accessed by staff. They can perform functionality like creating tenders, their requirements, and duration and so on.

Bidder

Bidders after registering themselves on the application, they will start receiving the tenders that are created. They are allowed to apply for any tender of their interest only if it has not reached past it's end date. The bid that is quoted from bidders are used as input data for AES encryption algorithm.
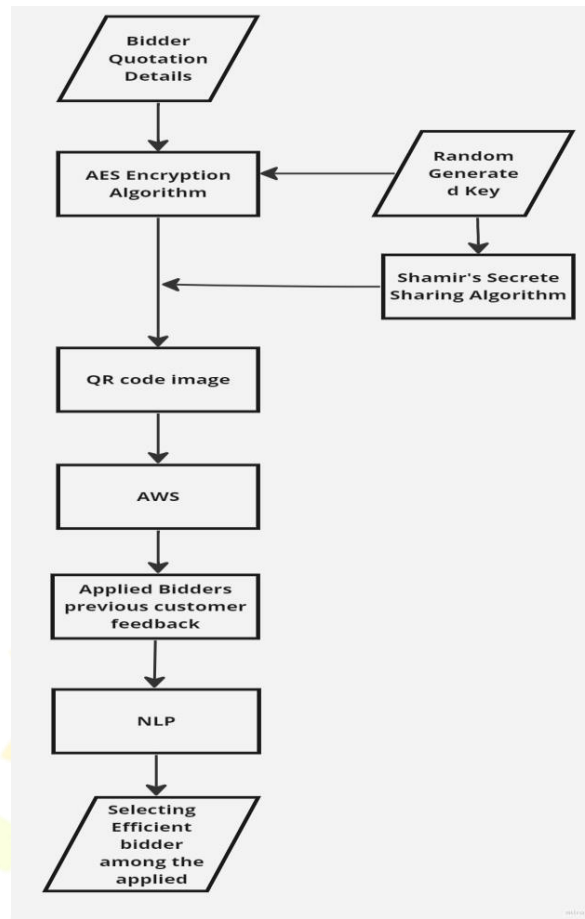
Fig 5.1: Flow diagram of the secure framework for tender using encryption algorithm, NLP, and QR code

6. References

1) Shailja Kumari,Jyoti Chawla "Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security", International Journal of Innovations & Advancement in Computer Science IJIACS, Vol 4, May 2015.

2) M. Mary shanthi rani1 , k.rosemary euphrasia,"Data security through qr code encryption and steganography", ACIJ , 2016.

3) Ekta agrawal, parashu ram pal, "A secure and fast approach for encryption and decryption of message communication", International journal of engineering science and computing, may 2017

4) Uttam Upadhyay, Pradeep Kumar and Deepti Aggarwal "Secure Migration of Mobile Agent using AES & Secret Sharing Approach", International Journal on Emerging Technologies, 17 July 2019.

5) Yanling Zhao ,Ye Li Xinchang Zhang, Guanggang Geng ,Wei Zhang "A survey of networking applications applying the software defined networking concept based on machine learning ",IEEE,2019.

6) Sanjeev Kumar Mandal1, A R Deepti,,"A Review Paper on Encryption Techniques", IJRAR, June 2019

7) Putri Mirah Delima and M.Dachyar "Advancing the E-Tendering Information System to Counter

Corruption by Proposing Anti-Corruption SMART Tools" International Conference on applied engineering(ICAE), 2020.

8) Sangeetha D R, Preeti V Hegde, Prerana N G, Manjunatha Kumar B H "Feedback and Recommendation System using Natural Language
Processing", Vol (2), Dec 2020.

9) Vikas, hassija vinay, chamola dara, nanda gopala krishna, neeraj kumar "A blockchain and edge-computing-based secure framework for government tender allocation" IEEE, 2020

10) Fursan Thabit, Associate Prof Sharaf Alhomdy, Abdulrazzaq H.A.Al-Ahdal Prof Dr Sudhir Jagtap Jagtap "A new lightweight cryptographic algorithm for enhancing data security in cloud computing" Global Transitions Proceedings, Vol 2, 2021.

11) Logith S, Nitish P S, Raghul S, Tamilarasan T "Secure framework for government tender allocation using blockchain" - International Research Journal of Modernization in Engineering Technology and Science, Vol 4, June 2022.

12) Kanchan Singh, Sakshi S Grover, Ranjini Kishen Kumar, "Cyber security vulnerability detection using natural language processing" IEEE,2022.

13) Santosh K, Behera Mitali M Nayak, " Natural language processing for text and speech processing: a review paper" International Journal of Advanced Research in Engineering and Technology (IJARET) 2020.

14) Meilin Wang, "Application Research of Data Encryption Technology in ComputerNetwork Information Security", Hindawi, 2022.

15) Bharti Kaushik, Vikas Malik, Vinod Saroha," A Review Paper on Data Encryption and Decryption",ijraset,2023.