WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancing Security and Transparency in Digital Tendering Using Blockchain Technology

Ashwini Gaikwad[1], Ashwini Thube[2], Vijaya Londhe[3], Prof. Rasika Pachhade[4]

[1 2 3] U.G. Student, Department of Computer Engineering, Vishwabharati Academy's Collage of Engineering, Sarola Baddi, Ahmednagar, Maharashtra, India 414201

[4] Associate Professor, Department of Computer Engineering, Vishwabharati Academy's Collage of Engineering, Sarola Baddi, Ahmednagar, Maharashtra, India 414201

ABSTRACT

The tendering procedure is commonly used by businesses and governments to acquire goods or services from producers or service providers. However, e-tendering, the popular mode of procurement, faces security issues. This study proposes the use of blockchain technology, specifically smart contracts built on the Ethereum blockchain, to create a distributed e-tendering system that addresses these security problems. The system aims to provide transparency, decentralization, and security while allowing bidders to monitor portal operations and tender site activities.

Keywords: Blockchain, Fair and Open Tendering Scheme, smart contract, Ethereum, e-tender.

Introduction

The "Online Tender Management System" is an online platform for publishing tenders and providing information about products, requirements, and terms. The current methods of tendering, such as newspaper advertisements, are expensive, time-consuming, and lack transparency. This paper proposes an online tendering system that leverages blockchain technology and smart contracts to improve the efficiency, transparency, and security of the tendering process.

Related Work

Several studies have explored the use of blockchain technology in various domains, including e-tendering. Davis discussed the importance of information availability in government records. Ambegaonker proposed the use of blockchain to enhance the security and reliability of tendering processes. Zheng provided an overview of blockchain technology, its architecture, consensus mechanisms, and future trends. Pilkington discussed the principles and applications of blockchain technology. Wang surveyed consensus mechanisms and mining strategy management in blockchain networks. Cachin examined consensus protocols in blockchain. Luu highlighted the need for smarter smart contracts to enhance security. Bhargavan explored the formal verification of smart contracts. Wood presented Ethereum as a decentralized transaction ledger.

Proposed System

The proposed system aims to create a transparent, decentralized, and secure e-tendering framework using blockchain technology and smart contracts. The system architecture involves the use of encryption algorithms like AES for data security. The system also utilizes the MD5 message-digest algorithm for data integrity verification. Experimental results demonstrate the feasibility and performance of the proposed system.

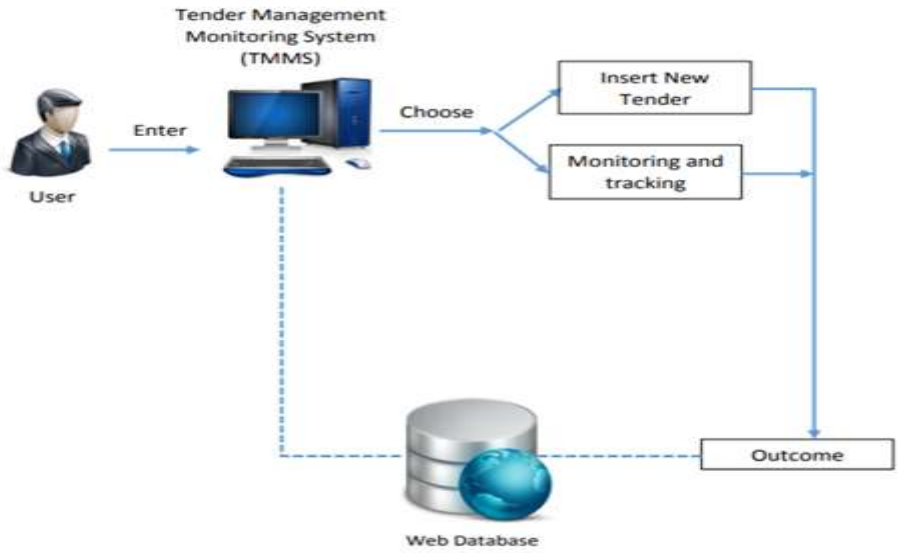

Figure 1. System Architecture

Monitoring the progression of every tender is another important aspect that contribute to the development of this system. Current way of monitoring the progression of the tender is not efficient and can be improved.

Algorithm

AES Algorithm for Encryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round:10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

Cipher text (128 bit)

MD5(Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Steps:

A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.

The output of a message digest is considered as a digital signature of the input data.

MD5 is a message digest algorithm producing 128 bits of data.

It uses constants derived to trigonometric Sine function.

It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.

Most modern programming languages provides MD5 algorithm as built-in functions

Result and Discussion:

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

Figure 2: overall system execution graph

Conclusion

In conclusion, this paper proposes a decentralized e-tendering system that leverages blockchain technology and smart contracts to address security issues and improve transparency in the tendering process. The system provides a secure and efficient platform for tendering, ensuring transparency, fairness, and accountability. Further research can explore advanced cryptographic techniques and the application of blockchain in other government services.

References

[1] Davis, K. C. (1967). The Information Act: A Preliminary Analysis. The University of Chicago Law Review, 34(4), 761-816.

[2] Ambegaonker, A., Gautam, U., & Rambola, R. K. (2018). Efficient approach for Tendering by introducing Blockchain to maintain Security and Reliability. 2018 4th International Conference on Computing Communication and Automation (ICCCA).

[3] Zheng, Z., et al. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress).

[4] Pilkington, M. (2016). Blockchain technology: Principles and applications. Research handbook on digital transformations.

[5] Wang, W., et al. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7, 22328-22370.

[6] Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873.

[7] Luu, L., et al. (2016). Making smart contracts smarter.