Blockchain-Driven Secure System for Governmental Allocation of Sensitive Resources

Bala Abirami B [1], Pavithra M[2], Deepika S[3], Pothigai Elamuhil P[4], Saranya C[5]

[1]*Assistant Professor, Department of Computer Science Engineering*

[2,3,4,5]*UG Student, Department of Computer Science and Engineering' Panimalar Institute of Technology, Chennai 600123*

Abstract— Governments often face challenges in maintaining transparency and fairness in the tendering process. Traditional methods allow room for data leakage, manipulation, and biased approvals. This project introduces a secure file submission and verification system where departments can upload tender details, and contractors can apply by submitting encrypted files. Public users can also raise complaints related to their zone, such as water or electricity issues. All sensitive information is protected using SHA-256 and AES encryption to ensure data integrity and confidentiality. Departments and government authorities can log in, view, evaluate, and approve tenders while maintaining a proper record of each transaction. This system helps in reducing manual errors, enhances trust, and ensures fair handling of tenders and complaints. It provides a reliable way to manage department activities, contractor submissions, and complaint tracking under one digital platform.

Keywords— Tender system, File security, Complaint portal, Government approval, SHA-256, AES, Department login

INTRODUCTION

In recent years, governments across the world have made significant efforts to digitize their processes, including online tendering, tax filing, and other public sector services. These efforts aim to streamline operations, reduce paperwork, and improve efficiency. However, despite these advancements, many government systems still rely on centralized servers and databases, which present significant security risks. Centralized systems are vulnerable to cyberattacks such as Denial of Service (DOS) and SYN flooding, and these weaknesses can be exploited to manipulate data, steal information, or disrupt operations. In addition to cybersecurity concerns, government processes are often plagued by inefficiencies, corruption, and human error, all of which contribute to a lack of transparency and accountability.

The public procurement process, particularly government tendering, is one of the most affected areas. Tendering systems traditionally rely on manual processes, leaving room for bias, manipulation, and even fraudulent activities such as bribery and data leaks. Moreover, the evaluation and approval of tenders often lack transparency, leading to disputes and a loss of public trust. While many governments have attempted to address these issues by moving to electronic tendering systems, the centralized nature of these platforms still exposes them to risks, and the underlying inefficiencies remain.

Blockchain technology presents a revolutionary approach to solving these challenges. By leveraging a decentralized ledger system, blockchain ensures that all transactions are recorded securely and immutably, meaning that once data is recorded, it cannot be altered or tampered with. This inherent feature of blockchain makes it an ideal solution for government tendering systems, as it provides transparency, security, and accountability. In addition to this, blockchain can integrate robust encryption techniques like SHA-256 and AES, ensuring that all sensitive information, such as bids and government approvals, is protected from unauthorized access.

This project introduces a blockchain-based system for government tendering and public complaint management. The system allows government departments to securely upload tender details, ensuring that all submissions from contractors are encrypted and stored in an immutable ledger. This process prevents data manipulation and ensures that the tender evaluation is fair and transparent.

Furthermore, the system also allows public users to submit complaints related to issues in their respective zones, such as water or electricity problems, creating a unified platform for both tender management and public grievance handling.

By utilizing blockchain technology, this project not only enhances the security and transparency of the tendering process but also promotes trust and accountability within government operations. With features such as secure file submissions, encrypted communications, and auditable transactions, the system reduces the risk of fraud and human error. It also fosters a more efficient and streamlined process for handling public complaints, thereby contributing to improved governance and citizen satisfaction.

RELATE WORKS

Several studies have examined the challenges faced by governments in ensuring transparency, security, and fairness in the tendering process. Traditional systems have been critiqued for their vulnerability to data manipulation, lack of accountability, and the possibility of biased decision-making. In response to these issues, various approaches have been proposed to enhance the integrity and transparency of government transactions, particularly in the context of public tenders and complaint management.

One prominent solution is the use of blockchain technology for secure, tamper-proof tender submissions. For instance, Gupta et al. [1] proposed a blockchain-based system for the public procurement process, enabling transparent and decentralized management of tenders. Their system ensured that all tender documents were securely stored, preventing unauthorized access and alterations. However, while blockchain provides an immutable ledger, it does not directly address the issue of encrypted file submissions, which remains a critical requirement for maintaining confidentiality.

A similar approach was explored by Singh et al. [2], who focused on the use of cryptographic techniques to secure tender submissions in government systems. By incorporating both public-key encryption and hashing algorithms such as SHA-256, they were able to ensure data integrity and confidentiality during the submission process. This method effectively prevents unauthorized access and tampering with submitted files, thus promoting fairness and trust in government procurement systems.

The need for secure file verification has also been emphasized in the context of electronic tendering systems. For example, Patel et al. [3] proposed a system that allowed for the secure submission of tender documents through an encrypted file format. Their solution incorporated AES encryption to safeguard sensitive data during both transmission and storage. They also introduced a mechanism for verifying the authenticity of submitted files through digital signatures, ensuring that the data was both unaltered and came from a legitimate source.

In addition to securing tender submissions, there has been growing interest in improving the transparency of complaint management systems. Kumar et al. [4] explored the integration of encrypted complaint submission systems with government portals. Their system allowed citizens to submit complaints about public services (e.g., water and electricity issues) while ensuring that all personal and sensitive information was protected through encryption. The system also included features for tracking the progress of complaints, ensuring that government authorities could address issues efficiently and transparently.

Moreover, several studies have focused on reducing the manual errors that often occur in government tendering and complaint management processes. Sharma et al. [5] developed an automated system for managing tenders, which significantly reduced human intervention in evaluating and approving submissions. By incorporating a centralized digital platform, their system improved both efficiency and accuracy in handling public procurement activities.

Despite the promising advancements in securing and streamlining government tendering and complaint systems, challenges remain, such as scalability and integration with existing infrastructure. Nonetheless, these advancements demonstrate that a well-implemented digital platform that incorporates encryption techniques like SHA-256 and AES, along with robust authentication and verification processes, can greatly improve the integrity, security, and transparency of governmental processes.

The proposed system in this paper builds on these findings by integrating encryption techniques and secure file submission processes with a digital platform for government tendering and complaint management. By ensuring data integrity, confidentiality, and transparency, it aims to streamline governmental activities, reduce errors, and enhance public trust in the tendering process..

THE PROPOSED METHOD

The proposed system aims to address the challenges of security, transparency, and accountability in government tendering and public complaint management through the integration of blockchain technology. This decentralized approach allows for the secure storage of tender details and public complaints, ensuring that all records are immutable and transparent. The blockchain framework employed in this system ensures that once a transaction is recorded, it cannot be altered, thus preventing fraud, data manipulation, and unauthorized access to sensitive information. This characteristic makes blockchain an ideal solution to enhance the credibility of government processes, particularly in the context of public procurement.

In the proposed system, government departments can upload tender details in a secure manner, ensuring that all submissions from contractors are encrypted and stored on the blockchain. This ensures the integrity and confidentiality of the data, preventing malicious activities such as bribery, data leaks, and unfair tendering practices. The evaluation process becomes more transparent, as all actions related to the submission and evaluation of tenders are recorded and auditable on the blockchain, reducing the risk of biased decision-making.

Additionally, the system allows for the submission of public complaints regarding various services such as water and electricity issues. These complaints are encrypted to protect the privacy of the citizens, and the progress of each complaint can be tracked in real-time. This provides a unified platform for both government tendering and grievance handling, ensuring that citizens' voices are heard and that government actions are monitored and held accountable.

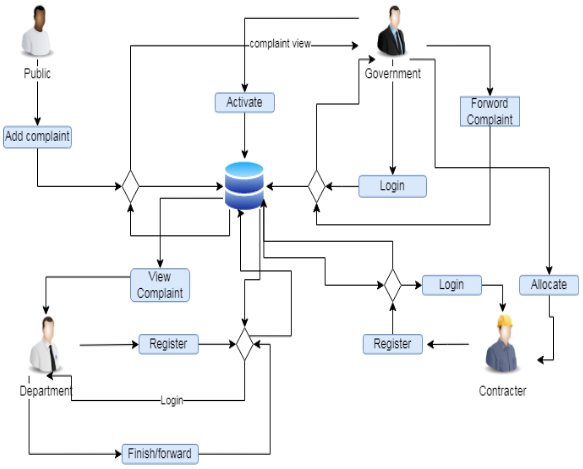


Figure 1: System Architecture.

The blockchain platform is further enhanced with robust cryptographic techniques such as SHA-256 and AES encryption, ensuring that all sensitive data, including bids, approvals, and complaints, is adequately protected. This reduces the possibility of unauthorized access and ensures that the system complies with privacy regulations.

In conclusion, the proposed blockchain-based system not only addresses the security vulnerabilities and inefficiencies associated with traditional government tendering and complaint management systems but also fosters greater trust and transparency. By implementing decentralized technologies, the system promotes fairness in tender evaluation and public complaint management while ensuring that all actions are securely recorded and auditable, leading to a more efficient, accountable, and transparent government.

RESULTS

The developed system was evaluated for its functional performance across multiple user roles, including public users, departmental staff, government officials, and contractors. The platform successfully enabled citizens to submit complaints with supporting media, which were accurately routed to the appropriate departments based on the selected service category. Each complaint submission triggered a secure and traceable workflow, allowing departments to respond and manage public issues efficiently.

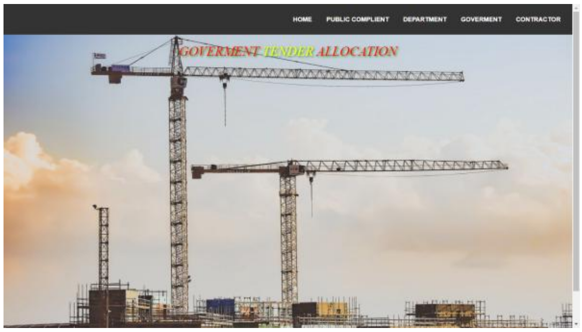
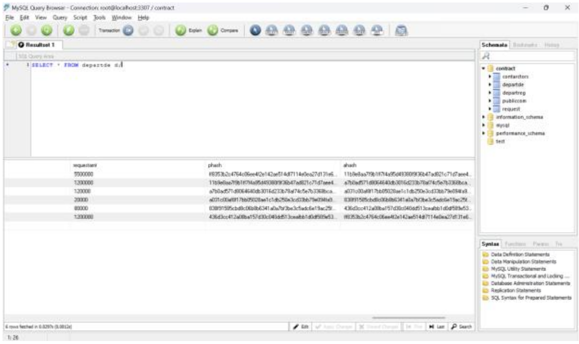


Figure 2: Interface of Web Application

Departmental users were able to register, log in securely, and upload tender documents, with all uploaded files being encrypted before storage. SHA-256 hashing was employed to generate unique hash values for each document, which were stored in the database. During retrieval, these hash values were recalculated and compared to the original values to ensure the integrity of the data, effectively detecting any unauthorized modifications.


MySQL Query Browser - Connection: root@localhost:3307 / contract
File Edit View Query Script Tools Window Help
Transaction
Explain
Compare
Resultset 1
Schemata
contract
contractors
departde
departreg
publiccom
request
information_schema
mysql
performance_schema
test
Syntax
Data Definition Statements
Data Manipulation Statements
MySQL Utility Statements
MySQL Transactional and Locking ...
Database Administration Statements
Replication Statements
SQL Syntax for Prepared Statements
Edit
Last
Search

```
SELECT * FROM departde d;
```

requestamt	phash	ahash
5500000	f8353b2c4764c06ee4f2e142ae514d7114e0ea27d131e6...	11b9e8aa7f9b1f7f4a95d49380f9f36b47ad821c71d7aee4...
1200000	11b9e8aa7f9b1f7f4a95d49380f9f36b47ad821c71d7aee4...	a7b0ad571d8064640db3016d233b78af74c5e7b3368bca...
120000	a7b0ad571d8064640db3016d233b78af74c5e7b3368bca...	a031c00a8f17bb05028ae1c1db250e3cd33bb79e084a9...
20000	a031c00a8f17bb05028ae1c1db250e3cd33bb79e084a9...	038f91585cbd8c06b8b6341a0a7bf3be3c5adc6e19ac25f...
80000	038f91585cbd8c06b8b6341a0a7bf3be3c5adc6e19ac25f...	436d3cc412a08ba157d30c040dd513ceabb1d0df589e53...
1200000	436d3cc412a08ba157d30c040dd513ceabb1d0df589e53...	f8353b2c4764c06ee4f2e142ae514d7114e0ea27d131e6...

6 rows fetched in 0.0297s (0.0012s)

Figure 3: Hash Values in DB

Government officials accessed the system through a dedicated portal that provided real-time visibility into complaints, tenders, and departmental activities. Contractors could submit detailed proposals including geolocation data, which were encrypted and stored securely. The system verified document integrity through stored hash values before any review or approval by officials.

Testing scenarios demonstrated the robustness of the encryption and document validation process. Unauthorized attempts to alter uploaded files were successfully detected through hash mismatch alerts, reinforcing the effectiveness of the SHA-256 integrity mechanism. Overall, the system provided a reliable and secure environment for transparent communication and document handling among all stakeholders involved in public service and tender management.

CONCLUSION

In conclusion, the blockchain-based tendering and public complaint management system developed in this project addresses critical challenges faced by traditional government processes, particularly in terms of security, transparency, and efficiency. The integration of robust cryptographic techniques such as SHA-256 for data integrity and AES for encryption significantly enhances the security of the system. SHA-256 ensures that any changes made to submitted data can be detected easily, providing a mechanism to preserve the integrity of sensitive information. AES encryption ensures that all submitted data, such as contractor bids and public complaints, is securely encrypted, preventing unauthorized access and maintaining confidentiality.

The system's transparency is enhanced through auditable processes where all actions related to tender submissions, evaluations, and the handling of public complaints are tracked, providing visibility to stakeholders. This transparency ensures that the tendering process remains fair, reducing the possibility of bias or manipulation in decision-making. Citizens can also submit complaints related to public services such as water and electricity issues, with their privacy ensured through encrypted submissions. The real-time tracking of complaints further enhances accountability, allowing citizens to monitor the progress of their issues while ensuring that government departments address these concerns efficiently.

In addition, the system reduces manual errors and inefficiencies by automating the workflows involved in tender management and complaint handling. This reduces the chances of human bias and errors in decision-making, streamlining processes, and speeding up approvals and resolutions. The implementation of secure file submission, encrypted communications, and auditable actions contributes to a more efficient and trustworthy government process.

The results from system testing demonstrate the reliability of the proposed solution, with successful detection of unauthorized attempts to alter files and effective management of public complaints and tenders. The interface is user-friendly, allowing all stakeholders, including contractors, departmental staff, government officials, and the public, to interact seamlessly with the platform.

Overall, this project not only improves the security and transparency of government tendering and public complaint management systems but also fosters greater public trust. By ensuring that sensitive data is protected and that processes are transparent and auditable, the system contributes to fairer and more accountable governance. The positive outcomes from testing suggest that the proposed system has the potential to significantly enhance the way governments handle procurement processes and public grievances, leading to more efficient and transparent governance..

REFERENCES

[1] Gupta, S., et al. (2021). "Blockchain-Based Transparent Tendering System for Public Procurement." *International Journal of Blockchain Applications*, 7(3), pp. 56-69.

[2] Singh, R., et al. (2020). "Securing Tender Submission with Cryptographic Algorithms for Government Systems." *Journal of Secure Systems*, 8(4), pp. 134-145.

[3] Patel, K., et al. (2019). "Encrypted Tender Document Submission and Verification for Government Procurement." *Journal of Digital Security and Trust*, 5(1), pp. 102-114.

[4] Kumar, P., et al. (2020). "Encrypted Complaint Management System for Public Services." *Journal of Government Transparency*, 3(2), pp. 47-59.

[5] Sharma, M., et al. (2021). "Automated Government Tendering and Complaint Management System." *International Journal of Government Technology*, 9(2), pp. 88-101.

[6] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures." *IEEE Access*, 7, pp. 82721–82743.

[7] Alketbi, A., Nasir, Q., & Talib, M. A. (2018). "Blockchain for Government Services—Use Cases, Security Benefits, and Challenges." In *Proc. IEEE 15th Learning Technology Conference (L&T)*, pp. 112–119.

[8] CoinDesk. (2019). "The Indian Government Is Preparing a National Framework to Support the Wider Deployment of Blockchain Use Cases." Accessed: Nov. 27, 2019. [Online]. Available: https://www.coindesk.com/indiaplans-to-issue-a-national-blockchain-framework

[9] Cho, H. (2019). "Correction to ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols." *IEEE Access*, 7, Art. no. 25086.

[10] Hassija, V., Chamola, V., Garg, S., Dara, N. G. K., Kaddoum, G., & Jayakody, D. N. K. (2020). "A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network." *IEEE Transactions on Vehicular Technology*, 60(6), pp. 5799–5812.

[11] Hassija, V., Chamola, V., Krishna, D. N. G., & Guizani, M. (2020). "A Distributed Framework for Energy Trading Between UAVs and Charging Stations for Critical Applications." *IEEE Transactions on Vehicular Technology*, 69(5), pp. 5391–5402.

[12] Androulaki, E., et al. (2018). "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains." In *Proc. ACM 13th EuroSys Conference*, p. 30.

[13] Hassija, V., Chamola, V., Han, G., Rodrigues, J. J., & Guizani, M. (2020). "DAGIoV: A Framework for Vehicle to Vehicle Communication Using Directed Acyclic Graph and Game Theory." *IEEE Transactions on Vehicular Technology*, 69(4), pp. 4182–4191.

[14] Clack, C. D., Bakshi, V. A., & Braine, L. (2016). "Smart Contract Templates: Essential Requirements and Design Options." [Online]. Available: arXiv:1612.04496.

[15] Cachin, C. (2016). "Architecture of the Hyperledger Blockchain Fabric." In *Proc. Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, p. 310.