

A Blockchain and Edge-Computing-Based Secure Framework for Government Tender Allocation

Dr. J. Jospin Jeya¹, V. Casbro², S. Logeshwaran³, J. Jenish galarance⁴

¹Assistant Professor, Department of Computer Science and Engineering, Jeppiaar Engineering college, Chennai, Tamil Nadu, India

^{2,3,4} Computer Science and Engineering Department, Jeppiaar Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

Governments and public sector entities around the world are actively exploring new ways to keep up with technological advancements to achieve smart governance, work efficiency, and cost optimization. Blockchain technology is an example of such technology that has been attracting the attention of Governments across the globe in recent years. Enhanced security, improved traceability, and lowest cost infrastructure empower the blockchain to penetrate various domains. Generally, gov- elements release tenders to some third-party organizations for different projects. During this process, different competitors try to eavesdrop on the tender values of others to win the tender. The corrupt government officials also charge high bribe to pass the tender in favor of some particular third party. In this article we presented a secure and transparent framework for government tenders using blockchain. Blockchain is used as a secure and immutable data structure to store the government records that are highly susceptible to tampering. This work aims to create a transparent and secure edge computing infrastructure for the workflow in government tenders to implement government schemes and policies by limiting human supervision to the minimal.

Keywords—Blockchain, digital signatures, distributed ledger technology, Edge computing, Ethereum, proof of work, smart contracts.

Article Info

Volume 9, Issue 3

Page Number : 281-290

Publication Issue

May-June-2022

Article History

Accepted : 10 May 2022

Published : 30 May 2022

I. INTRODUCTION

There have been various attempts to implement the technology to make government processes paperless and instantaneous, such as online ticketing systems, online issuing of tenders, filing tax returns, etc. Although most of these systems seem robust and well

implemented, all of them are based on the idea of a central server that has a single point of failure, as hackers can easily hack or disrupt its functioning by attacks, such as DOS, Slow-loris, SYN Flooding, etc. In most governments, complicated bureaucratic systems often result in highly inefficient workflow fraught with corruption, mismanagement, and human

errors. Some of the governance processes, such as government tenders include malpractices like information leaks, corruption, bribery, etc. Most of the existing electronic services and IT infrastructure have the above-mentioned limitations, however, new technologies, such as blockchain have the potential to greatly ameliorate the existing problems. A permissioned blockchain network can provide the necessary transparency to effectively implement government policies for the benefit of the citizens of the country and fix responsibilities in case of abuse of the system.

II. LITERATURE SURVEY

Proof-of-PUF Enabled Block chain: Concurrent Data and Device Security for Internet-of-Energy

A detailed review on the technological aspects of Blockchain and Physical Unclonable Functions (PUFs) is presented in this article. It stipulates an emerging concept of Blockchain that integrates hardware security primitives via PUFs to solve bandwidth, integration, scalability, latency, and energy requirements for the Internet-of-Energy (IoE) systems. This hybrid approach, hereinafter termed as PUF Chain, provides device and data provenance which records data origins, history of data generation and processing, and clone-proof device identification and authentication, thus possible to track the sources and reasons of any cyberattack. In addition to this, we review the key areas of design, development, and implementation, which will give us the insight on seamless integration with legacy IoE systems, reliability, cyber resilience, and future research challenges

Blockchain and Edge Computing-based Secure Framework for Government Tender Allocation

Governments and public sector entities around the world are actively exploring new ways to keep up

with technological advancements to achieve smart governance, work efficiency, and cost optimization. Block chain technology is an example of such technology that has been attracting the attention of Governments across the globe in recent years. Enhanced security, improved traceability and lowest cost infrastructure empower the block chain to penetrate various domains. Generally, governments release tenders to some third-party organizations for different projects. During this process, different competitors try to eavesdrop on the tender values of others to win the tender. The corrupt government officials also charge high bribes to pass the tender in favor of some particular third party. In this paper, we presented a secure and transparent framework for government tenders using block chain. Block chain is used as a secure and immutable data structure to store the government records that are highly susceptible to tampering. This work aims to create a transparent and secure edge computing infrastructure for the workflow in government tenders to implement government schemes and policies by limiting human supervision to the minimum.

A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures

The Internet of Things (IoT) is the next era of communication. Using the IoT, physical objects can be empowered to create, receive, and exchange data in a seamless manner. Various IoT applications focus on automating different tasks and are trying to empower the inanimate physical objects to act without any human intervention. The existing and upcoming IoT applications are highly promising to increase the level of comfort, efficiency, and automation for the users. To be able to implement such a world in an ever glowing fashion requires high security, privacy, authentication, and recovery from attacks. In this regard, it is imperative to make the required changes in the architecture of the IoT applications for achieving end-to-end secure IoT

environments. In this paper, a detailed review of the security-related challenges and sources of threat in the IoT applications is presented. After discussing the security issues, various emerging and existing technologies focused on achieving a high degree of trust in the IoT applications are discussed. Four different technologies, blockchain, fog computing, edge computing, and machine learning, to increase the level of security in IoT are discussed.

A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures

The Internet of Things (IoT) is the next era of communication. Using the IoT, physical objects can be empowered to create, receive, and exchange data in a seamless manner. Various IoT applications focus on automating different tasks and are trying to empower the inanimate physical objects to act without any human intervention. The existing and upcoming IoT applications are highly promising to increase the level of comfort, efficiency, and automation for the users. To be able to implement such a world in an ever-growing fashion requires high security, privacy, authentication, and recovery from attacks. In this regard, it is imperative to make the required changes in the architecture of the IoT applications for achieving end-to-end secure IoT environments. In this paper, a detailed review of the security-related challenges and sources of threat in the IoT applications is presented. After discussing the security issues, various emerging and existing technologies focused on achieving a high degree of trust in the IoT applications are discussed. Four different technologies, blockchain, fog computing, edge computing, and machine learning, to increase the level of security in IoT are discussed.

Block chain for government services-Use cases, security benefits and challenges

Public sector and governments have been actively exploring new technologies to enable the smart services transformation and to achieve strategic objectives such as citizens satisfaction and happiness, services efficiency and cost optimization. Blockchain technology is a good example of an emerging technology that is attracting government attention. Many government entities such as the United Kingdom, Estonia, Honduras, Denmark, Australia, Singapore and others have taken steps to unleash the potential of Block chain technology. Dubai Government is aiming to become paperless by adopting the Block chain technology for all transactions by 2021. The Block chain is a disruptive technology that is playing a vital role in many sectors. It's a revolutionary technology transforming the way we think about trust as it enables transacting data in a decentralized structure without the need to have trusted central authorities. Block chain technology promises to overcome security challenges in IoT enabled services such as enabling secure data sharing and data integrity. However, it also introduces new security challenges that should be investigated and tackled. In this paper, we review the literature to identify the potential use cases and application of Block chain to enable government services. We also synthesized literature related to the security of Block chain implementations to identify the security benefits, challenges and the proposed solutions. The analysis shows that there is huge potential for Block chain technology to be used to enable smart government services. This paper also highlights future research in the areas of concerns that required further investigation.

III. IMPLEMENTATION

EXISTING SYSTEM

Some of the governance processes, such as government tenders include malpractices like information leaks, corruption, bribery, etc. Most of

the existing electronic services and IT infrastructure have some limitations and ECDSA algorithm is used

IV. SYSTEM ARCHITECTURE

The systems architect establishes the basic structure of the system, we propose a Hash code Solomon algorithm. We can put a small part of data in local machines and fog servers in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is really a powerful supplement to the existing cloud storage scheme.

Our architecture work flow diagram is given below.

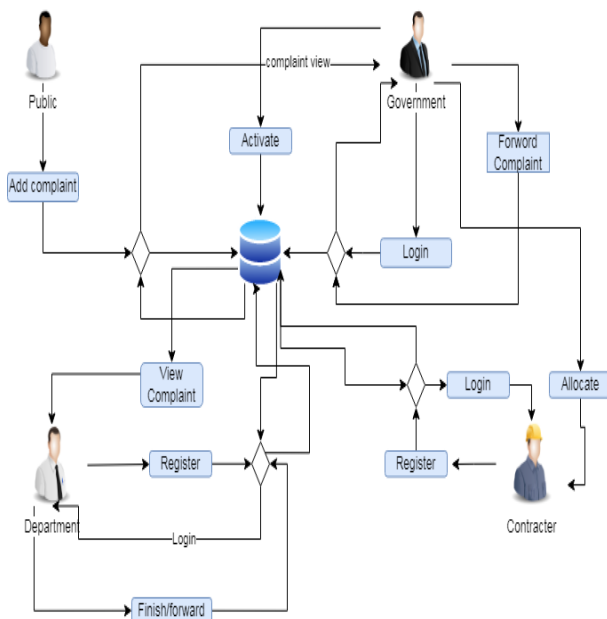


Fig. 1. Architecture diagram

ALGORITHM USED:

SHA ALGORITHM:

In the field of cryptography and crypt analytics, the SHA-1 algorithm is a crypt-formatted hash function that is used to take a smaller input and produces a

string that is 160 bits, also known as 20-byte hash value long.

The hash value therefore generated, is known as a message digest which is typically rendered and produced as a hexadecimal number which is specifically 40 digits long.

Uses of SHA Algorithm:

These SHA algorithms are widely used in security protocols and applications, including the ones such as TLS, PGP, SSL, IPsec, and S/MIME. These also find their place in all the majority of cryptanalytic techniques and coding standards which is mainly aimed to see the functioning and working of majorly all governmental as well as private organizations and institutions.

Major giants today such as Google, Microsoft, or Mozilla have started to recommend the use of SHA-3 and stop the usage of the SHA-1 algorithm.

BASIC CONCEPT OF SECURE HASH GENERATION:

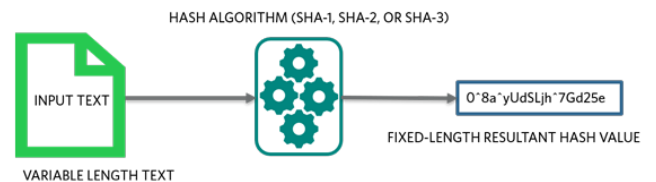


Fig. 2. Hash key generation diagram

V. SYSTEM REQUIREMENTS

SOFTWARE REQUIREMENTS:

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the team's and tracking the team's progress throughout the development activity.

Front End : J2EE(JSP,SERVLETS)
 JAVASCRIPT
 Back End : MY SQL 5.5
 Operating System : Windows 07
 IDE : Eclipse

HARDWARE REQUIREMENTS:

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the system does and not how it should be implemented.

PROCESSOR : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.
 RAM : 4GB DDR RAM
 MONITOR : 15" COLOR
 HARD DISK : 40 GB

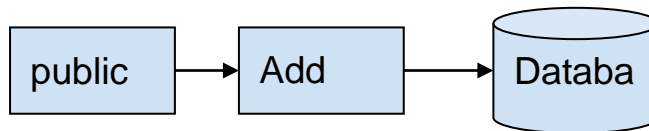
VI. PROPOSED SYSTEM

A permissioned block chain network can provide the necessary transparency to effectively implement government policies for the benefit of the citizens of the country and fix responsibilities in case of abuse of the system and SHA algorithm is used

MODULE EXPLANATION:

1.PUBLIC COMPLAINT:

In this module in our project, here symbolizes a unit of work performed within a database management system. Public add complaint something about some issues about his/her area or zone such as water department issue, Electricity related issue with the picture of that.



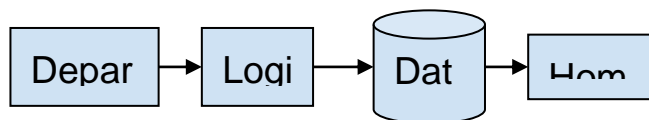
2.DEPARTMENT REGISTER:

The register module provides a conceptual framework for entering data on those department in a way that: easeus data entry & accuracy by matching the department entry to the data source (usually paper files created at point of care), ties easily back to individual department records to connect registers to department data, and collects data elements to enable better supervision of tender programs.



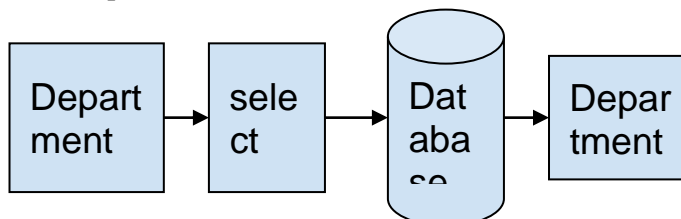
VII. DEPARTMENT LOGIN

In this module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to the provider.



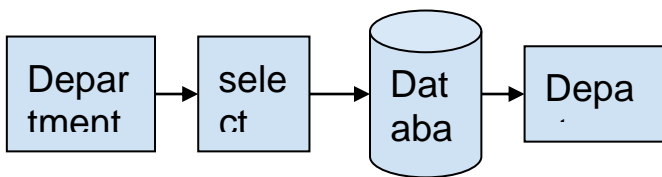
4. SELECT DEPARTMENT:

In this module in our project, here the department is needed to select the department like construction or some department for the tender allocation.



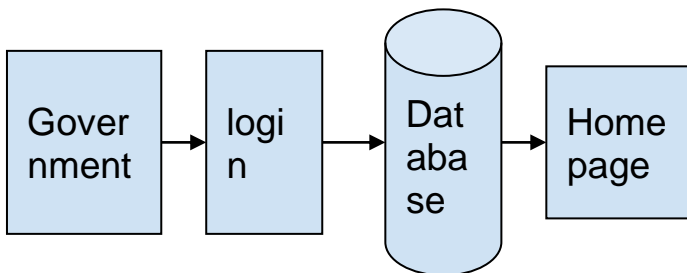
5. DEPARTMENT UPLOAD

The register module provides a conceptual framework for uploading data on those department in a way that: easeus data entry & accuracy by matching the department entry to the data source (usually paper files created at point of care), ties easily back to individual department records to connect registers to department data, and collects data elements to enable better supervision of donation programs.



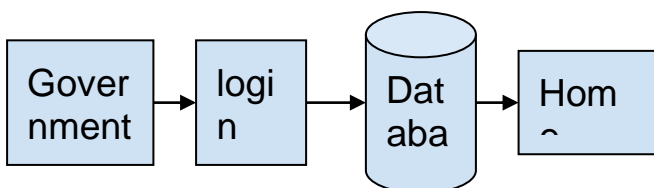
VIII. GOVERNMENT LOGIN

In this module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database users will transfer the amount to the provider.



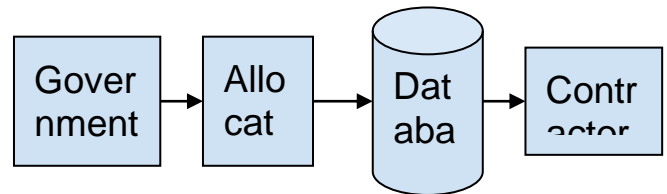
7.GOVERNMENT VIEW

In this module the government will also view the contractor. And analysis the details will be responsible for your file stored in the database.



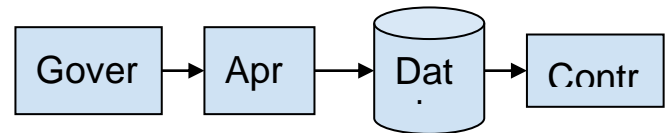
8.GOVERNMENT TENDER ALLOCATION:

In this module the government will allocate the tender for the government project. Analysis of the details will be responsible for your file stored in the database.



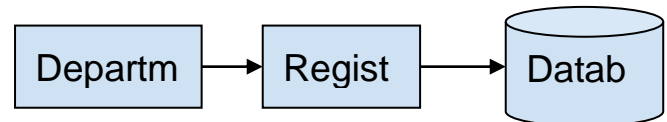
9.GOVERNMENT APPROVE:

This module is used to help the contractor to request the tender with the land longitude and the contractor will update the report along with their opinion and it will be stored in the database.



10.CONTRACTOR REGISTER:

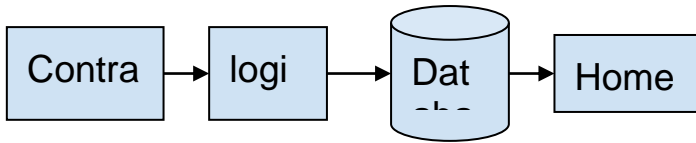
The register module provides a conceptual framework for entering data on the contractor in a way that: eases data entry & accuracy by matching the contractor entry to the data source (usually paper files created at point of care), ties easily back to individual charity records to connect registers to contractor data, and collects data elements to enable better supervision of tender programs.



11.CONTRACTOR LOGIN:

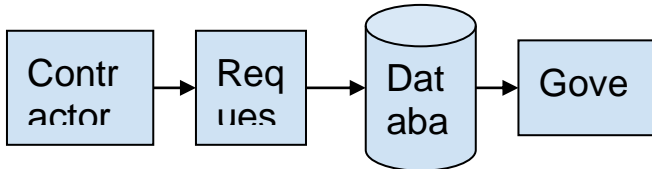
In this module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents

any change in database user will transfer the amount to the provider.



12.CONTRACTOR TENDER REQUEST:

In this module the contractor will also view the request. And analysis the details will be responsible for your file stored in the database.



13.CONTRACTOR APPOINTMENT:

This module is used to help the contractor to request the tender with the appointment by the government and the contractor will update the report along with their opinion and it will be stored in the database.



IX. FUTURE ENHANCEMENTS

- 1.Implementing a real-world database system for government projects.
2. Improving the efficiency of protocols, in terms of number of tenders exchanged and in terms, as well.
3. Implement using two more algorithms.

X. RESULT AND CONCLUSION

In this article, we have discussed the need and benefits of using block chain technology in the government tender assignment process. We have used to implement the end-to-end edge computing framework for a government tender Workflow.

The SHA algorithm is proposed to associate the best-suited constructors to the tender projects, thereby

enhancing the profit of both the government Tenders and the construction companies.

We have also studied the performance evaluation of the proposed model. The proposed model proves to give better results in terms of different tender parameters as compared to its counterparts.

Output:

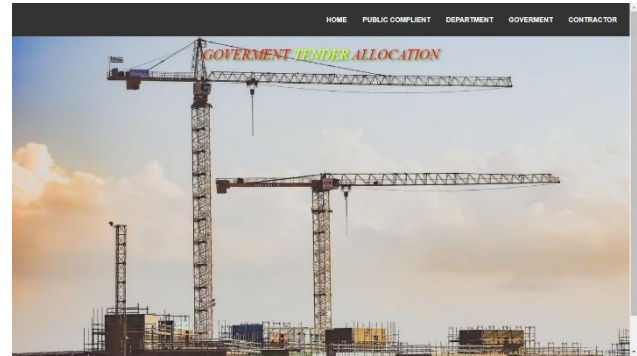


Figure 1: SNAPSHOTS: Home page

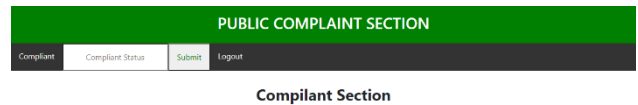


Figure 2: Public Complaint Page

Figure 3: Complaint Form



Figure 4: Department Login Page:



Figure 8: Government Main page



Figure 5: Department Register Page

DEPARTMENT	DATE	ZONE	COMPLAIN	COMPLAIN STREET	REPORT	ENSR
WATER.MANAGEMENT	2022-02-02	TONDICARPET	pls supply drinking water	12 th street tondicarpet	VIEW	Done

Figure 9: Complaint Status Page

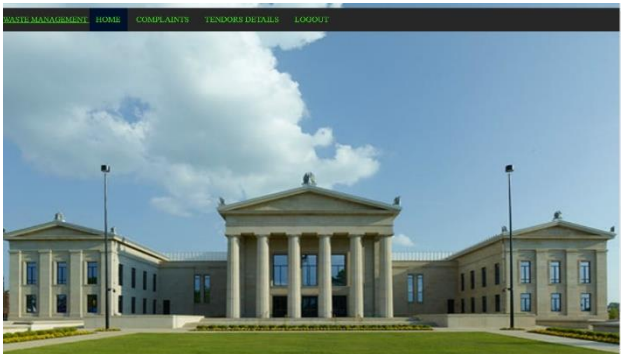


Figure 6: Department Main Page:

HOME	COMPANY NAME	EMAIL	COMPANY NUMBER	KYC	STATUS	VIEW	ACTIVATE
PUBLIC COMPLAINT	jk construction	jk@gmail.com	7900897089	sample.pdf	Activate	VIEW	ACTIVATE
COMPLAIN STATUS	abb corporation	abb@gmail.com	8908908907	sample (3).pdf	Activate	VIEW	ACTIVATE
ACTIVATE	bb corporation	bb@gmail.com	9087908790	Dilation, Erosion, Opening and Closing.txt	Activate	VIEW	ACTIVATE
DEPART STATUS							
RESPONSE							
TENDORS DETAILS							
LOGOUT							

Figure 10: Construction Activate Page

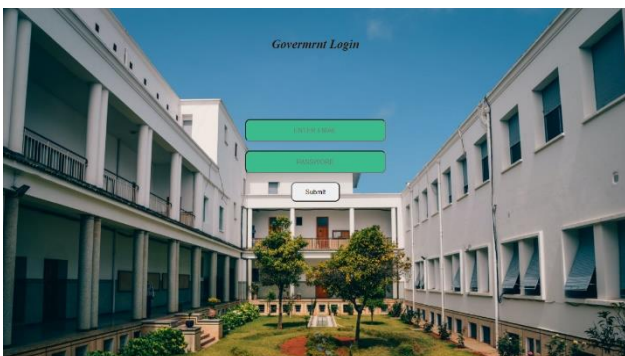


Figure 7: Government Login Page:

Zone	Address	Department	Company Name	Project Details	Duration	Allocate Date	Total Cost
THIRUVOTRIYUR	Gandhi Nagar	WATER.MANAGEMENT	abb corporation	Erk.txt	6 months	2022-02-02T17:49	1100000
MANALI	12 th street tondicarpet	ROAD SECTOR	abb corporation	Dilation, Erosion, Opening and Closing.txt	3 months	2022-02-02T17:58	1300000
PERUNGUDI	2nd street oranganje	WATER.MANAGEMENT	jk construction	Edge Detection & Image Grayscale.txt	3 months	2022-02-02T18:04	90000
TONDICARPET	1 st tondicarpet questru	ROAD SECTOR	bb corporation	sample.pdf	3 months	2022-02-04T17:35	1100000

Figure 11: Tendors Details

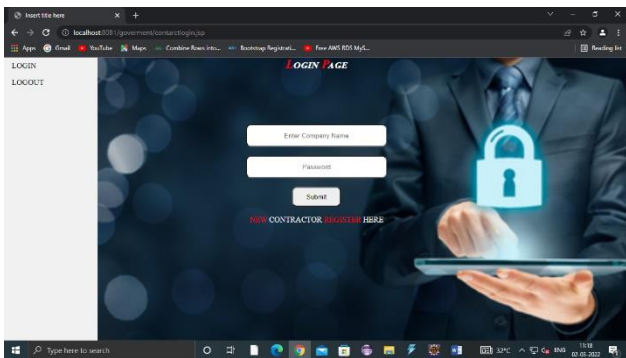


Figure 11: Contractor Login Page



Figure 12: Contractor Main Page

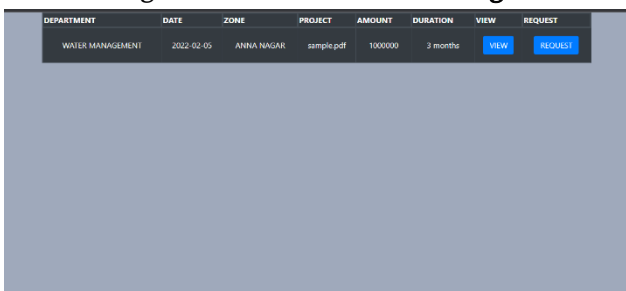


Figure 13: Contract View:

bb corporation Back

Zone	Address	Department	Project Details	Duration	Allocate Date	Total Cost
TONDHARPET	1 st tondharpet quarters	ROAD SECTOR	sample.pdf	3 months	2022-02-04T17:35	1100000

Figure 14: Confirmation View

XI. REFERENCES

- [1]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
- [2]. A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in *Proc. IEEE 15th Learn. Technol. Conf. (L&T)*, 2018, pp. 112–119.
- [3]. coindesk. 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>
- [4]. H. Cho, "Correction to asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," *IEEE Access*, vol. 7, 2019, Art. no. 25086.
- [5]. V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 60, no. 6, pp. 5799–5812, Jun. 2020.
- [6]. V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations for critical applications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5391–5402, May 2020.
- [7]. E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. ACM 13th EuroSys Conf.*, 2018, p. 30.
- [8]. V. Hassija, V. Chamola, G. Han, J. J. Rodrigues, and M. Guizani, "DAGIoV: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE*

Trans. Veh. Technol., vol. 69, no. 4, pp. 4182–4191, Jan. 2020.

- [9]. C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: Essential requirements and design options," 2016. Online]. Available: arXiv:1612.04496.
- [10]. C. Cachin, "Architecture of the hyperledger blockchain fabric," in Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers, 2016, p. 310.
- [11]. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)
- [12]. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [13]. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
- [14]. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 Digests 9th Annual Conf. Magnetism Japan, p. 301, 1982].
- [15]. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989

Cite this article as :

Dr. J. Jospin Jeya, V. Casbro, S. Logeshwaran, J. Jenish Galarance, "A Blockchain and Edge-Computing-Based Secure Framework for Government Tender Allocation", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 3, pp. 281-290, May-June 2022.

Journal URL : <https://ijsrst.com/IJSRST229352>