iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52162

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

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

B. Dilly Babu[1], GB. Karthikeyan K[2], Anitha[3]
G.K.M College of Engineering and Technology

Abstract: ***Block chain innovation is an illustration of such innovation that has been drawing in the consideration of Legislatures across the globe as of late. Upgraded security, further developed detectability, and least expense foundation engage the block chain to infiltrate different spaces. By and large, legislatures discharge tenders to some outsider associations for various tasks. During this interaction, various contenders attempt to snoop the delicate upsides of others to win the delicate. Block chain procedure utilized under different security administration with various model. It is utilized as backend data set model that keeps up with. No. of clients can enlist and make the delicate citation under different division. Administrator will check and give the reaction from the citation result. Administrator or authority check the experience and interaction the board level ability for universally useful.***

I. INTRODUCTION

There have been different endeavours to carry out the innovation to make government processes paperless and quick, for example, internet tagging frameworks, web-based giving of tenders, recording government forms, and so on. Albeit the greater part of these frameworks appears to be vigorous and very much executed, every one of them depend on the possibility of a focal server that has a weak link, as programmers can undoubtedly hack or disturb its working by assaults, like DOS, Slow-loris, SYN Flooding, and so forth. In many states, muddled administrative frameworks frequently bring about exceptionally wasteful work process loaded with defilement, botch, and human mistakes. A portion of the administration processes, for example, government tenders incorporate misbehaviours like data spills, defilement, pay off, and so on. The vast majority of the current electronic administrations and IT framework have the previously mentioned constraints, in any case, new advancements, for example, blockchain can possibly extraordinarily improve the current issues. A permissioned blockchain organization can give the fundamental straightforwardness to execute government strategies to support the residents of the nation and fix liabilities in the event of maltreatment of the framework really.

Blockchain technology is a highly promising solution that can be employed in the government tender process to enhance the level of security, privacy, transparency, and speed of work. Blockchain can allow all the parties involved in a particular tender to be a part of the same network and to monitor the workflow step by step . Governments like Georgia, U.K., UAE, Australia, China, Japan, and Russia are currently progressing at a rapid pace in adapting blockchain in their day to day functioning. The government of Dubai has an ambitious plan of becoming completely paperless through the widespread implementation of blockchain technology . Governments of several developing countries like India have also been promoting various projects and policies for adaptation of blockchain technology in recent years

In the current digital space, data manipulation is one of the most important tools that is being used by all the adversaries and malicious entities to cause harm to the public and the government bodies . Most of the existing systems rely on the data and if the data itself is far given correlated or misreported, then the complete system becomes corrupt. The shift from storing data in physical files to storing data in digital form is a paradigm shift [10].

However, if the digital data is not secure, then the harm caused by the loss of digital data would be much more than the harm that was faced due to the loss of physical files [11]. According to 2019 statistics, there are more than 130 large-scale targeted data breaches in the U.S. per year, and that number is growing by around 27% per year. Digital identity theft is one of the major sources of data breaches.

It is estimated that 74% of the data breaches are caused by identity thefts across the world. The United States leads other countries with almost 85% of digital identities stolen worldwide . Apart from data breaches, bribery and unnecessary delays in the processes is another issue being specifically faced in government processes. Government officials tend to misuse their bureaucratic powers and demand high bribes to pass the tenders.

II. LITTERATURE SURVEY

TITLE: Proof-of-PUF Enabled Block chain:
Concurrent Data and Device Security for Internet-of-Energy AUTHOR: Rameez Asif, Kinan Ghanem and James Irvine YEAR: 2020 PAPER
EXPLANATION: 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 PUFChain, 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.

TITLE: A Blockchain and Edge Computing-based Secure Framework for Government Tender Allocation AUTHOR:
Vikas Hassija, Vinay Chamola, Senior Member, IEEE, Dara Nanda Gopala Krishna, Neeraj Kumar.
YEAR: 2020 PAPER EXPLANATION: 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 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 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 minimal.

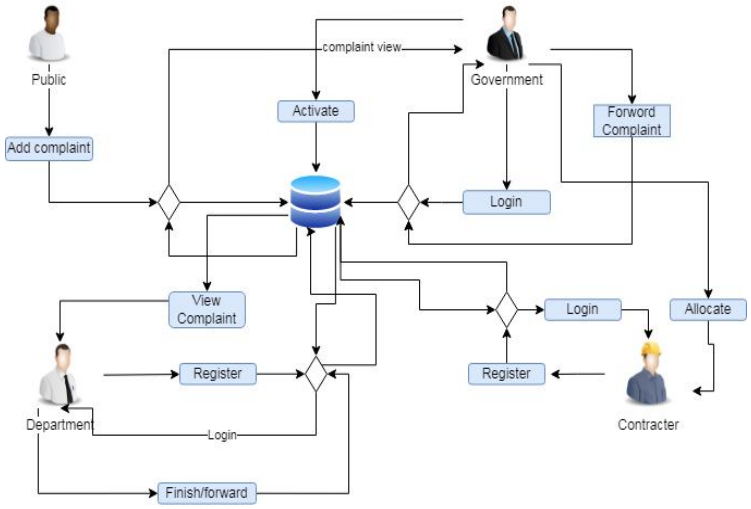
TITLE: A Survey on IoT Security:
Application Areas, Security Threats, and Solution Architectures
AUTHOR: VIKAS HASSIJA, VINAY CHAMOLA, VIKAS SAXENA, DIVYANSH JAIN, PRANAV GOYAL, AND BIPLAB SIKDAR. YEAR: 2019 PAPER
EXPLANATION:
The Internet of Things (IoT) is the next era of communication. Using the IoT, 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, ef_ciency, and automation for the users. To be able to implement such a world in an evergrowing 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.

TITLE: Block chain for government services-Use cases, security benefits and challenges
AUTHOR: Ahmed Alketbi; Qassim Nasir; Manar Abu Talib
YEAR: 2018 PAPER EXPLANATION 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. The Blockchain technology is a good example of an emerging technology that is attracting government attention. Many government entities such as 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.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

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 is huge potential for Block chain technology to be used in to enable smart government services. This paper also highlights future research in the areas of concerns that required further investigation

III.METHODOLOGY



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.

A. Characteristics

1) The cryptographic hash functions are utilized and used to keep and store the secured form of data by providing three different kinds of characteristics such as pre-image resistance, which is also known as the first level of image resistance, the second level of pre-image resistance and collision resistance.

2) The cornerstone lies in the fact that the pre-image crypt resistance technique makes it hard and more time consuming for the hacker or the attacker to find the original intended message by providing the respective hash value.

3) The security, therefore, is provided by the nature of a one way that has a function that is mostly the key component of the SHA algorithm. The preimage resistance is important to clear off brute force attacks from a set of huge and powerful machines.

4) Similarly, the second resistance technique is applied where the attacker has to go through a hard time decoding the next error message even when the first level of the message has been decrypted. The last and most difficult to crack is the collision resistance, making it extremely hard for the attacker to find two completely different messages which hash to the same hash value.

5) Therefore, the ratio to the number of inputs and the outputs should be similar in fashion to comply with the pigeonhole principle. The collision resistance implies that finding two different sets of inputs that hash to the same hash is extremely difficult and therefore marks its safety 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.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

IV. OPTIMAL PRICE FORMULATION

In this section, we formulate the problem for dynamic pricing which is also aimed at enhancing the overall profit for the constructors and the government lenders. The government lenders get the best resources at the lowest prices, and the constructors get the best tenders matching to the resources they have. The set of constructors is denoted by ζC = (Cx|x ∈ X), X = {0, 1, 2,..., X }. The set of government lenders is denoted by ζL = (Ly|y ∈ Y), Y = {0, 1, 2,...,Y} and the set of tenders is denoted by ζT = (Tz|z ∈ Z),Z = {0, 1, 2,..., Z}. We consider five major parameters to choose a suitable constructor for a tender. These parameters include the time required to complete the tender, cost, quality of work, maintenance period after tender completion, and the overall voting of the constructor. The government lender Ly presents a proposal for a tender to be accomplished with all the required parameters. Let Dzy, Pzy, Qzy, Szy, and Vzy denote the expected time period, cost value, quality of work, maintenance period and votes with a constructor, respectively, for the tender Tz. These parameters are broadcasted in the network where all the constructors can read the specifications. Once the lenders have set their parameters, the set of constructors interested in the tender can start with the first round of bidding for the tender. In the traditional system, the first best fit constructor is selected and allocated to the tender based on time, cost, quality of work, maintenance period, and vote parameters associated with the constructor. The proposed model incorporates multiple iterations of bidding so as to optimally evaluate the most suitable constructor for the tender given by the government lender. The iterations continue till the point that the same constructor is the winner in the bid subsequently for two successive iterations. We consider this situation to be the equilibrium point, and the tender is allocated to that constructor. Let Dzx, Pzx, Qzx, Szx, and Vzx denote the proposed time, cost, quality of work, maintenance period, and votes, respectively, by the constructor Cx for the tender Tz where x ∈ X, X = {0, 1, 2,..., X } and z ∈ Z,Z = {0, 1, 2,..., Z}. Next, we calculate normalized time, cost, maintenance period, and vote for all the constructors so as to compare them against the respective parameters that are assigned by the lender. We start with defining the normalized parameters as

$$ND = \frac{D_X - \min(D)}{\max(D) - \min(D)}(b-a) + a$$
$$NP = \frac{P_X - \min(P)}{\max(P) - \min(P)}(d-c) + c$$
$$NQ = \frac{Q_X - \min(Q)}{\max(Q) - \min(Q)}(f-e) + e$$
$$NS = \frac{S_X - \min(S)}{\max(S) - \min(S)}(h-g) + g$$
$$NV = \frac{V_X - \min(V)}{\max(V) - \min(V)}(j-i) + i$$

where ND,NP,NQ,NS, and NV represent the normalized values of time, cost, quality of work, maintenance period, and votes, respectively. The maximum and minimum time limits that can be entered for a tender by the government lenders and the constructors are represented by a and b, respectively. Similarly, c, d, e, f , g, h, i, and j specify the maximum and minimum values of cost, quality of work, maintenance period, and votes for a tender. These formulations are not specific to a constructor, government lender, or tender. Any normalized value can be calculated for any tender, constructor, or government lender by using (1)–(5). For example, the normalized HASSIJA et al. time for zth tender by the xth constructor can be expressed as

$$ND_{zx} = \frac{D_{zx} - \min(D)}{\max(D) - \min(D)}(b-a) + a.$$

Note that in the above equation, min(D) and max(D) denotes the min(Dzx) and max(Dzx) among all constructors, respectively. Similarly, normalized cost NPzx, quality of work NQzx, maintenance period NSzx, and vote NVzx for zth tender by the xth constructor can be calculated with the help of (2)–(5), respectively. The normalized time NDzy, cost NPzy, quality of work NQzy, maintenance period NSzy, and vote NVzy for zth tender by the yth lender can be calculated with the help of (1)–(5), respectively. Note that we assume that the constructors bidding for the tenders do not bid with costs which are better than the expectations of the lender. For example, constructors will always tend to ask for more time, charge a higher price, provide less maintenance time and a lesser vote for the tenders as compared to the time, cost, maintenance period and vote expected by the government lender. As a result of this assumption, we have few constraints given as a

$$a \leq ND_{zy} \leq ND_{zx} \leq b$$
$$c \leq NP_{zy} \leq NP_{zx} \leq d$$
$$f \geq NQ_{zy} \geq NQ_{zx} \geq e$$
$$h \geq NS_{zy} \geq NS_{zx} \geq g$$
$$j \geq NV_{zy} \geq NV_{zx} \geq i.$$

It is also possible that the parameters expected by the lender are unrealistic and it is not feasible for any of the constructors to fairly accept the tender on those terms. We propose a double auction model, where the parameters expected by the government lender are changed if they appear too diverse from the median expectation of all the constructors. We discuss the process of this double auctioning in the next section.

A Double Auctioning Model In this section the set of government lenders ζL make sure that their parameters, such as time, cost, quality of work, maintenance period, and vote related to set of tenders ζT lie in the range of parameters, such as time, cost, quality of work, maintenance period, and vote given by a set of constructors ζC. Next, the set of constructors ζC starts bidding among themselves for a set of tenders ζT iteratively. Finally, the set of tenders ζT given by the set of government lenders ζL are allocated to the set of constructors ζC. Let us assume the tender Tz is given by government lender Ly. The government lender Ly gives the expected time period NDzy, cost NPzy, quality of work NQzy, maintenance period NSzy, and support NVzy, respectively. The cumulative cost of the government lender Ly for tender Tz in terms of the time, cost, quality of work, maintenance period, and votes are kept public for all the constructors ζC. The set of constructors ζC willing to obtain the tender Tz will release their cumulative cost in terms of time period NDzx, cost NPzx, quality of work NQzx, maintenance period NSzx, and support NVzx, respectively. Before initiating the bidding among a set of constructors ζC, it is necessary that for a particular tender Tz

A. Algorithm

Algorithm 1 Cost Optimization Among Government Lenders

Input: The expected ND_{zy}, NP_{zy}, and NS_{zy} for the tender T_z given by L_y.

Output: The expected ND_{zy}, NP_{zy}, and NS_{zy} given by government lender L_y brought in the range of ND_{zx}, NP_{zx}, and NS_{zx} values given by ζ_C for the tender T_z.

The median position μ after sorting the values given by set of constructors ζ_C:

$$\mu = \frac{x+1}{2}$$

for $z = 1 : z$ **do**
  repeat
    $ND_{zy} = ND_{zy} + \nu$
  until $(|ND_{zx}^{\mu} - ND_{zy}| \geq \tau)$
  repeat
    $NP_{zy} = NP_{zy} + \nu$
  until $(|NP_{zx}^{\mu} - NP_{zy}| \geq \tau)$
  repeat
    $NS_{zy} = NS_{zy} - \nu$
  until $(|NS_{zx}^{\mu} - NS_{zy}| \geq \tau)$
end for

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Algorithm 2 Cost Optimization Among Constructors

Input: The ND_{zx}, NP_{zx}, and NS_{zx} values given by set of constructors ζ_C bidding for the tender T_z.
Output: Final win counts ω_{zx} of constructors bidding for T_z after they reach stopping criteria.

$\omega_{zx} = \{\omega_{z1}, \omega_{z2}, .., \omega_{zx}\}$
Initialize $\xi = 1$
for $z = 1 : z$ **do**
  while $|\rho_{zx,b} - \rho_{zx,b-1}| > \Theta$ **do**
    $\xi = \xi + 1$
    for $x = 1 : x$ **do**
      $ND_{zx} = \frac{D_{zx} - min(D)}{max(D) - min(D)}(b - a) + a$
      $NP_{zx} = \frac{P_{zx} - min(P)}{max(P) - min(P)}(d - c) + c$
      $NQ_{zx} = \frac{Q_{zx} - min(Q)}{max(Q) - min(Q)}(f - e) + e$
      $NS_{zx} = \frac{S_{zx} - min(S)}{max(S) - min(S)}(h - g) + g$
      $NV_{zx} = \frac{V_{zx} - min(V)}{max(V) - min(V)}(j - i) + i$
      $\rho_{zx} = [(w_{dzy} * ND_{zx}) + (w_{pzy} * NP_{zx}) + (w_{qzy} * NQ_{zx}) + (w_{szy} * NS_{zx}) + (w_{vzy} * NV_{zx})]$
    end for
    if $\rho^x_{zx=1} = min(\rho)$ **then**
      $\omega_{zx} = \omega_{zx} + 1$
    end if
    for $x = 1{:}x$ **do**
      if $ND^x_{zx=1} \neq min(ND_{zx}), ND^x_{zx=1} \geq \tau_1$ **then**
        $ND^x_{zx=1} = ND^x_{zx=1} - \nu_1$
      end if
      if $NP^x_{zx=1} \neq min(NP_{zx}), NP^x_{zx=1} \geq \tau_2$ **then**
        $NP^x_{zx=1} = NP^x_{zx=1} - \nu_2$
      end if
      if $NS^x_{zx=1} \neq min(NS_{zx}), NS^x_{zx=1} \leq \tau_3$ **then**
        $NS^x_{zx=1} = NS^x_{zx=1} + \nu_3$
      end if
    end for
  end while
end for

Algorithm 3 Allocation of Tenders to Constructors

Input: Final win count ω of set of constructors ζ_C participating in bidding for tender T_z

$\omega_{zx} = \{\omega_{z1}, \omega_{z2}, ..., \omega_{zx}\}$
Output: Tender T_z is allocated to the contructor C_x

$T_z \iff C_x$
for $z = 1 : z$ **do**
  if Only one constructor has maximum win count: **then**
    for $x = 1 : x$ **do**
      if $\omega^x_{zx=1} = max(\omega)$ **then**
        $\mathbf{x} = x$
        $T_z \iff C_{\mathbf{x}}$
      end if
    end for
  else
    for $x = 1{:}x$ **do**
      if $\varphi^x_{zx=1} = min(\varphi)$ **then**
        $\mathbf{x} = x$
        $T_z \iff C_{\mathbf{x}}$
      end if
    end for
  end if
end for

B. Performance Evaluation

We have only considered time period, cost value, and maintenance period parameters to evaluate the performance of our model. Because the weights associated with these parameters are more compared to the quality of work and votes, which influence the cumulative cost value ρzx.

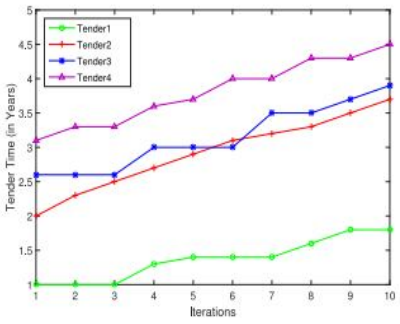


Fig. 2. Change of time period given by government lenders over iterations.

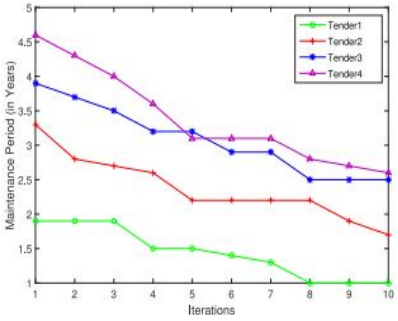


Fig. 4. Change of maintenance period given by government lenders over iterations.

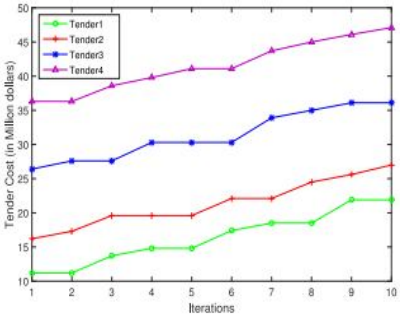
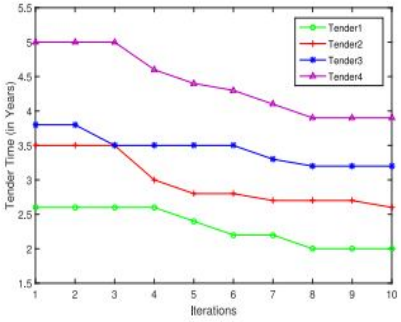


Fig. 3. Change of cost value given by government lenders over iterations.



\\

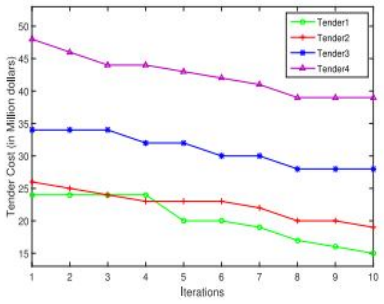


Fig. 6. Change of cost value given by constructors over iterations.

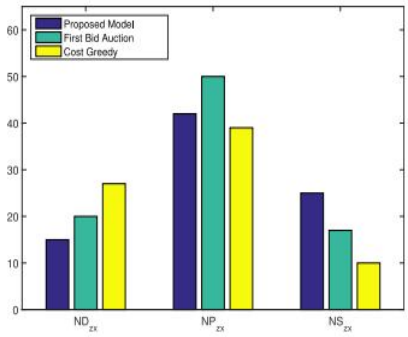


Fig. 8. Comparison of the proposed, first bid, and cost greedy approaches.

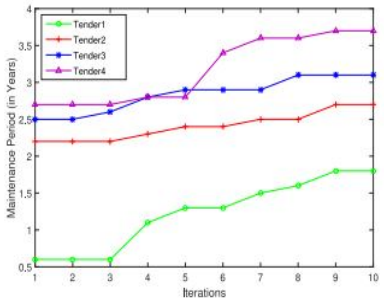


Fig. 7. Change of maintenance period given by constructors over iterations.

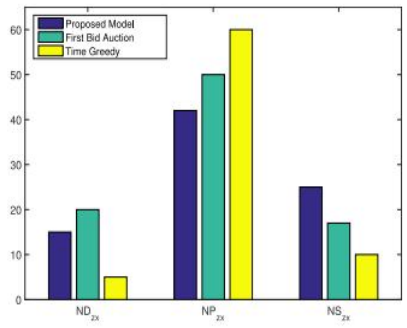


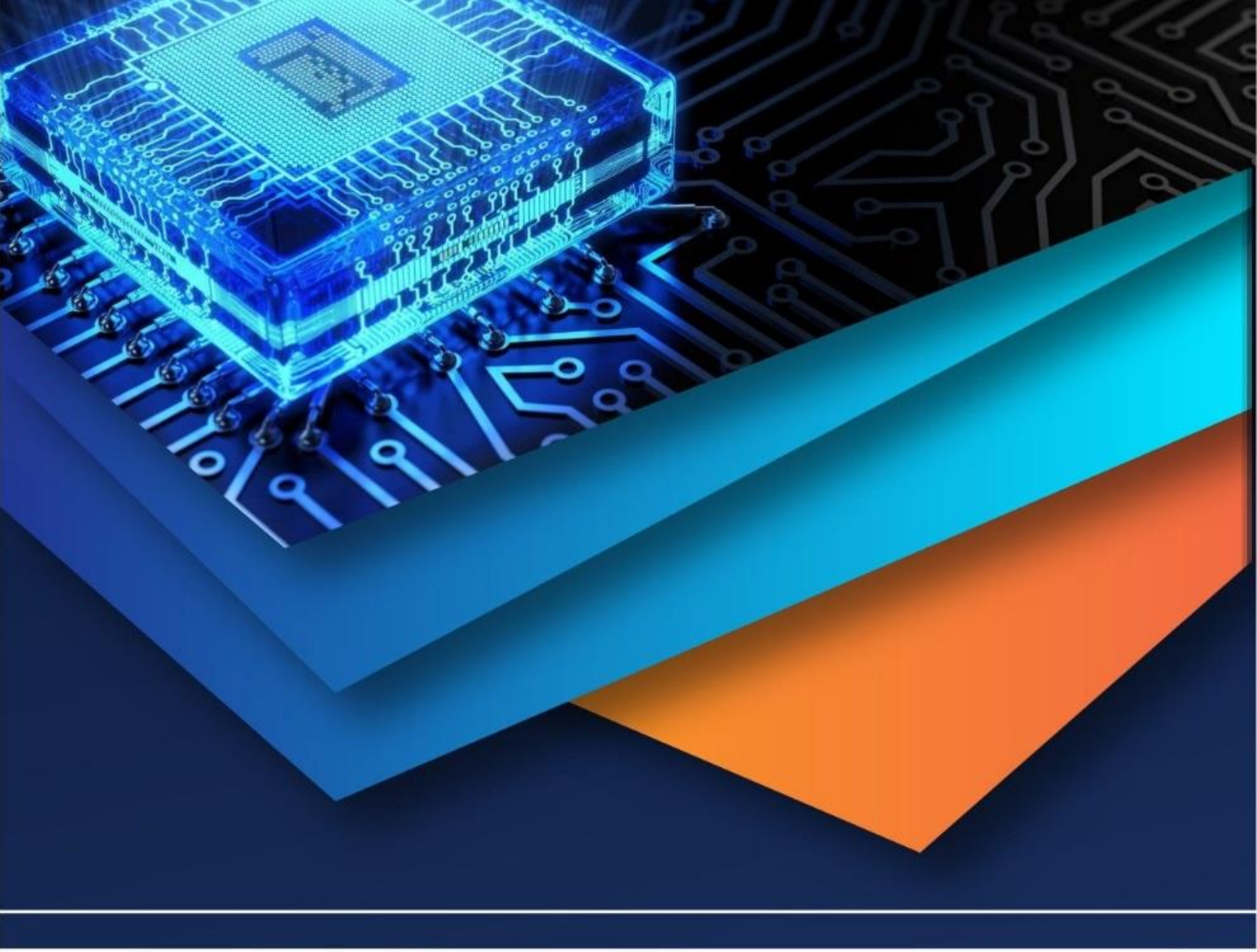
Fig. 9. Comparison of the proposed, first bid, and time greedy approaches.

V. CONCLUSIONS

In this article, we have discussed on the need and benefits of using blockchain technology in the government tender assignment process. We have used Ethereum to implement the end-to-end edge computing framework for a government tender workflow. The iterative auction algorithm is proposed to associate the best-suited constructors to the tender projects, thereby enhancing the profit of both the government lenders 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.

REFERENCES

[1] 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. 2418 IEEE INTERNET OF THINGS JOURNAL, VOL. 8, NO. 4, FEBRUARY 15, 2021
[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] H. Cho, "Asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," IEEE Access, vol. 6, pp. 66210–66222, 2018.
[12] J. D. Groot. The History of Data Breaches. Accessed: Oct. 24, 2019. [Online]. Available: https://digitalguardian.com/blog/history-databreaches
[13] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2543–2585, 3rd Quart., 2018.
[14] J. A. Jaoude and R. G. Saade, "Blockchain applications—Usage in different domains," IEEE Access, vol. 7, pp. 45360–45381, 2019.
[15] H. Hou, "The application of blockchain technology in e-government in china," in Proc. IEEE 26th Int. Conf. Comput. Commun. Netw. (ICCCN), 2017, pp. 1–4.
[16] S. Ølnes and A. Jansen, "Blockchain technology as S support infrastructure in e-government," in Proc. Int. Conf. Electron. Govt., 2017, pp. 215–227.
[17] S. Ølnes, "Beyond bitcoin enabling smart government using blockchain technology," in Proc. Int. Conf. Electron. Govt., 2016, pp. 253–264.
[18] S. Rama, S. V. Flowerday, and D. Boucher, "Information confidentiality and the chinese wall model in government tender fraud," in Proc. IEEE Inf. Security South Africa, 2012, pp. 1–8.
[19] A. Dello and C. Yoshida, "Online tendering and evaluation for public procurement in tanzania," in Proc. 18th IEEE/ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel Distrib. Comput. (SNPD), 2017, pp. 137–141.
[20] Z. Hui and J. Yang, "Research on application of e-Tender in China," in Proc. IEEE Int. Conf. Internet Technol. Appl., 2011, pp. 1–3.
[21] H. Fukui and K. Kobayashi, "Optimal comprehensive tendering models for project procurement," in Proc. IEEE Int. Conf. Syst. Man Cybern., 2010, pp. 3258–3264.
[22] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," IEEE Security Privacy, vol. 16, no. 4, pp. 20–29, Aug. 2018. [
[23] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An IDbased linearly homomorphic signature scheme and its application in blockchain," IEEE Access, vol. 6, pp. 20632–20640, 2018.
[24] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," IEEE Access, vol. 6, pp. 28203–28212, 2018.
[25] P. Noizat, "Blockchain electronic vote," in Handbook of Digital Currency. Amsterdam, The Netherlands: Elsevier, 2015, pp. 453–461.
[26] Y. Zhang, S. Deng, Y. Zhang, and J. Kong, "Research on government information sharing model using blockchain technology," in Proc. IEEE 10th Int. Conf. Inf. Technol. Med. Educ. (ITME), 2019, pp. 726–729.
[27] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchainenabled smart contracts: Architecture, applications, and future trends," IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 11, pp. 2266–2277, Nov. 2019.
[28] M. O'Neill and M. J. B. Robshaw, "Low-cost digital signature architecture suitable for radio frequency identification tags," IET Comput. Digit. Techn., vol. 4, no. 1, pp. 14–26, Jan. 2010.
[29] R. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," IEEE Commun. Stand. Mag., vol. 2, no. 3, pp. 29–37, Sep. 2018.
[30] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in Proc. 9th Int. Conf. Computi. Commun. Netw. Technol. (ICCCNT), Jul. 2018, pp. 1–4.
[31] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3680–3689, Jun. 2019.
[32] V. Hassija, V. Saxena, V. Chamola, and R. Yu, "A parking slot allocation framework based on virtual voting and adaptive pricing algorithm," IEEE Trans. Veh. Technol., vol. 60, no. 6, pp. 5945–5957, Jun. 2020.
[33] V. Hassija, V. Saxena, and V. Chamola, "A mobile data offloading framework based on a combination of blockchain and virtual voting," Softw. Pract. Exp., to be published.
[34] N. G. Saglam, A. Z. Yılmaz, C. Becchio, and S. P. Corgnati, "A compre- ˘ hensive cost-optimal approach for energy retrofit of existing multi-family buildings: Application to apartment blocks in Turkey," Energy Build., vol. 150, pp. 224–238, Sep. 2017.
[35] C. Yang, C. Liu, X. Zhang, S. Nepal, and J. Chen, "A time efficient approach for detecting errors in big sensor data on cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 2, pp. 329–339, Jan. 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY