Blockchain enabled Security Framework for handling Security and privacy challenges in Smart cities

Divya [a] , Dr. Yogesh Kumar Sharma[b]
[a]Research Scholar Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan
[b]Associate Professor & Research coordinator; Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan
[b]Email: dr.sharmayogeshkumar@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: One of the intriguing secure applications with regards to the keen city is communicating data to authentic clients, alluringly with client protection. Broadcast encryption has been considered as a helpful device to ensure the information security and give information access control. Most works in broadcast encryption are about the information security, while less consideration is paid to the information access control and the character protection. In this paper, in view of transmission encryption, we present a plan called Fully Privacy-Preserving and Revocable Identity-Based Broadcast Encryption, which protects the information security and the personality security of the collector just as the denied client. The information can be safely ensured and just the approved client can get to the information. The repudiation cycle doesn't uncover any data about the information substance and the collector personality. The general population adapts nothing about the recipient character and the repudiated client personality. These properties lead to pleasant applications in the shrewd city where character protection is attractive. The security of our plan is end up being semantically secure in the arbitrary prophet model

Keywords: Smart City, Security, Privacy, Unauthorized access, Blockchain

1. Introduction

Savvy urban communities plan to improve the nature of metropolitan administrations and guarantee manageability by utilizing present day data and correspondence advancements. The shrewd city certainly will turn into the up and coming age of urbanization. This anyway brings some new difficulties. One of the centers of the savvy city is information, which could be touchy, for instance, ledger number and passwords to shop on the web, an organization may impart their information to different gatherings in the keen city. All these are identified with the security of information transmission. Step by step instructions to productively ensure the information security and protection has become a significant issue in savvy urban communities. Broadcast Encryption presented by Fiat and Naor [1] has been generally acknowledged as a powerful technique to ensure the information security and protection in multi-recipient situations and turns into a valuable apparatus to accomplish information access control with the end goal that lone the approved clients can get to the information.

Broadcast encryption incredibly improves the productivity when one message ought to be imparted to multi-clients. It permits an information proprietor to disperse one basic information to a gathering of clients S so that solitary the client has a place with S can get to the information. The clients outside S can't gain proficiency with any data about the information substance regardless of whether they plot. Because of these stand-apart benefits of transmission encryption, it has been broadly acknowledged as a helpful instrument for some, applications, ranging from ensuring protected substance conveyed as put away media [2], to overseeing advanced membership to satellite TV, to controlling admittance to encoded record frameworks [3-10].

The transmission encryption instrument can likewise be sent to ensure the information protection and give information access control. For instance, in the brilliant water framework, it can utilize broadcast encryption to convey a key to a gathering of those clients who have paid for water administration. With this key, the client can appreciate the water supply administration. Interestingly, without a key, the client can't get to the water administration [11]. In the brilliant city, "savvy" gadgets ought to be adequately shrewd and can manage information access control naturally somewhat. For instance, a brilliant gadget ought to have the option to choose which client/client has the entrance advantage to specific sorts of information as far as access control approaches. Just the approved clients can get to the comparing information asset. Moreover, when a few collectors ought to be denied, these shrewd gadgets additionally can deny these clients such that the repudiated client can't get to the information any longer [12].

We stress that the thought of disavowal in this paper is completely unique in relation to [13-19] which read the renouncement framework for the future transmissions. Disavowal framework is a negative simple of transmission encryption. In repudiation frameworks, a message is scrambled by utilizing the personalities of denied clients with the end goal that all non-renounced clients can utilize their private keys to unscramble the ciphertext. In examination with this denial encryption idea, the renouncement in this paper centers around the how to disavowed a few recipients after the ciphertext has been produced, however without uncovering the message content and the character data of beneficiaries.

2. Literature review

In this subsection, we examine the security issues when utilizing broadcast encryption instrument to accomplish information access control. Since Fiat and Naor [14] presented broadcast encryption for information access control, resulting works [5, 7, 9–11, 15, 21] have proposed communicated encryption frameworks with various properties. They essentially centered around lessening public key sizes, private key sizes, ciphertext sizes, and computational expenses for encryption and unscrambling. The idea of identitybased broadcast encryption (IBBE) was presented by Sakai and Furukawa [22] and by Delerabl'ee [9]. Both proposed plans accomplish consistent size ciphertext and private keys. Every one of these plans anyway didn't contemplate the collector security. The principal work considers the obscurity in broadcast encryption showed up in [24]. The creators introduced the idea of private transmission encryption to secure the personalities of the recipients. Boneh et al. [6] stretched out this idea to private direct transmission encryption. In this manner, numerous mysterious ID-based transmission encryption plans were proposed [3, 6, 12, 13, 17, 20, 25].

Chu et al. [8] broadened the idea of intermediary re-encryption to build the intermediary broadcast re-encryption (PBRE). PBRE permits the intermediary to change a ciphertext planned for a beneficiary set to another ciphertext expected for another collector set. As of late, roused by the cloud email framework, Xu et al. [24] introduced a contingent personality based transmission intermediary re-encryption plot with steady ciphertext dependent on [26]. By the by, in PBRE framework, the information proprietor needs to designate a re-encryption key to the intermediary and the intermediary knows the new beneficiaries' personalities [22].

The primary work which considered renouncement in broadcast encryption showed up in [23]. It permits any outsider to renounce any beneficiaries without uncovering the information substance to the outsider. In any case, the downside is that the outsider knows the beneficiary personality. Lai et al. [18] later tackled the issue. They proposed a mysterious identitybased broadcast encryption with renouncement plot. The outsider plays out the renouncement can't get any data about the collector security. Nonetheless, the personalities of disavowed clients ought to be appended as a feature of ciphertext, which some way or another uncovered the collector protection. Expecting to accomplish completely protection saving, we propose another structure dependent on [18].Without giving the repudiation list which contains client personalities, it was difficult to recuperate the full unscrambling key in [18].

3. Hybrid Security framework for Smart cities

The shrewd city has become an arising worldview with the development and progression of IoT. It is vital to consider the downstream handling of the organization when planning the design of a shrewd city organization. A model is a keen structure wherein a sensor is associated with a lighting apparatus that can be important for a bigger structure application. The shrewd structure can likewise be essential for an organization of savvy urban areas. For this situation, we should consider the way that the information is sent locally as well as to a bigger organization of structures lastly to a bigger organization of urban areas [26].

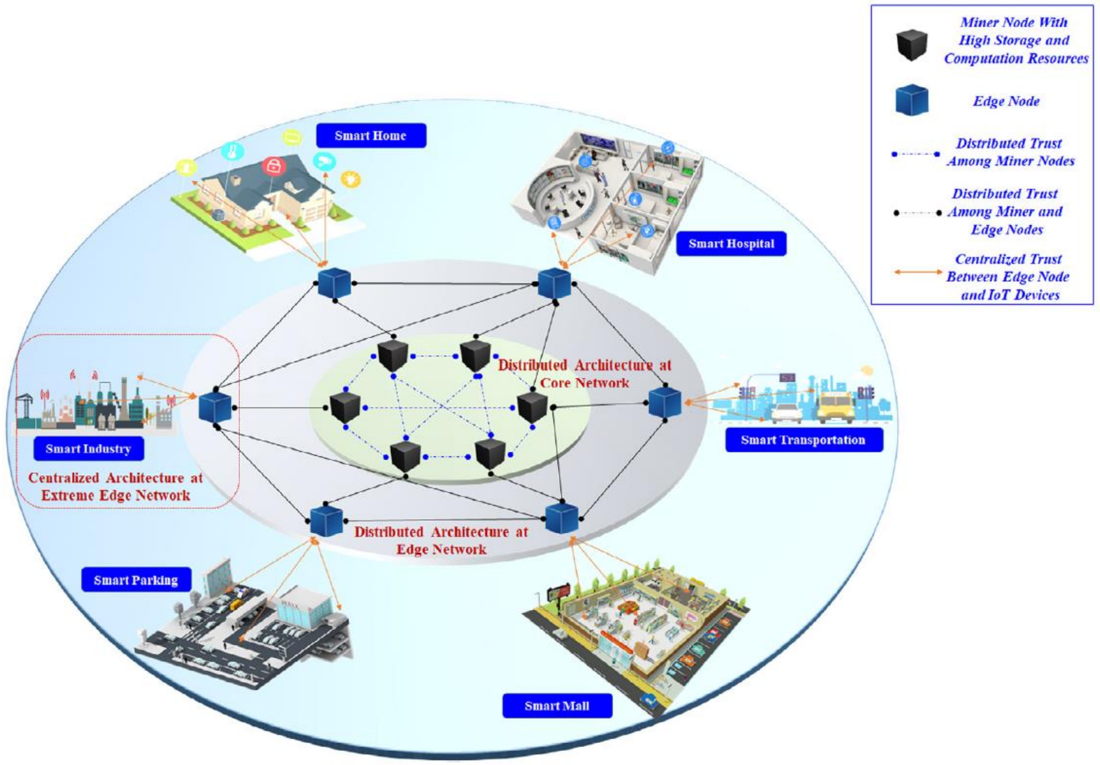
Miner Node With High Storage and Computation Resources
Edge Node
Distributed Trust Among Miner Nodes
Distributed Trust Among Miner and Edge Nodes
Centralized Trust Between Edge Node and IoT Devices
Smart Home
Smart Hospital
Distributed Architecture at Core Network
Smart Transportation
Smart Industry
Centralized Architecture at Extreme Edge Network
Distributed Architecture at Edge Network
Smart Parking
Smart Mall

Fig. 1 Proposed hybrid network architecture for a sustainable smart city network.

Fig. 1 shows the by and large proposed cross breed engineering of the versatile shrewd city organization. In the proposed model, the savvy city network is separated into two unique gatherings – the center organization and the edge organization – utilizing the blockchain strategy. The center organization comprises of excavator hubs with high calculation and capacity assets, though the edge hub has restricted capacity and calculation power. Digger hubs will be answerable for making blocks and confirming evidence of-work. Every hub is empowered with SDN regulator to accomplish high dexterity and security, diminish equipment the board cost, and acknowledge simplicity of sending in the brilliant city network framework. Here, we utilized the security strength of the FS-OpenSecurity SDN model from our past work [35].

In our proposed design, each edge hub goes about as a concentrated worker for explicit public foundation to offer fundamental types of assistance and accomplish limitations. It stores the entrance strategies and certifications of its privately enrolled elements in its data set and accomplishes low inactivity and decrease network transmission capacity. The disseminated idea of the proposed model can make the entire framework stronger and limit the effect of assaults in any event, when the hub is undermined. As such, if the edge hub is undermined, the subsequent impact should be restricted to the neighborhood.

Proposed model work process

In the brilliant city, IoT gadgets produce a huge volume of information and require constant handling. In our proposed model, edge hubs offer constant handling with low dormancy and organization transfer speed utilizations and get sent at the edge of the organization. The edge hub has restricted capacity and calculation power and preprocesses the crude information transferred by the end gadgets to channel the information and get valuable data. When information is preprocessed, the edge hub moves the pre-handled scrambled information to the center organization of the brilliant city if vital. The excavator hub in the center organization will additionally break down the pre-prepared information, decide, approve and confirm the PoW, and create blocks. To guarantee the honesty of information put away in the center organization, we utilize computerized mark and store hashes in blockchain. These hashes in blockchain are changeless, filling in as proof to demonstrate the uprightness of the information. It exhibits the work process of our proposed model, where we utilized the Argon2 based hashing plan.

4. Results & Analysis

To assess the presentation overhead of our proposed model, we noticed the dormancy and throughput in our test examination. Here, we believe inertness to be the absolute time taken from receipt of the occasion by the edge hub to the time it sends the ideal reaction, exchange hash, producing block, and so forth Here, we composed test contents to trigger occasions at the edge hub when it gets the reaction of the past occasion. Fig. 4 shows the aftereffects of inactivity perception in our proposed model contrasted and the public Ethereum blockchain. The mining task is intentionally intended to be hard to register, and the span for a square to be mined relies upon the intricacy of the mining task.

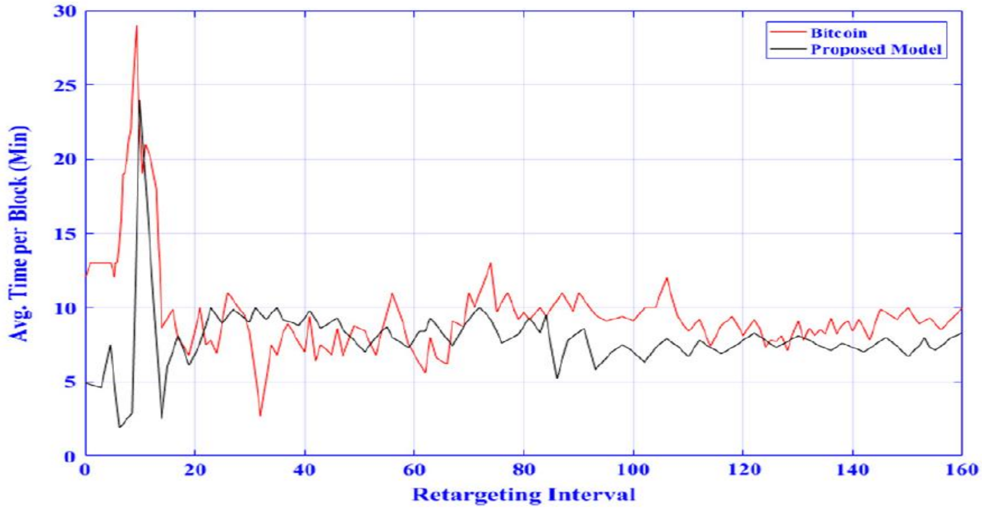

Fig. 2. Average time per block.

As demonstrated in Fig. 2, the middle idleness accomplished in our reproduction utilizing the public Ethereum blockchain is 21 s; in our proposed model, be that as it may, we accomplished a middle inertness of 3.9 s, which is reasonable for sending in many brilliant city applications. Since we acquired the SDN regulator security highlights from our past work, we skirted further security examination of the SDN regulator here.

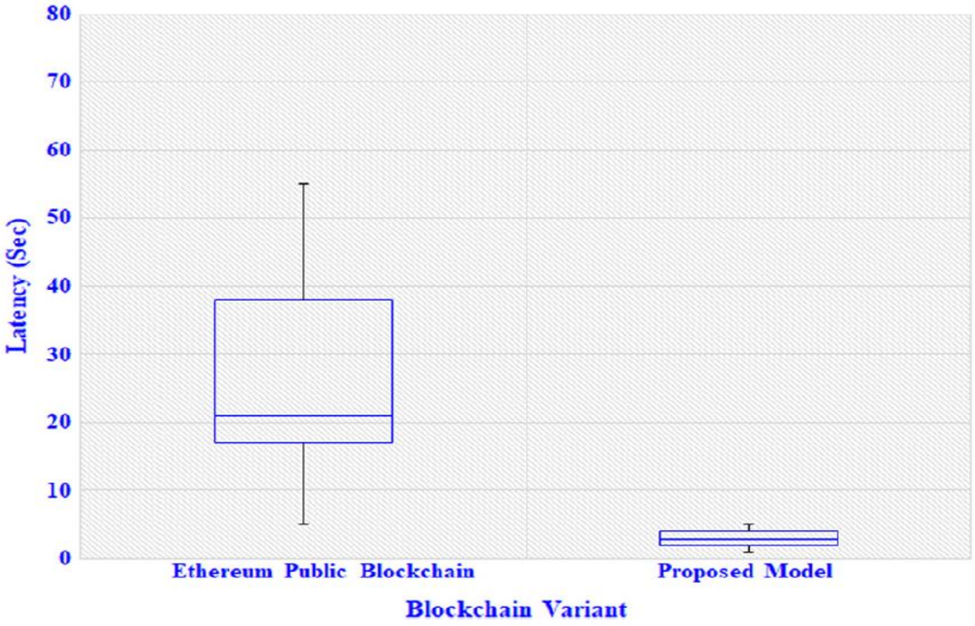

Fig. 3. Results of latency in our proposed model

5. Conclusion

Huge progressions in different advancements like CPS, IoT, WSNs, distributed computing, and UAVs have occurred recently. The keen city worldview joins these significant new advances to improve the personal satisfaction of city occupants, give productive usage of assets, and lessen operational expenses. All together for this model to arrive at its objectives, it is fundamental to give effective systems administration and correspondence between the various parts that are included to help different brilliant city applications. In this work, we explored the systems administration necessities for the various applications and distinguished the fitting conventions that can be utilized at the different framework levels. Also, we showed organizing structures for five distinctive shrewd city frameworks. This region of exploration is as yet in its underlying stages. Future investigations can zero in on significant necessities including directing, energy proficiency, security, unwavering quality, versatility, and heterogeneous organization support. Thusly, more examinations and studies should be done, which should prompt the plan and advancement of productive systems administration and correspondence conventions and designs to meet the developing necessities of the different significant and quickly growing shrewd city applications and administrations.

References

1. Agyeman J, McLaren D (2014) ‘Smart Cities’ Should Mean ‘Sharing Cities’. In: Times
2. Al-Hader M, Rodzi A, Sharif AR, Ahmad N (2009) Smart city components architicture, 2009 International Conference on Computational Intelligence, Modelling and Simulation, IEEE., pp 93–97
3. Anthopoulos L, Fitsilis P (2010) Intelligent Environments (IE), 2010 Sixth International Conference on, IEEE., pp 301–306
4. Aurigi A (2005) Making the digital city: the early shaping of urban internet space. Ashgate Publishing, Ltd, Hampshire
5. Avizienis A, Laprie JC, Randell B, Landwehr C (2004) Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secure Comput 1(1):11–33
6. Bătăgan L (2011) Smart cities and sustainability models. Inf Econ 15(3):80–87
7. Belk R (2014) You are what you can access: Sharing and collaborative consumption online. J Bus Res 67(8):1595–1600
8. Bhattacherjee A (2002) Individual trust in online firms: Scale development and initial test. J Manag Inf Syst 19(1):211–241
9. Boulton A, Brunn SD, Devriendt L (2011) 18 cyberinfrastructures and ‘smart’world cities: physical, human and soft infrastructures. In: International Handbook of Globalization and World Cities., p 198
10. Caragliu A, Del Bo C, Nijkamp P (2011) Smart cities in Europe. J Urban Technol 18(2):65–82
11. Chourabi H, Nam T, Walker S, Gil-Garcia JR, Mellouli S, Nahon K, Pardo TA, Scholl HJ (2012) Understanding smart cities: An integrative framework, System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE., pp 2289–2297
12. Cocchia A (2014) Smart and Digital City: A Systematic Literature Review. Smart City: How to Create Public and Economic Value with High Technology in Urban Space. Dameri RP and Rosenthal-Sabroux C (eds). Springer International Publishing, Cham, p 13–43
13. Ashok Kumar and Dr. Yogesh Kumar Sharma,” Reviewing cloud resource management schemes used in Cloud computing system”, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3 Issue 4, December 2016, pp. 104-111.
14. Dillahunt TR, Malone AR (2015) The Promise of the Sharing Economy among Disadvantaged Communities. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, Seoul, pp 2285–2294
15. V. A. Sindekar, Y. K. Sharma, and D. Sharma, “A Guide for Selecting CMS Tools: Wordpress, Joomla, Drupal,” Studies in Indian Place Names, vol. 40, no. 35, pp. 621–626, 2020.
16. Ergazakis K, Metaxiotis K, Psarras J (2004) Towards knowledge cities: conceptual analysis and success stories. J Knowl Manag 8(5):5–15
17. Forest F, Lavoisy O, Eurich M, Van Gurp J, Wilson D (2009) Roadmap for Real World Internet applications, Towards the Future Internet-A European Research Perspective., pp 325–334
18. Giffinger R, Gudrun H (2010) Smart cities ranking: an effective instrument for the positioning of the cities? ACE Archit City Environ 4(12):7–26.
19. Larsen K (1999) Learning cities: the new recipe in regional development, vol 217/218, Organisation for Economic Cooperation and Development. The OECD Observer., p 73
20. Malek JA (2009) Informative global community development index of informative smart city. Proceedings of the 8th WSEAS International Conference on Education and Educational Technology.
21. Malhotra A, Alstyne MV (2014) The dark side of the sharing economy & hellip; and how to lighten it. Commun ACM 57(11):24–27
22. Dalal S., Agrawal A., Dahiya N., Verma J. (2020) Software Process Improvement Assessment for Cloud Application Based on Fuzzy Analytical Hierarchy Process Method. In: Gervasi O. et al. (eds)

Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12252. Springer, Cham. https://doi.org/10.1007/978-3-030-58811-3_70

23. Morrison A (2016) Blockchain and smart contract automation: How smart contracts automate digital business., http://www.pwc.com/us/en/technology-forecast/blockchain/digital-business.html
24. Seth B., Dalal S., Kumar R. (2019) Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage. In: Kumar R., Wiil U. (eds) Recent Advances in Computational Intelligence. Studies in Computational Intelligence, vol 823. Springer, Cham.
25. S. Pradeep and Y. K. Sharma, “A Pragmatic Evaluation of Stress and Performance Testing Technologies for Web Based Applications,” in 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 399–403.
26. Seth B, Dalal S, Jaglan V, Le DN, Mohan S, Srivastava G Integrating encryption techniques for secure data storage in the cloud. Trans Emerg Telecommun Technol e4108, 1-24
27. Ranchordás S (2015) Does sharing mean caring: Regulating innovation in the sharing economy. Minn JL Sci Tech 16:413
28. Schuler D (2001) Digital cities and digital citizens. In Kyoto Workshop on Digital Cities. Springer, Berlin Heidelberg, p71–85
29. SpendMatters (2015) Why Bitcoin’s Blockchain Technology Could Revolutionize Supply Chain Transparency. In: Spend Matters., http://spendmatters.com/2015/11/09/why-bitcoins-blockchain-technology-could-revolutionize-supplychain-transparency/
30. Sundararajan A (2014) Peer-to-peer businesses and the sharing (collaborative) economy: Overview, economic effects and regulatory issues, Written testimony for the hearing titled The Power of Connection: Peer to Peer Businesses, January
31. Tedjasaputra A, Sari E (2016) Sharing Economy in Smart City Transportation Services. In: Proceedings of the SEACHI 2016 on Smart Cities for Better Living with HCI and UX. ACM, San Jose, pp 32–35
32. Panthee, M., & Sharma, Y. K. (2019). Review of e-government implementation. International Journal of Recent Research Aspects, ISSN: 2349-7688, 6(1), 26–30.
33. Washburn D, Sindhu U, Balaouras S, Dines R, Hayes N, Nelson L (2009) Helping CIOs understand “smart city” initiatives. Growth 17(2):1–15
34. Y. K. Sharma and M. D. Rokade, "Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic.," IOSR Journal of Engineering, pp. 63-67, 2019.
35. Bijeta Seth, Surjeet Dalal, Dac-Nhuong Le, Vivek Jaglan, Neeraj Dahiya, Akshat Agrawal, Mayank Mohan Sharma, Deo Prakash, K. D. Verma, Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm, Computers, Materials & Continua, Vol.67, No.1, 2021, pp.779-798, doi:10.32604/cmc.2021.014466
36. Zhao JL, Hsu C, Jain HK, Spohrer JC, Tanniru M, Wang HJ (2008) ICIS 2007 Panel report: bridging service computing and service management: how MIS contributes to service orientation. Commun Assoc Inf Syst 22(1):22