International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Design of a Blockchain-Based Access Control Model with QoS-Awareness Via Bioinspired Computing Techniques

Sonali Mahendra Sonavane[1], Dr. Prashantha G. R[2], Jyoti Yogesh Deshmukh[3], Mangesh D. Salunke[4], Hemantkumar B Jadhav[5], Pranjali Deepak Nikam[6]

Submitted: 25/03/2023 **Revised**: 28/05/2023 **Accepted**: 13/06/2023

Abstract: Designing access control models requires effective analysis of different cloud components, user behavior patterns, identity parameters, etc. Existing access control models perform data overwriting for design of rule-update access control, thus do not incorporate dynamic pattern tracking for temporal user sets. Models that enable dynamic pattern tracking are either too complex to deploy, or do not incorporate immutability in their designs. To overcome these limitations, a novel blockchain-based access control model with Quality of Service (QoS)-awareness via bioinspired computing techniques is discussed in this text. The proposed model initially uses a single chained blockchain for storing access rules. Blockchain also allows the model to integrate rule-tracing, which assists in tracking access changes for user-to-entity behavioral patterns. But single blockchains might affect QoS of the cloud deployment, thus a bioinspired model for QoS-aware side chaining is deployed. This model assists in performing 'archive & split' operations on current blockchain, depending upon its current QoS performance. To estimate this performance, the model proposes use of a dynamic fitness function that incorporates service delay, throughput, access rule characteristics and service consistency metrics. These metrics along with temporal cloud performance are integrated to evaluate final decisions regarding 'archive & split' operations. The model was tested for smart farming applications, and was related with different state-of-the-art methods. The proposed model can be implemented for a wide range of real-time access control scenarios as a result of this performance optimization process.

Keywords*: Access, Control, Blockchain, Bioinspired, Archive, Consistency, Throughput, Performance*

1. Introduction

Designing an access control model for clouds is a multi-level task that involves design of rule engines, rule checkers, rule analyzers, user-level behavioral control, and other deployment-specific techniques. A typical access control model that uses blockchain for internal operations is depicted in [1], wherein Cipher text Policy Attribute-Based Encryption (CP ABE) is combined with Group based operations for better control performance.

The model uses a combination of access policies with user-data in order to generate session tokens. These tokens are encrypted, and stored on blockchains for improved security performance. They can be either revoked or accessed via use of different hash components, which are validated by different attribute authorities. In the following section of this article, a survey of comparable models [2,3,4] together with their cloud-specific nuances, functionality-specific benefits, context-specific drawbacks, and application-specific future research horizons, are described. Based on this discussion, it was observed that existing models are either capable of storing static rules, or cannot be used for large-scale deployments due to their performance complexity. To overcome these limitations, section 3 proposes design of a blockchain-based access control model with QoS-awareness via bioinspired computing techniques. This model uses a combination of immutable sidechains that are formed via QoS-aware 'archive & split' operations. Section 4 evaluates the model's performance and compares it to several cutting-edge techniques. This paper concludes with a few functional and context-specific observations regarding the suggested model and suggestions for ways to enhance it further in various use cases.

2. Literature Review

Authentication and access control systems are often implemented by using non-standard and personalized security methods. The immutability and traceability of blockchain data made it possible to standardize the

[1]*G H Raisoni College of Engineering and Management, Pune, Maharashtra, India*
Corresponding author e-mail: sonali.sonavane@raisoni.net
[2]*Jain Institute of Technology,Davangere, Karnataka, India*
prashanthagr.sjce@gmail.com
[3]*G H Raisoni College of Engineering and Management, Pune, Maharashtra, India*
jyoti1584@gmail.com
[4]*Marathwada Mitramandal's Institute of Technology,Lohgaon, Pune, Maharashtra, India*
salunkemangesh019@gmail.com
[5]*Adsul's Technical Campus,Ahmednagar, Maharashtra, India*
hem3577@gmail.com
[6]*Anantrao Pawar College of Engineering and Research, Pune, Maharashtra, India*
pranjali.amore@gmail.com

implementation of authentication and access control after the invention of blockchain technology. This made it possible to standardize the implementation of authentication and access control. It was suggested in [5,6] that the Privacy-Preserving Parallel Pedersen Commitment (P4C) Model be used in combination with Smart Contracts in order to implement context-specific access control mechanisms for different types of networks. On the other hand, these models are very sophisticated, which significantly limits not just their use but also their ability to scale. In order to achieve this level of speed, [7] advises using a Blockchain-Based Lightweight Vehicle to Infrastructure Handover Authentication Model. By relying on hash-based tests, which are known for their ease of use, this model contributes to the simplification of the authentication process, which is a significant benefit. Using blockchain technology, the concept may be executed in a wide variety of various ways, and it has an extremely high scalability factor. This idea was subsequently refined by [8,9,10], which includes the use of Edge Servers, low power blockchain for energy trade, and decentralized authentication. [8,9,10] Under real-time use scenarios, the optimization of deployment performance is helped greatly by each and every one of these parameters. There are discussions of similar models in [11,12,13]. These models suggest the use of the Roaming Authentication Protocol (RAP), the Modular Square Root Model (MSRM), and an authentication system developed on Transfer Learning enabled Blockchain (ATLB). By adopting consensus models that are both cheap on power and high on speed, these models contribute to the improvement of the computing performance of blockchains.

Models that take use of innate physical capabilities that cannot be replicated in a laboratory (PUFs) CD2A2, which is an acronym for "Cross-Domain Dynamic Accumulator Authentication" SDN stands for software-defined networking. [16] There is also discussion among researchers over the light weighted PUF [17] and the Conditional Privacy-Preserving Authentication (CPPA) [18]. [17] [18] These models are very malleable and have the capacity to have their configuration altered while they are operating in order to accomplish highly effective communication tasks. The performance of the Models was further enhanced by the work done in [19,20], which suggests the usage of a cross-domain authentication model in conjunction with Merkle R-trees. Both of them have the potential to be developed for use in a variety of deployment domains with just a little increase in overhead. These models [21,22,23] projected the use of Domain Certificate Authentication and Validation Model, Quantum-Defended Blockchain-Assisted Data Authentication Model (QDB ADAM), and Homomorphic Encryption Models, all of which have the capability of being extended to a wide variety of low-power and high-density network deployments. Domain Certificate Authentication and Validation Model, Quantum-Defended Blockchain-Assisted Data Authentication Model (QDB ADAM), and These models are improved with the help of a protocol known as Certificate less Key Agreement [24, 25, 26, 27] and data storage models [28, 29, 30] based on the interplanetary file system (IPFS), both of which may be used for distributed applications without the need for additional computational overheads to be carried out. These models are beneficial for establishing block chains; but they are unable to do dynamic pattern tracking for temporal user sets; they are too difficult to install; and their designs do not include traceability. These models do not integrate traceability into their designs; yet, they are beneficial for deployment due to their portability. In order to find a solution to these issues, the following industry has suggested developing a cutting-edge access control model that is built on block chains and is cognizant of issues with the quality of service. For the purpose of determining whether or not its performance can be validated under a variety of different network configurations, the model makes use of Grey Wolf Optimization (GWO) and evaluates it in relation to a wide variety of innovative approaches while facing a variety of different kinds of attacks.

Proposed blockchain-based access control model with QoS-awareness via bioinspired computing techniques

From the above survey it is perceived that various existing access control models are capable of overwriting access rules, but are not capable of dynamic pattern tracking for temporal user sets. While, the models that are capable of dynamic pattern tracking are either too complex to deploy, or do not incorporate immutability & traceability in their designs. Due to which, administrators are unable to keep a track of access changes for different network entities. To get around these restrictions, this section proposes design of a novel blockchain-based access control model with QoS-awareness. The model uses Grey Wolf Optimization (GWO) in order to decide split & merging decisions for underlying blockchains. Figure 1. Shows the model's overall flow, where it is apparent that the model initially uses a single chained blockchain for storing access rules. Due to use of blockchain, its inherent characteristics including immutability, rule-traceability, access transparency, and distributed computing are already incorporated into the deployments.

Blockchain also allows the model to integrate access & rule-tracing, that assists in tracking changes for user-to-entity behavioral patterns. But as number of rules & their updates increase, length of block chain increases, which exponentially increases mining delay & complexity, which affects QoS of the cloud deployment. Thus, a GWO model for QoS-aware side chaining is deployed. This model assists in performing 'archive & split' operations on current blockchain, via a QoS-aware dynamic fitness function that incorporates service delay, throughput, access rule characteristics and service consistency metrics. These metrics along with temporal cloud performance are integrated to evaluate final decisions regarding 'archive & split' operations.

To perform these tasks, the model initially converts existing cloud access database into blockchain format via the following process,

- All records from access tables are converted into blocks, and stored on the chain
- To store these records, a recommended block structure is proposed, which can be observed from table 1 as follows,

Table 1 the proposed block structure for access control operations

Previous Hash	Required Node	Required Timestamp	Respective Node	Grant
Current Hash	Meta Data	Grant Timestamp	Nonce	Other Information

- In this structure, information about Previous Hash & Current Hash is stored for traceability, and immutability
- Requesting Node & timestamp of request are also stored
- Along with this, Meta Data & Other Information about the requesting entities are stored for future tracking purposes
- Information related to granting of requests along with its timestamp is stored for validation operations
- A nonce number is stored, which assists in unique identification of hashes

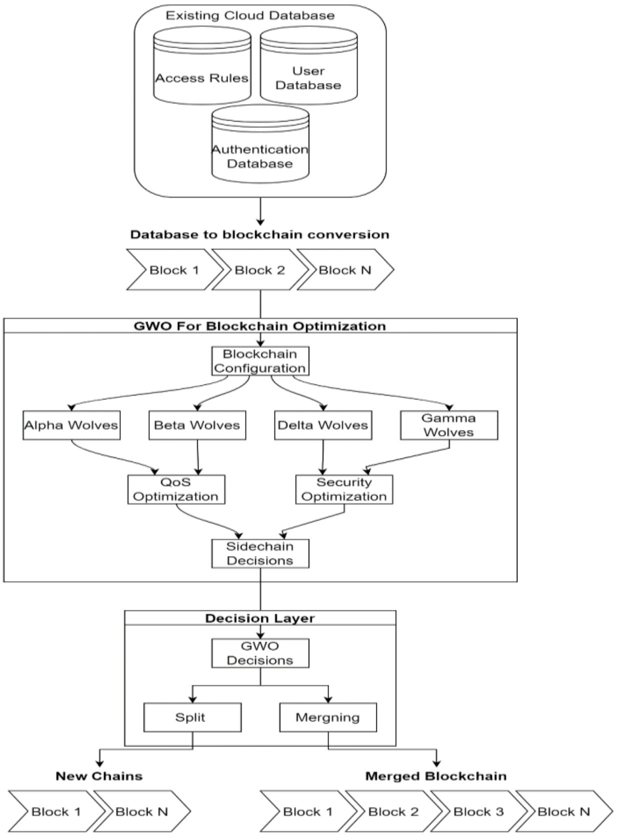

Fig 1. Overall flow of the proposed GWO Based Model

Based on this structure, all access rules are converted into single chained blockchains. These blockchains are further processed via a GWO Model, which assists in making split & merge decisions. The model works via the following process,

- Initially setup the following parameters for GWO,
  - Total GWO Iterations (N_i)
  - Total wolves used to obtain optimum solutions (N_w)
  - Wolf learning rate (W_r)
  - Maximum number of dummy blocks used for evaluation ($MaxN_d$)
  - Total sidechains in the current configuration (N_{sc})
- Initialize all wolves by marking them as 'Delta Wolves'
- Go to each iteration, and scan all wolves in each iteration via following process,
  - If wolf is not marked as 'Delta Wolf', then go to the next wolf in sequence
  - Else, generate new wolf configuration via following process,
    - Add N_d dummy access control blocks to the one of the existing sidechains, and identify wolf fitness via equation 1,

$$f_w = \frac{1}{N_d}\sum_{i=1}^{N_d}\frac{d(mine)_i}{Max(d(mine))} + \frac{e(mine)_i}{Max(e(mine))} + \frac{Max(Thr(mine))}{Thr(mine)_i} \ldots (1)$$

Where, $N_d = STOCH(W_r * MaxN_d, MaxN_d)$, while $d, e\ \&\ Thr$ represents delay of mining, energy needed for mining & throughput of the mining process. $STOCH$ represents a Stochastic Markovian Process, used to generate numbers between given range of inputs.

- Evaluate fitness for each wolf, then estimate iteration fitness threshold via equation 2,

$$f_{th} = \frac{1}{N_w}\sum_{i=1}^{N_w} f_{w_i} * L_w \ldots (2)$$

- Based on this fitness value, mark wolves via the following process,
  - If $f_w < f_{th}$, then mark wolf as 'Alpha Wolf'
  - Else if, $f_w > 3 * f_{th}$, then mark wolf as 'Gamma Wolf'
  - Else if, $f_w > 2 * f_{th}$, then mark wolf as 'Delta Wolf'
  - Else if, $f_w \geq f_{th}$, then mark wolf as 'Beta Wolf'
- Follow this procedure through all iterations, and after the final iteration, evaluate Split & Merge Decision (SMD) via equation 3,

$$SMD = \frac{N(alpha) + N(beta)}{N(Gamma) + N(Delta)} \ldots (3)$$

Where, $N(W)$ represents number of wolves in category W, which is an indicative of Wolf segregation based on their fitness levels. After this, evaluate Split Merge Threshold (SMT) via equation 4,

$$SMT = Max\begin{pmatrix} N(alpha), N(beta), \\ N(Gamma), N(Delta) \end{pmatrix} \ldots (4)$$

Based on the values of $SMD\ \&\ SMT$, perform the following tasks,

- If $SMD \geq L_w * SMT$, then most Wolves have better QoS performance, thus there is no need to split or merge any blockchain
- If $SMD < L_w * \frac{SMT}{2}$, then merge all sidechains selected by the Gamma Wolves, and split current sidechain into 2 equal parts. Use any one of the split sidechains as main blockchain for adding new blocks
- Else, merge all sidechains selected by the Gamma & Delta Wolves, and split current sidechain into 2 equal parts. Use any one of the split sidechains as main blockchain for adding new blocks.

Based on this process, the main blockchain is divided into multiple sidechains, and other sidechains are merged for archival purposes. Due to use of blockchains, the model is capable of reducing mining delay, and improving throughput performance when compared with other sidechaining methods. The following portion of this text compares these models in terms of, energy, delay, throughput, and consistency for various communications.

3. Result evaluation & comparison

The projected model is capable of optimizing sidechain formation delays and improves security via use of GWO based optimization processes. To evaluate performance of this model, it was simulated on the NS2 platform, and matched with recent models, which are discussed in ATLB [13] [14] and QDB ADAM [22] w.r.t. standard network parameters and, values for energy consumption (E), communication delay (D), jitter (J), and throughput (T), were evaluated for all models. These parameters were evaluated via equations 5, 6, 7 & 8 respectively,

$$E = \frac{1}{N_c}\sum_{i=1}^{N_c} E_{start_i} - E_{complete_i} \ldots (5)$$

$$D = \frac{1}{N_c}\sum_{i=1}^{N_c} t_{complete_i} - t_{start_i} \ldots (6)$$

$$J = D - \sum_{i=1}^{N_c}\frac{D_i}{N_c} \ldots (7)$$

$$T = \frac{1}{N_c}\sum_{i=1}^{N_c}\frac{NP_i}{D} \ldots (8)$$

Where, $E_{start}\ \&\ E_{complete}$ represents energy levels while starting & completing communications, while, $t_{complete}\ \&\ t_{start}$ represents timestamp for completion & start of the communications, NP represents number of communicated packets, and N_c represents total number of communications used for evaluation process. To standardize the simulation, these comparisons were made for 1000 communications, with different number of nodes. By employing this technique, the following communication delay may be seen in figure 2, where it is seen, that the suggested model is 18.5% faster than ATLB [13], 19.5% faster than PUF [14], and 15.4% faster than QDB ADAM [22] under different network conditions. Due to which, it can be used for high-speed network deployments.

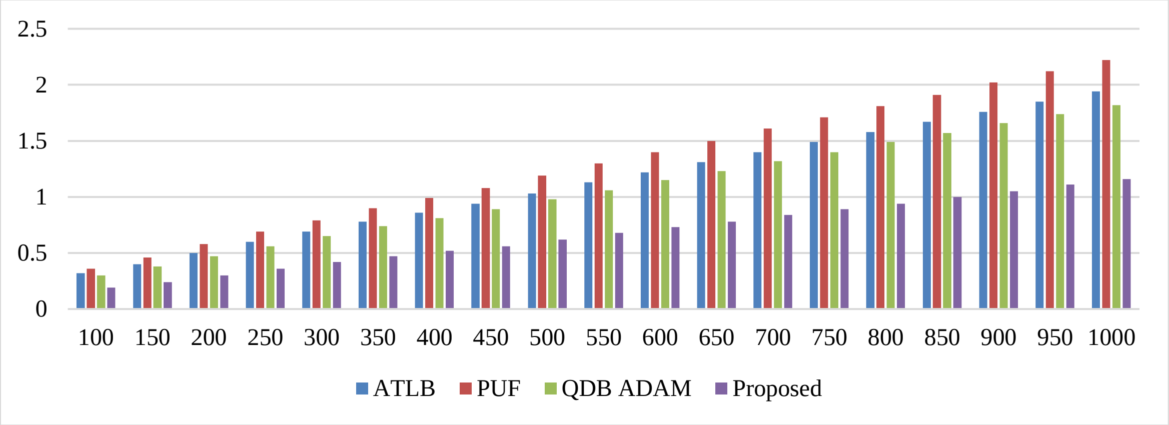

Fig 2. End-to-end delay v/s Number of nodes

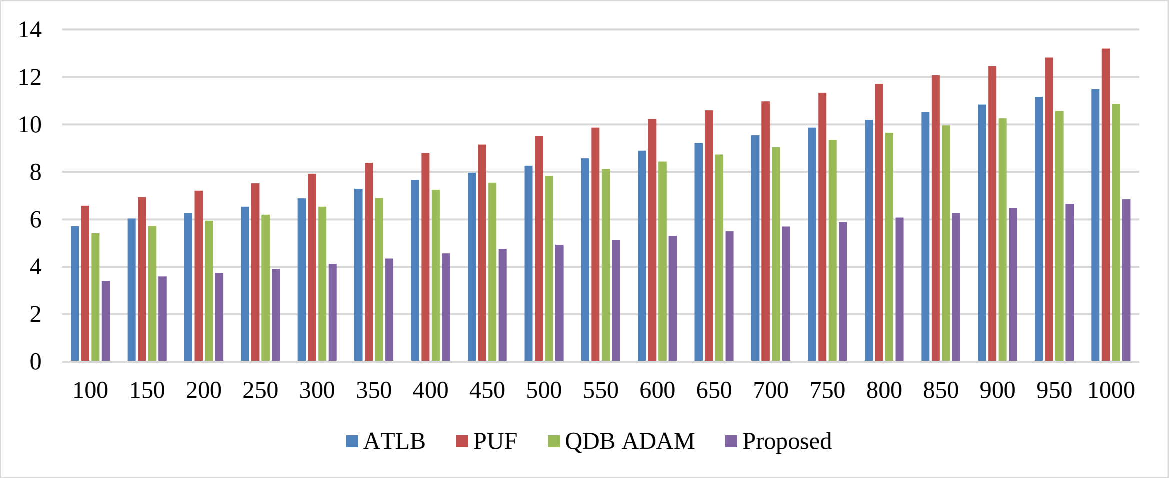

Fig 3. Energy consumption v/s Number of nodes

The primary cause of this improvement is use of delay while identification of sidechains. Similar evaluations were done for energy consumption, and the information below can be seen in figure 3, that the suggested model has an energy efficiency that is 8.5% higher than [13], 9.5% higher than [14], and 8.3% higher than QDB ADAM [22] under different network conditions. Due to which, it can be used for higher lifetime network deployments. The usage of residual energy is the primary driver of this improvement. while identification of sidechains, which assists in selecting sidechains that can be used for low energy operations. Similar evaluations were done for throughput, and figure 4 illustrates where it is perceived that the suggested model is 5.9% higher throughput than ATLB [13], 8.5% higher throughput than [14], and 3.5% higher throughput than QDB ADAM[22] under different network conditions. Due to which, it can be used for higher bandwidth network deployments.

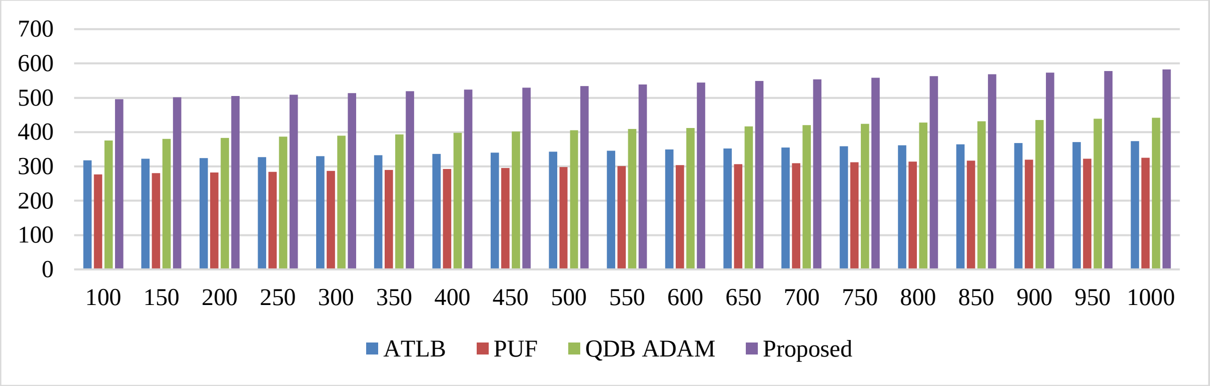

Fig 4. Throughput v/s Number of nodes

The main reason for this improvement is use of throughput while identification of sidechains, which assists in selecting sidechains that can be used for high throughput operations. Similar evaluations were done for network consistency in terms of Jitter, and can be realized from figure 5,where it can be observed that the proposed model is 4.5% consistent than ATLB (X. Wang et al., 2021), 4.6% consistent than [14] and 3.5% consistent than QDB ADAM (D. S. Gupta et al.,2022) under different network conditions. Due to which, it can be used for high stability network deployments.

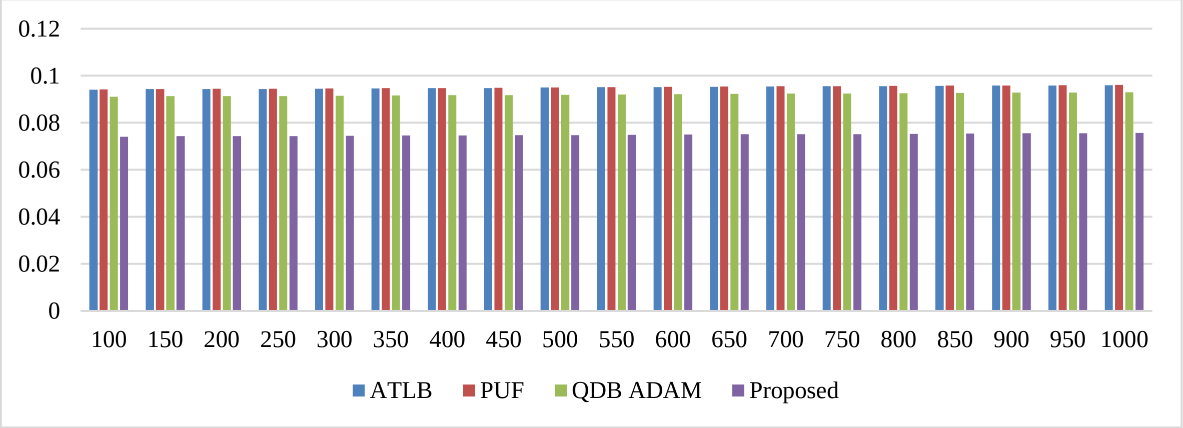

Fig 5. Throughput v/s Number of nodes

The main reason for this improvement is use of delay & throughput while identification of sidechains, which assists in selecting sidechains that can be used for highly scalable operations. Based on similar configurations, the network's performance was evaluated for different authentication & access control attack types.

The sidechain model is capable of mitigating different network attacks. To test it attack detection capabilities & mitigation performance, its QoS performance was evaluated under different authentication & access control attack types. This performance was compared with QoS performance of other models under the following conditions. Based on different attack configurations, the network was simulated for 20% attacker nodes, and its average QoS parameters for communication delay & energy consumption were evaluated, and tabulated in figure 6 where it can be observed that the proposed model is capable of mitigating different attacks, and performs amicably well even under authentication & access control attacks.

Table 2. Different attack configurations

MT	Masquerading & authentication attack with proposed model
DT	Dictionary attack with proposed model
BT	Brute force attack with proposed model
NT	Normal network with proposed model
MA	Masquerading & authentication attack without proposed model

DA	Dictionary attack without proposed model
BA	Brute Force attack without proposed model
NA	Normal network without attacks

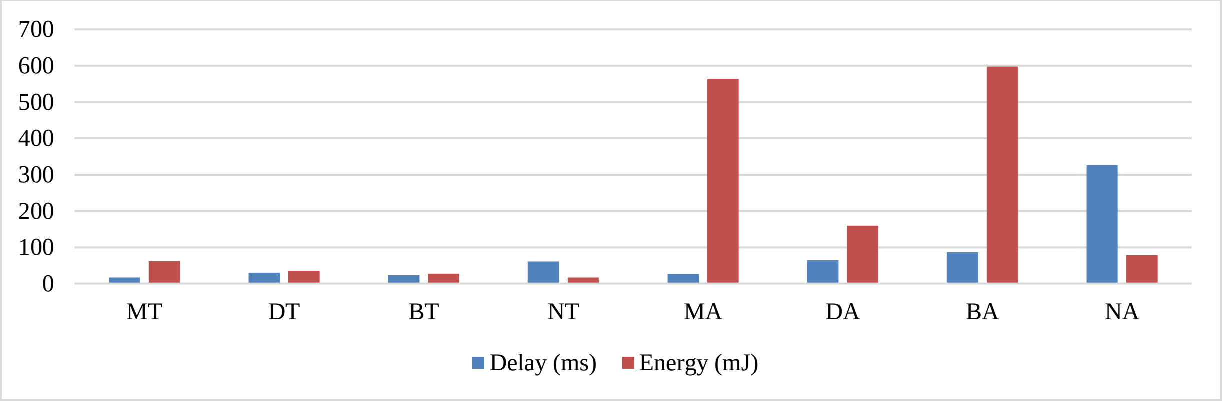

Fig 6. QoS performance under different attack types

This further directs that the projected network model is useful for real-time network deployments.

4. Conclusion

The proposed model initially converts all access control databases into blockchains, and optimizes blockchain performance via use of sidechains. These sidechains are formed via use of GWO Model that contributes to raising QoS performance even under Masquerading, Dictionary & Brute Force attack types. It was also noted that, for various network scenarios, the suggested model demonstrated superior communication performance when compared with other advanced models. The suggested model was observed to be 18.5% faster than ATLB [13] 19.5% faster than PUF [14], and 15.4% faster than QDB ADAM [22] it was also observed to be, is 8.5% higher energy efficient than ATLB [13] 9.5% higher energy efficient than PUF [14] and 8.3% higher energy efficient than QDB ADAM [22] making it extremely beneficial for a wide range of network circumstances. The model was also observed to posses 5.9% higher throughput than ATLB [13]8.5% higher throughput than PUF ([14] and 3.5% higher throughput than QDB ADAM [22], while, it was also observed to achieve 4.5% consistency than ATLB [13]4.6% consistency than PUF [14] and 3.5% consistency than QDB ADAM [22] under different network conditions. Due to which, it can be used for high stability network deployments. This was possible due to use of these parameters while selecting sidechain configurations. The model was also evaluated under different attack types, and its performance was observed to be consistent even under authentication & access control attacks.

Future Scope

In future, the model's performance can be enhanced through use of bioinspired computing models that include Genetic Algorithm, Particle Swarm Optimization, etc. that can be combined to achieve hybrid optimizations. Moreover, use of Auto encoders, Convolutional Neural Networks (CNNs), and other Machine Learning Models (MLMs) is also recommended to improve overall QoS performance while retaining higher security levels for various deployments.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] Garba, Z. Chen, Z. Guan and G. Srivastava, LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme, *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1698-1710, 1 April-June 2021, doi: 10.1109/TNSE.2021.3069128.

[2] Vangala, A. K. Sutrala, A. K. Das and M. Jo, Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming, *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10792-10806, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050676.

[3] Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar and Y. Park, Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems, *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15824-15838, 15 July15, 2021, doi: 10.1109/JSEN.2020.3009382.

[4] Yazdinejad, R. M. Parizi, A. Dehghantanha and K. -K. R. Choo, Blockchain-Enabled Authentication Handover With Efficient Privacy Protection in SDN-Based 5G Networks, *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1120-1132, 1 April-June 2021, doi: 10.1109/TNSE.2019.2937481.

[5] Feng, B. Liu, Z. Guo, K. Yu, Z. Qin and K. -K. R. Choo, Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones, *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224-6238, 15 April15, 2022, doi: 10.1109/JIOT.2021.3113321.

[6] Lin, D. He, X. Huang, N. Kumar and K. -K. R. Choo, BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp. 7408-7420, Dec. 2021, doi: 10.1109/TITS.2020.3002096.

[7] Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz and Y. Park, Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation, *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8092-8107, Aug. 2021, doi: 10.1109/TVT.2021.3091163.

[8] S. Gupta, A. Karati, W. Saad and D. B. da Costa, Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles, *IEEE Transactions on Vehicular Technology,* vol. 71, no. 3, pp. 3255-3266, March 2022, doi: 10.1109/TVT.2022.3144785.

[9] Jhade, S. ., Kumar, V. S. ., Kuntavai, T. ., Shekhar Pandey, P. ., Sundaram, A. ., & Parasa, G. . (2023). An Energy Efficient and Cost Reduction based Hybridization Scheme for Mobile Ad-hoc Networks (MANET) over the Internet of Things (IoT). International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 157–166. https://doi.org/10.17762/ijritcc.v11i2s.6038

[10] Cheng, Y. Chen, S. Deng, H. Gao and J. Yin, A Blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing, *IEEE Transactions on Computational Social Systems,* vol. 9, no. 1, pp. 146-158, Feb. 2022, doi: 10.1109/TCSS.2021.3056540.

[11] Liu, J. Wu and T. Wang, Blockchain-enabled fog resource access and granting, *Intelligent and Converged Networks*, vol. 2, no. 2, pp. 108-114, June 2021, doi: 10.23919/ICN.2021.0009.

[12] Chai, S. Leng, J. He, K. Zhang and B. Cheng, CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-Preserving Authentication in Internet of Vehicles, *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 4620-4631, May 2022, doi: 10.1109/TVT.2021.3132961.

[13] K. Xue, X. Luo, Y. Ma, J. Li, J. Liu and D. S. L. Wei, A Distributed Authentication Scheme Based on Smart Contract for Roaming Service in Mobile Vehicular Networks, *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5284-5297, May 2022, doi: 10.1109/TVT.2022.3148303.

[14] L. Wang, Y. Tian and D. Zhang, Toward Cross-Domain Dynamic Accumulator Authentication Based on Blockchain in Internet of Things, *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2858-2867, April 2022, doi: 10.1109/TII.2021.3116049.

[15] M. Loporchio, A. Bernasconi, D. D. F. Maesa and L. Ricci, Authenticating Spatial Queries on Blockchain Systems, *IEEE Access*, vol. 9, pp. 163363-163378, 2021, doi: 10.1109/ACCESS.2021.3132990.

[16] M. Zhaofeng, M. Jialin, W. Jihui and S. Zhiguang, Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment, *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116-2123, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3037733.

[17] R. Chen et al., BIdM: A Blockchain-Enabled Cross-Domain Identity Management System, *Journal of Communications and Information Networks*, vol. 6, no. 1, pp. 44-58, March 2021, doi: 10.23919/JCIN.2021.9387704.

[18] S. Aggarwal, N. Kumar and P. Gope, An Efficient Blockchain-Based Authentication Scheme for Energy-Trading in V2G Networks, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 6971-6980, Oct. 2021, doi: 10.1109/TII.2020.3030949.

[19] Mrs. Monika Soni. (2015). Design and Analysis of Single Ended Low Noise Amplifier. International Journal of New Practices in Management and Engineering, 4(01), 01 - 06. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/33

[20] S. K. Dwivedi, R. Amin and S. Vollala, Blockchain-Based Secured IPFS-Enable Event Storage Technique With Authentication Protocol in VANET, *IEEE/CAA Journal of Automatica Sinica,* vol. 8, no. 12, pp. 1913-1922, December 2021, doi: 10.1109/JAS.2021.1004225.

[21] S. Son, J. Lee, Y. Park, Y. Park and A. K. Das, Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET, *IEEE Transactions on Network Science and Engineering,* vol. 9, no. 3, pp. 1346-1358, 1 May-June 2022, doi: 10.1109/TNSE.2022.3142287.

[22] W. Liang, D. Zhang, X. Lei, M. Tang, K. -C. Li and A. Y. Zomaya, Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection, *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1410-1420, 1 July-Sept. 2021, doi: 10.1109/TETC.2020.2993032.

[23] W. Wang et al., Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks,*IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883-8891, 1 June1, 2022, doi: 10.1109/JIOT.2021.3117762.

[24] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu and M. S. Hossain, Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7725-7733, Nov. 2021, doi: 10.1109/TII.2021.3049405.

[25] Ms. Pooja Sahu. (2015). Automatic Speech Recognition in Mobile Customer Care Service. International Journal of New Practices in Management and Engineering, 4(01), 07 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/34

[26] X. Yang et al., Blockchain-Based Secure and Lightweight Authentication for Internet of Things, *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3321-3332, 1 March1, 2022, doi: 10.1109/JIOT.2021.3098007.

[27] Y. Yang, L. Wei, J. Wu, C. Long and B. Li, A Blockchain-Based Multidomain Authentication Scheme for Conditional Privacy Preserving in Vehicular Ad-Hoc Network, *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8078-8090, 1 June1, 2022, doi: 10.1109/JIOT.2021.3107443.

[28] Y. Zhang, B. Li, B. Liu, Y. Hu and H. Zheng, A Privacy-Aware PUFs-Based Multiserver Authentication Protocol in Cloud-Edge IoT Systems Using Blockchain, *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13958-13974, 15 Sept.15, 2021, doi: 10.1109/JIOT.2021.3068410.

[29] Khan, W., Haroon, M. An efficient framework for anomaly detection in attributed social networks, *International Journal of information technology* (2022) https://doi.org/10.1007/s41870-022-01044-2

[30] Mahbub, M., Barua, B. Joint energy and latency-sensitive computation and communication resource allocation for multi-access edge computing in a two-tier 5G HetNet, *International Journal of information technology* (2022). https://doi.org/10.1007/s41870-022-01037-1

[31] Kenei, J., Opiyo, E. Semantic modeling and visualization of semantic groups of clinical text documents. *International Journal of information technology*, 2585–2593 (2022). https://doi.org/10.1007/s41870-022-00970-5

[32] Quamara, S., Singh, A.K. SChain: towards the quest for redesigning supply-chain by augmenting Blockchain for end-to-end management. *International Journal of information technology* **,** 2343–2354 (2022). https://doi.org/10.1007/s41870-022-00959-0

[33] Sudhakar, T., Ramalingam, P. & Jagatheswari, S. An improved proxy-vehicle based authentication scheme for vehicular ad-hoc networks. *International Journal of information technology* **,** 2441–2449 (2022). https://doi.org/10.1007/s41870-022-00938-5