International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

BMSQABSE: Design of a Bioinspired Model to Improve Security & QoS Performance for Blockchain-Powered Attribute-based Searchable Encryption Applications

Roshni Bhave[1], Bhakti P. Thakre[2], Vijaya Kamble[3], Purva Gogte[4], Dhananjay Bhagat[5]
[1]Department of Computer Science and Engineering
YeshwantRao Chavan College of Engineering
Nagpur, India
Roshnibhave12@gmail.com
[2]Department of Information Security
Rashtrasant Tukadoji Maharaj Nagpur University
Nagpur, India
Bthakre11@gmail.com
[3]Department of Computer Science and Engineering
GuruNanak Institute of Engineering & Technology
Nagpur, India
researchvijaya7@gmail.com
[4] Department of Computer Science and Engineering
Shri Ramdeobaba College of Engineering and *Management*
Nagpur, India
Purva.gogte1@gmail.com
[5]Department of Artificial Intelligence
G H Raisoni College of Engineering
Nagpur, India
Dhananjaybhagat84@gmail.com

Abstract—Attribute-based searchable encryption (ABSE) is a sub-field of security models that allow intensive searching capabilities for cloud-based shared storage applications. ABSE Models require higher computational power, which limits their application to high-performance computing devices. Moreover, ABSE uses linear secret sharing scheme (LSSS), which requires larger storage when compared with traditional encryption models. To reduce computational complexity, and optimize storage cost, various researchers have proposed use of Machine Learning Models (MLMs), that assist in identification & removal of storage & computational redundancies. But most of these models use static reconfiguration, thus cannot be applied to large-scale deployments. To overcome this limitation, a novel combination of Grey Wolf Optimization (GWO) with Particle Swarm Optimization (PSO) model to improve Security & QoS performance for Blockchain-powered Attribute-based Searchable Encryption deployments is proposed in this text. The proposed model augments ABSE parameters to reduce its complexity and improve QoS performance under different real-time user request scenarios. It intelligently selects cyclic source groups with prime order & generator values to create bilinear maps that are used for ABSE operations. The PSO Model assists in generation of initial cyclic population, and verifies its security levels, QoS levels, and deployment costs under multiple real-time cloud scenarios. Based on this initial analysis, the GWO Model continuously tunes ABSE parameters in order to achieve better QoS & security performance levels via stochastic operations. The proposed BMSQABSE model was tested under different cloud configurations, and its performance was evaluated for healthcare deployments. Based on this evaluation, it was observed that the proposed model achieved 8.3% lower delay, with 4.9% lower energy consumption, 14.5% lower storage requirements when compared with standard ABSE models. It was able to mitigate Distributed Denial of Service (DDoS), Masquerading, Finney, and Sybil attacks, which assists in deploying the proposed model for QoS-aware highly secure deployments.

Keywords-Attribute, Encryption, Searchable, PSO, GWO, Stochastic, Security, QoS

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

I. INTRODUCTION

Attribute based Searchable Encryption (ABSE) requires design of multidomain modules, that include but are not limited to, selective encryption, attribute analysis, access tree generation, search operation modelling, privacy analysis, etc. A typical ABSE model [1] applied to healthcare scenario can be observed from figure 1, wherein data owner sets multiple attributes, that assist in improving access capabilities for other users. In this case, one part of the data is accessible to Math & Doctor entities, while other part is accessible to Computer & Professor entities. These entities and their respective access token are managed via an access tree, which assists in deploying attribute-based search capabilities. Each access token is traversed through the tree and series of 'AND/OR' based rules are applied to these tokens. If attributes stored within these tokens pass the traversal conditions, then access is granted, and users can search the database, else request is discarded and its parameters are reported for future attack identification & control.

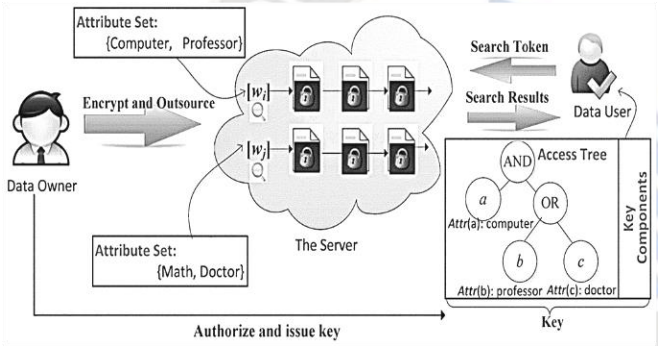

Figure 1. A typical ABSE Model for Hospital Deployments

Similar models along with their nuances, application-specific advantages, context-specific limitations, and deployment-specific future research scopes is discussed in next section [2, 3, 4, 5, 6] of this text. Based on this discussion, it was observed that most of these models use static reconfiguration, thus cannot be applied to large-scale deployments. Due to static reconfiguration, the model showcases good QoS & security performance for a specific type of deployment, but the same ABSE configuration cannot be applied to other deployments. To overcome this limitation, a novel combination of Grey Wolf Optimization (GWO) with Particle Swarm Optimization (PSO) model to improve Security & QoS performance for Blockchain-powered Attribute-based Searchable Encryption deployments is discussed in section 3 of this text. Performance of the model is evaluated in section 4, wherein it is compared in terms of energy consumption, computational delay, storage cost, and attack resilience performance.

II. LITERATURE REVIEW

A large number of characteristically varying models are proposed by researchers for deployment of ABSE systems. For instance, work in [4, 5, 6] propose use of verifiable with multiple keyword searchable attribute-based encryption (VMKS-ABE), and ABE for sharing & retrieval of datasets that are in encrypted domains. These models are highly variant in terms of their performance metrics, thus cannot be used for general purpose ABS applications. To standardize this performance, work in [7] proposes use of Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) that uses a combination of linear classifiers with low complexity models for high efficiency search purposes. The model is used as a baseline for multiple encryption applications, and can be applied to general purpose ABS deployments. It is further extended in [8, 9, 10], where researchers have proposed use of Blockchain-Assisted Secure Fine Grained Searchable Encryption (BAS FGSE), Multiple Authority Ciphertext-Policy Attribute-Based Keyword Search (MAC PAB KS), and Polynomial Search, which assist in integration of blockchains for ABSE applications. But these models do not incorporate privacy preservation techniques while deploying blockchains. To overcome this limitation, work in [11, 12, 13] propose use of Privacy Preserving Searchable Encryption (PPSE), Multiple Value with Independent Ciphertext-Policy ABE (MVIC ABE), and use of fine-tuned search operations under different attribute-based access & ownership control mechanisms. These models are highly optimized for general purpose applications, and can be used for large-scale deployment scenarios.

Other high-efficiency ABE models include ABE with Hierarchical Data [14], Keyword-Based Search with Receiver Anonymity (KeySea), [15], Hidden Policy CP ABE [16], & Identity-Based Personalized Recommendation Model (IBPM), which assist in improving recommendation performance under different attack types. These models are highly useful under multiple attack scenarios, and can be extended via use of ML & AI based methods. Similar methods are discussed in [17, 18, 19, 20], where researchers have proposed use of Lattice based Search, Virtual Environment Search, and Outsourced Data Storage applications, that assist in improving classification performance even under different attack types. these models must be evaluated for other attack types, and can be extended via use of Blockchain-Based Anti-Key-Leakage Key Aggregation (BAK LKA) [21], ABS with Partial Bilinear Map (ABSE PBM) [22], Self-Verifiable ABE [23, 24], and CPABE with keyword search and data sharing (CPAB-KSDS) [25], which assist in incorporating multiple use cases for small, medium & large-scale applications. But, none of these models utilize dynamic reconfiguration rules, due to which their performance is limited when applied to real-time applications. To overcome this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

limitation, next section proposes design of a Bioinspired Model to improve Security & QoS performance for Blockchain-powered Attribute-based Searchable Encryption applications. The model was also evaluated under different attack types, and its QoS performance was compared with other state-of-the-art methods.

III. DESIGN OF A BIOINSPIRED MODEL TO IMPROVE SECURITY & QOS PERFORMANCE FOR BLOCKCHAIN-POWERED ATTRIBUTE - BASED SEARCHABLE ENCRYPTION APPLICATIONS

From the brief literature survey, it was observed that existing models that extend blockchain for ABSE use static reconfiguration, thus cannot be applied to large-scale deployments. Because of these static reconfiguration rules, these models showcase good security & QoS performance for application-specific use cases, but they cannot be applied to other deployments. To overcome these issues limitation, this section proposes design of a hybrid Grey Wolf Optimization (GWO) with Particle Swarm Optimization (PSO) model for general-purpose Security & QoS enhancements when applied to Blockchain-powered Attribute-based Searchable Encryption deployments. Flow of the model is depicted in figure 2, wherein different text-based databases are initially combined with each other using group policies. These models are initially optimized via PSO, which assists in selection of ABSE parameters, and GWO which assists in tuning these parameters, & selection of blockchain configurations for improving overall performance.

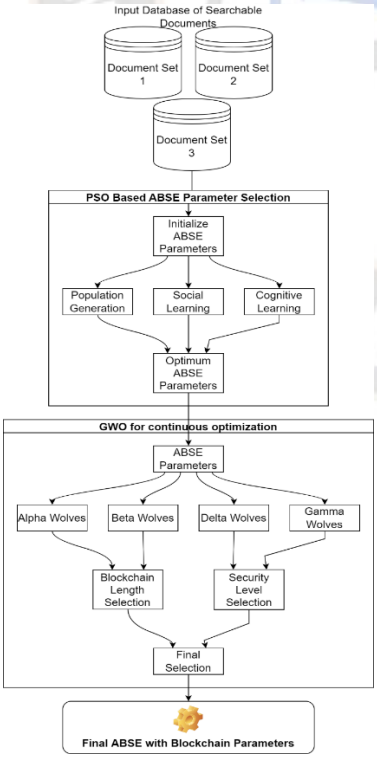

Figure 2. Overall flow of the PSO & GWO based Blockchain ABSE Model

The model design is segregated into 2 different parts, which are described is separate sub sections of this text. After referring these parts, researchers will be able to implement these sub models in part(s), or as a whole, depending upon their application-specific requirements.

IV. DESIGN OF THE PSO BASED ABSE PARAMETER SELECTION LAYER

To integrate ABSE into the model, a Ranked Keyword Searchable Encryption (RKSE) Method was employed, which assisted in estimation of fuzzy rules for improving security and deployment capabilities of underlying databases. The RKSE Method is depicted in figure 3, where input documents are converted into keywords,

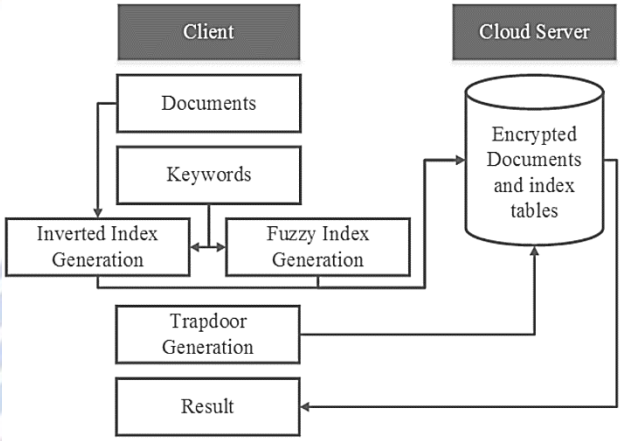

Figure 3. Design of RKSE Model for integration of ABSE

The model initially converts all input documents into keywords via Parts of Speech (PoS) tagging, and generates inverted indices via estimation of Relevance Frequency (RF). This RF value is calculated via equation 1,

$$RF(W,D) = \sum_{t=1}^{W} \frac{1}{D} * (1 + \log_n(f(D,T)) * \log_n\left(1 + \frac{N}{f_T}\right) \dots (1)$$

Where, D represents total number of sentences in the document, $f(D,T)$ represents frequency of word in the document D, T represents current word in the document, N represents total documents in the combined input datasets, while f_T represents frequency of word T in the databases. These RF values are estimated for each input word, and documents are ranked based on these values, which assists in their efficient retrieval under different input query types. The RF values are inverted to generate Inverted Indices, and Fuzzified via equation 2 to generate Fuzzy Indices.

$$F_{index}(W,D) = \frac{RF(W,D) * 3}{Max(\cup_{w=1}^{N} RF(w,D))} \dots (2)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

Both the indices are combined via equation 3 to obtain the final rank index (RI) for each word in the input query,

$$RI(W,D) = \frac{1}{F_{index}(W,D)} + \frac{1}{RF(W,D)} \dots (3)$$

To estimate correct value of RI, it is essential to identify correct database sizes. This is controlled by the variable N, and is estimated via a PSO model that works via the following process,

- Initialize the following PSO parameters,
  - Total number of PSO Particles (N_p)
  - Total number of PSO Iterations (N_i)
  - Cognitive Learning Rate (L_c)
  - Social Learning Rate (L_r)
  - Total documents present in the database (N_{doc})
- Initially generate stochastic population via the following process,
  - Generate stochastic database sizes via equation 4,

$$DB_{size} = STOCH(Max(L_c, L_r) * N_{doc}, N_{doc}) \dots (4)$$

Where, $STOCH$ represents a Markovian Stochastic process.

  - Select the database of size DB_{size}, and then estimate $RI(W,D)$ for each input query.
  - Based on this value of $RI(W,D)$, estimate particle fitness via equation 4,

$$PBest_i = \frac{N_c}{N_t} \dots (4)$$

Where, $PBest$ represents particle best fitness value, while N_c & N_t represents correctly retrieved entries, and total entries which were used for retrieval of input documents.

  - Out of these $PBest$ values, estimate maximum fitness value and use it as Global Best via equation 5,

$$GBest = Max\left(\bigcup_{i=1}^{N_p} PBest_i\right) \dots (5)$$

- For each iteration between 1 to N_i, perform the following tasks,
  - Shift particles to new positions via equation 6,

$$P(New) = P(Old) * s + L_c * (P(Old) - PBest) + L_s(P(Old) - GBest) \dots (6)$$

Where, $P(Old)$ represents old position of the particle (initially $Pbest$), while s represents a stochastic value which is used to move static particles.

  - Update the particle position if $P(New) > PBest$, else discard it
  - Based on the value of $P(New)$ identify value of N_t, which represents size of used databases.
  - If $PBest$ is updated, then update $GBest$ via equation 5, and repeat the process
- At the end of final iteration, identify value of $GBest$, and use its database size for operating ABSE

Based on this process, database sizes for ABSE are evaluated, which assists in selection of relevant cyclic source groups with prime order & generator values for creation of bilinear maps. These maps are further augmented in order to estimate the final ABSE parameters, which are used for high-speed & high-accuracy searchable encryption operations. Results from ABSE are further processed via use of GWO based optimization, which assists in continuous selection of database & blockchain lengths, for high security & high QoS performance under multiple search conditions. Design of this model is discussed in the next section of this text.

V. DESIGN OF THE GWO BASED OPTIMIZATION LAYER FOR ABSE & BLOCKCHAIN DEPLOYMENTS

All input queries & their search results are stored into blockchains for efficient future retrieval. To perform this task, a Proof of Work (PoW) based blockchain model is used, and is optimized via use of a GWO based chain length selection layer. This layer works via the following process,

- Initialize the following GWO parameters,
  - Number of iterations (N_i)
  - Total number of Wolves (N_w)
  - Wolf learning rate (L_r)
- Initially mark all wolves as 'delta wolves'
- For each iteration between 1 to N_i, perform the following tasks,
  - Go to each wolf, and perform the following tasks,
    - If the wolf is marked not marked as 'delta wolf', then skip it and go to the next wolf
    - Else, modify the wolf's configuration via the following process,
      - Generate a blockchain length (L_B) via equation 7,

$$L_B = STOCH\big(N_{PSO}, N_{PSO} * (1 + L_r)\big) \dots (7)$$

Where, N_{PSO} is the database length given by the PSO Model

      - Based on this length, estimate delay to add a block into the chain via equation 8,

$$D_{block} = D_{read} * L_B + D_{verify} * L_B + D_{write} \dots (8)$$

Where, D_{read}, D_{write} & D_{verify} represents reading, writing & verification delays for the blockchain.

      - Using these delay values, estimate wolf fitness via equation 9,

$$f_i = \frac{GBest}{D_{block}} \dots (9)$$

    - Update ABSE database size to L_B, to incorporate more entries for multiple evaluations

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

- Repeat this process for all wolves, and evaluate iteration fitness threshold via equation 10,

$$f_{th} = \sum_{i=1}^{N_w} f_i * \frac{L_r}{N_w} \dots (10)$$

- Mark wolf as 'delta wolf' if $f_i < f_{th} * L_r$, else mark wolf as 'gamma wolf', if $f_i < f_{th} * \frac{L_r}{2}$, else mark wolf as 'beta wolf', if $f_i < f_{th} * \frac{L_r}{4}$, else mark wolf as 'alpha wolf'
- Repeat this process for all iterations, and select 'Alpha Wolf' configuration for tuning the ABSE model performance.

Based on these processes, optimizations are done for both blockchain size & ABSE configurations. Due to these optimizations, the model is capable of showcasing higher QoS & security performance when compared with state-of-the-art methods. This comparison is discussed in the next section of this text.

VI. RESULTS AND STATISTICAL COMPARISON

The proposed BMSQABSE model uses a combination of GWO with PSO to improve QoS & security performance under different real-time conditions. In addition to this, the model is able to enhance the performance of security measures by making use of sidechain-based Internet of Things Network installations. Comparing the quality-of-service metrics of the proposed model with those of BC SABE [2], BAS FGSE [8], and MVIC ABE [12] helps assess the performance of the model. These Internet of Things networks make use of blockchain and other similar technologies in order to enhance the quality of service and security of the underlying network. The models were evaluated on the following databases,

- Stat Log (Heart) Database, which is available at, https://archive.ics.uci.edu/ml/datasets/statlog+(heart)
- Ciphertext Challenge II Dataset, which is available at, https://www.kaggle.com/c/ciphertext-challenge-ii/data
- Amazon Reviews Dataset, which is available at, https://www.kaggle.com/datasets/bittlingmayer/amazonreviews
- Enron Email Dataset, which is available at https://www.cs.cmu.edu/~./enron/

These databases were combined to form a total of 100k entries, which were split into 70:30 ratio for training & testing respectively. To estimate security performance of the model, attacks including man in the middle (MITM), distributed denial of service (DDoS) & worm hole (WH), were introduced, and performance was measured in terms of average of QoS metrics. These metrics include energy consumption (E), end-to-end communication delay (D), storage cost (SC), and throughput (T) for different input queries.

Initially, the QoS performance was evaluated without any attacks, and these metrics were compared with BC SABE [2], BAS FGSE [8], and MVIC ABE [12] models. To evaluate this performance, values for end-to-end delay (D) were estimated w.r.t. Test Search Entries (TSE) for different models and were tabulated in table 1 as follows,

TSE	D (ms) BC SABE [2]	D (ms) BAS FGSE [8]	D (ms) MVIC ABE [12]	D (ms) Proposed
3000	1.64	1.83	2.01	1.44
3600	1.75	1.95	2.13	1.52
4200	1.84	2.05	2.24	1.60
4800	1.93	2.16	2.37	1.70
5400	2.04	2.34	2.61	1.90
6000	2.25	2.74	3.11	2.29
7500	2.76	3.43	3.87	2.85
9000	3.52	4.24	4.69	3.42
12000	4.24	4.91	5.38	3.89
13500	4.75	5.45	5.98	4.33
15000	5.24	6.08	6.68	4.84
16500	5.89	6.82	7.50	5.43
18000	6.59	7.67	8.43	6.02
21000	7.06	8.35	9.16	6.46
24000	7.32	8.77	9.61	6.74
30000	7.55	9.01	9.87	6.96

Table 1. Average delay for processing different test set entries

Based on this evaluation, it can be observed that the proposed model is 10.5% faster than BC SABE [2], 16.5% faster than BAS FGSE [8], and 20.5% faster than MVIC ABE [12] for different number of test set entries. This is possible due to inclusion of delay during selection of blockchain lengths, which assists in shortening the blockchain as per delay requirements. Similar observations were made for energy requirements while processing these requests, and can be observed from table 2 as follows,

TSE	E (mJ) BC SABE [2]	E (mJ) BAS FGSE [8]	E (mJ) MVIC ABE [12]	E (mJ) Proposed
3000	3.99	6.07	5.40	3.97
3600	4.38	6.53	5.77	4.25
4200	4.62	6.91	6.10	4.49
4800	4.89	7.31	6.44	4.74
5400	5.16	7.68	6.75	4.96
6000	5.41	8.01	7.04	5.16
7500	5.62	8.32	7.32	5.38
9000	5.83	8.67	7.67	5.64

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

12000	6.11	9.19	8.14	5.98
13500	6.53	9.79	8.62	6.32
15000	6.93	10.23	8.94	6.52
16500	7.14	10.44	8.87	6.35
18000	7.24	10.59	8.59	5.97
21000	7.42	10.84	8.38	5.64
24000	7.76	11.27	8.72	5.88
30000	8.07	11.70	9.25	6.32

Table 2. Average energy consumption for processing different test set entries

Based on this evaluation, it can be observed that the proposed model is 8.5% energy efficient than BC SABE [2], 15.5% energy efficient than BAS FGSE [8], and 12.5% energy efficient than MVIC ABE [12] for different number of test set entries. This is possible due to use of delay & accuracy while selection of database & blockchain lengths, which assists in modifying the blockchain & ABSE models as per application requirements. Similar observations were made for throughput requirements while processing these requests, and can be observed from table 3 as follows,

TSE	T (kbps) BC SABE [2]	T (kbps) BAS FGSE [8]	T (kbps) MVIC ABE [12]	T (kbps) Proposed
3000	506.51	528.34	610.97	615.96
3600	510.52	532.42	615.71	620.84
4200	514.30	536.76	620.79	626.11
4800	518.85	541.52	626.28	631.62
5400	523.48	546.19	631.72	637.01
6000	527.88	550.74	637.07	642.32
7500	532.28	555.28	642.38	647.62
9000	536.68	559.83	647.64	652.93
12000	541.08	564.38	652.91	658.23
13500	545.48	568.97	658.17	663.54
15000	549.88	573.60	663.43	668.84
16500	554.28	578.23	668.69	674.15
18000	558.68	582.78	673.94	679.43
21000	563.08	587.26	679.15	684.67
24000	567.43	591.73	684.37	689.93
30000	571.76	596.24	689.62	695.21

Table 3. Average throughput for processing different test set entries.

Based on this evaluation, it can be observed that the proposed model has 15.5% higher throughput than BC SABE [2], 16.5% higher throughput than BAS FGSE [8], and 3.5% higher throughput than MVIC ABE [12] for different number of test set entries. This is possible due to minimization of delay while selection of database & blockchain lengths, which assists in modifying the blockchain & ABSE models as per application requirements. Similar observations were made for storage costs requirements while processing these requests, and can be observed from table 4 as follows,

TSE	SC (MB) BC SABE [2]	SC (MB) BAS FGSE [8]	SC (MB) MVIC ABE [12]	SC (MB) Proposed
3000	122.48	121.88	123.25	83.63
3600	123.45	122.82	124.21	84.29
4200	124.37	123.83	125.24	84.99
4800	125.47	124.93	126.35	85.74
5400	126.58	126.01	127.44	86.48
6000	127.65	127.06	128.50	87.20
7500	128.72	128.12	129.56	87.92
9000	129.78	129.17	130.63	88.64
12000	130.85	130.23	131.69	89.36
13500	131.91	131.28	132.76	90.08
15000	132.97	132.34	133.83	90.80
16500	134.03	133.39	134.89	91.52
18000	135.10	134.45	135.95	92.25
21000	136.16	135.49	137.01	92.97
24000	137.21	136.54	138.07	93.69
30000	138.26	137.57	139.12	94.40

Table 4. Average storage cost for processing different test set entries

Based on this evaluation, it can be observed that the proposed model requires 8.5% lower storage than BC SABE [2], 8.3% lower storage than BAS FGSE [8], and 8.5% lower storage than MVIC ABE [12] for different number of test set entries. This is possible due to modification of blockchain & ABSE model sizes as per application requirements. Based on these evaluations, it was observed that proposed model has higher QoS than existing deployments.

To estimate security performance, these evaluations were extended for different number of attacks during ABSE operations. The performance was evaluated via varying number of attackers (NA) between 1% to 10%; and estimating the QoS values for different models. As per this evaluation strategy, values for end-to-end delay (D) for these models under DDoS, MiTM & WH attacks is tabulated in table 5 as follows,

NA	D (ms) BC SABE [2]	D (ms) BAS FGSE [8]	D (ms) MVIC ABE [12]	D (ms) Proposed
1	2.18	2.41	2.32	1.17
1.5	2.32	2.54	2.45	1.24
2	2.45	2.67	2.59	1.32
2.5	2.59	2.87	2.83	1.42
3	2.83	3.25	3.27	1.60
3.5	3.31	3.94	3.98	1.92
4	4.12	4.86	4.86	2.37

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

4.5	5.06	5.78	5.72	2.83
5	5.87	6.57	6.46	3.23
5.5	6.54	7.32	7.19	3.60
6	7.28	8.19	8.05	4.02
6.5	8.17	9.19	9.01	4.51
7	9.15	10.22	9.98	5.02
8	9.88	11.00	10.70	5.40
9	10.33	11.50	11.19	5.65
10	10.64	11.88	11.59	5.84

Table 5. Evaluation of processing delay for different attack types

Based on this evaluation, it can be observed that the proposed model is able to achieve 8.3% faster performance than BC SABE [2], 9.4% faster performance than BAS FGSE [8], and 8.5% faster performance than MVIC ABE [12] for different attack types. This is because the underlying model uses blockchains that integrate transparency, traceability, and immutability characteristics. Similar observations are done for energy performance, this can be observed for different attacks from table 6 as follows,

NA	E (mJ) BC SABE [2]	E (mJ) BAS FGSE [8]	E (mJ) MVIC ABE [12]	E (mJ) Proposed
1	6.16	6.79	6.59	3.03
1.5	6.64	7.25	7.01	3.24
2	7.03	7.66	7.39	3.42
2.5	7.43	8.07	7.77	3.61
3	7.81	8.45	8.13	3.78
3.5	8.14	8.79	8.47	3.94
4	8.46	9.17	8.85	4.10
4.5	8.84	9.64	9.34	4.30
5	9.35	10.23	9.89	4.56
5.5	9.94	10.76	10.33	4.80
6	10.36	11.01	10.39	4.92
6.5	10.41	10.55	9.86	4.77
7	9.51	9.74	9.27	4.41
8	8.68	9.47	9.28	4.25
9	8.75	10.03	9.91	4.44
10	9.66	10.92	10.64	4.83

Table 6. Evaluation of energy requirements for different attack types

Based on this evaluation, it can be observed that the proposed model is able to reduce energy consumption by 15.5% when compared with BC SABE [2], 20.5% when compared with BAS FGSE [8], and 19.5% when compared with MVIC ABE [12] for different attack types. This is because the underlying model uses blockchains that integrate transparency, traceability, and immutability characteristics. Similar observations are done for throughput performance, this can be observed for different attacks from table 7 as follows,

NA	T (kbps) BC SABE [2]	T (kbps) BAS FGSE [8]	T (kbps) MVIC ABE [12]	T (kbps) Proposed
1	688.53	733.10	700.34	905.94
1.5	693.92	738.94	706.01	913.15
2	699.52	745.19	712.03	920.79
2.5	705.70	751.72	718.22	928.87
3	711.82	758.12	724.31	936.82
3.5	717.78	764.44	730.33	944.63
4	723.74	770.75	736.35	952.43
4.5	729.70	777.06	742.37	960.24
5	735.65	783.38	748.39	968.05
5.5	741.60	789.70	754.41	975.86
6	747.55	796.02	759.62	983.32
6.5	753.51	799.11	744.58	980.76
7	759.46	799.59	713.75	970.34
8	763.86	784.80	678.03	969.81
9	769.37	787.08	681.80	979.54
10	774.83	791.32	699.38	996.40

Table 7. Evaluation of throughput requirements for different attack types

Based on this evaluation, it can be observed that the proposed model is able to improve search throughput by 25.5% when compared with BC SABE [2], 23.8% when compared with BAS FGSE [8], and 28.5% when compared with MVIC ABE [12] for different attack types. This is because the underlying model uses blockchains that integrate transparency, traceability, and immutability characteristics, which assists in mitigation of multiple attack types. Similar observations are done for storage cost, and can be observed for different attacks from table 8 as follows,

NA	SC (MB) BC SABE [2]	SC (MB) BAS FGSE [8]	SC (MB) MVIC ABE [12]	SC (MB) Proposed
1	98.93	94.79	104.06	90.96
1.5	99.72	95.52	104.87	91.68
2	100.45	96.29	105.74	92.45
2.5	101.34	97.15	106.67	93.27
3	102.24	97.99	107.59	94.06
3.5	103.11	98.81	108.50	94.84
4	103.97	99.63	109.40	94.98
4.5	104.83	100.45	110.29	95.12
5	105.68	101.27	111.18	95.25
5.5	106.54	102.09	112.08	96.01
6	107.40	102.92	112.98	96.78
6.5	108.26	103.74	113.89	97.55
7	109.13	104.56	114.79	98.32
8	109.98	105.37	115.68	99.09
9	110.83	106.18	116.57	99.67
10	111.68	106.99	117.46	100.19

Table 8. Evaluation of storage cost for different attack types

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.7114
***Article Received**: 18 March 2023 **Revised**: 20 May 2023 **Accepted**: 31 May 2023*

Based on this evaluation, it can be observed that the proposed model is able to reduce storage cost by 10.5% when compared with BC SABE [2], 9.5% when compared with BAS FGSE [8], and 14.5% when compared with MVIC ABE [12] for different attack types. This is because the underlying model uses dynamic length blockchains that integrate transparency, traceability, and immutability characteristics, which assists in mitigation of multiple attack scenarios. Thus, the proposed model showcases higher QoS & security performance under different types of attack scenarios, and can be used for real-time application deployments

VII. CONCLUSION

The proposed model uses a combination of dynamic length blockchains with modifiable fuzzy searchable encryption that assists in improving its security & QoS performance under different attack types. The model uses PSO for estimation of ABSE parameters, which is followed by GWO that assists in estimation of blockchain length along with fine tuning of ABSE parameters. Due to these ABSE based optimization operations, the model is capable of showcasing better QoS performance when compared with other state-of-the-art methods. The model is also capable of showcasing higher security due to use of GWO for blockchain optimizations. Due to these operations, the model showcases 10.5% faster performance than BC SABE [2], 16.5% faster performance than BAS FGSE [8], 20.5% faster performance than MVIC ABE [12], 8.5% lower energy than BC SABE [2], 15.5% lower energy than BAS FGSE [8], 12.5% lower energy than MVIC ABE [12], 15.5% higher throughput than BC SABE [2], 16.5% higher throughput than BAS FGSE [8], 3.5% higher throughput than MVIC ABE [12], and requires 8.5% lower storage than BC SABE [2], 8.3% lower storage than BAS FGSE [8], 8.5% lower storage than MVIC ABE [12] for different number of test set entries. This performance was also observed to be consistent when the model was evaluated under Worm Hole, DDoS, and MiTM attack types. Under these attacks, the model showcased 8.3% faster performance than BC SABE [2], 9.4% faster performance than BAS FGSE [8], 8.5% faster performance than MVIC ABE [12], 15.5% lower energy consumption when compared with BC SABE [2], 20.5% lower energy consumption when compared with BAS FGSE [8], 19.5% lower energy consumption when compared with MVIC ABE [12], improves search throughput by 25.5% when compared with BC SABE [2], 23.8% when compared with BAS FGSE [8], 28.5% when compared with MVIC ABE [12], and reduce storage cost by 10.5% when compared with BC SABE [2], 9.5% when compared with BAS FGSE [8], and 14.5% when compared with MVIC ABE [12] for these attack types. Due to which, the model is capable of deployment for a wide variety of real-time scenarios. In future, the model's performance must be validated for different attack types, and can be improved via integration of Q-Learning, and incremental learning, which will assist in feedback-based learning under a wide variety of real-time conditions. Moreover, the model must be integrated with other bioinspired techniques, & Convolutional Networks, which will further assist in improving their search efficiency under different input types.

REFERENCES

[1] L. Zhang, J. Su and Y. Mu, "Outsourcing Attributed-Based Ranked Searchable Encryption With Revocation for Cloud Storage," in IEEE Access, vol. 8, pp. 104344-104356, 2020, doi: 10.1109/ACCESS.2020.3000049.

[2] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang and B. Yan, "BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7851-7867, Sept. 2020, doi: 10.1109/JIOT.2020.2993231.

[3] S. Wang, L. Yao, J. Chen and Y. Zhang, "KS-ABESwET: A Keyword Searchable Attribute-Based Encryption Scheme With Equality Test in the Internet of Things," in IEEE Access, vol. 7, pp. 80675-80696, 2019, doi: 10.1109/ACCESS.2019.2922646.

[4] S. Wang, S. Jia and Y. Zhang, "Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage," in IEEE Access, vol. 7, pp. 50136-50147, 2019, doi: 10.1109/ACCESS.2019.2910828.

[5] J. Sun, L. Ren, S. Wang and X. Yao, "Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage," in IEEE Access, vol. 7, pp. 66655-66667, 2019, doi: 10.1109/ACCESS.2019.2917772.

[6] Mittal, P. ., & Navita. (2023). Early-Stage Detection of Covid-19 Patient using ML Model: A Case Study. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 84–89. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2480.

[7] M. Morales-Sandoval, M. H. Cabello, H. M. Marin-Castro and J. L. G. Compean, "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud," in IEEE Access, vol. 8, pp. 170101-170116, 2020, doi: 10.1109/ACCESS.2020.3023893.

[8] Anthony Thompson, Ian Martin, Alejandro Perez, Luis Rodriguez, Diego Rodríguez. Utilizing Machine Learning for Educational Game Design. Kuwait Journal of Machine Learning, 2(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/183.

[9] H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," in IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484-494, 1 April-June 2020, doi: 10.1109/TCC.2017.2769645.

[10] Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1877-1890, December 2021, doi: 10.1109/JAS.2021.1004003.

[11] Y. Miao, R. H. Deng, X. Liu, K. -K. R. Choo, H. Wu and H. Li, "Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 1667-1680, 1 July-Aug. 2021, doi: 10.1109/TDSC.2019.2935044.

[12] S. Niu, L. Chen, J. Wang and F. Yu, "Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain," in IEEE Access, vol. 8, pp. 7195-7204, 2020, doi: 10.1109/ACCESS.2019.2959044.

[13] P. Chaudhari and M. L. Das, "Privacy Preserving Searchable Encryption with Fine-Grained Access Control," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 753-762, 1 April-June 2021, doi: 10.1109/TCC.2019.2892116.

[14] H. Wang, X. Dong and Z. Cao, "Multi-Value-Independent Ciphertext-Policy Attribute Based Encryption with Fast Keyword Search," in IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1142-1151, 1 Nov.-Dec. 2020, doi: 10.1109/TSC.2017.2753231.

[15] H. Yin et al., "CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme," in IEEE Access, vol. 7, pp. 5682-5694, 2019, doi: 10.1109/ACCESS.2018.2889754.

[16] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang and J. Zhang, "Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing," in IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 985-998, 1 Nov.-Dec. 2020, doi: 10.1109/TSC.2017.2757467.

[17] Pande, S. D., Kanna, R. K., & Qureshi, I. (2022). Natural Language Processing Based on Name Entity With N-Gram Classifier Machine Learning Process Through GE-Based Hidden Markov Model. Machine Learning Applications in Engineering Education and Management, 2(1), 30–39. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/22.

[18] P. Chaudhari and M. L. Das, "KeySea: Keyword-Based Search With Receiver Anonymity in Attribute-Based Searchable Encryption," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 1036-1044, 1 March-April 2022, doi: 10.1109/TSC.2020.2973570.

[19] J. Gao and F. Zhou, "An Encrypted Cloud Email Searching and Filtering Scheme Based on Hidden Policy Ciphertext-Policy Attribute-Based Encryption With Keyword Search," in IEEE Access, vol. 10, pp. 8184-8193, 2022, doi: 10.1109/ACCESS.2021.3136331.

[20] H. Yin, Y. Xiong, T. Deng, H. Deng and P. Zhu, "A Privacy-Preserving and Identity-Based Personalized Recommendation Scheme for Encrypted Tasks in Crowdsourcing," in IEEE Access, vol. 7, pp. 138857-138871, 2019, doi: 10.1109/ACCESS.2019.2943114.

[21] L. Liu, S. Wang, B. He and D. Zhang, "A Keyword-Searchable ABE Scheme From Lattice in Cloud Storage Environment," in IEEE Access, vol. 7, pp. 109038-109053, 2019, doi: 10.1109/ACCESS.2019.2928455.

[22] Y. Yu, J. Shi, H. Li, Y. Li, X. Du and M. Guizani, "Key-Policy Attribute-Based Encryption With Keyword Search in Virtualized Environments," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1242-1251, June 2020, doi: 10.1109/JSAC.2020.2986620.

[23] M. Zeng, H. Qian, J. Chen and K. Zhang, "Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 426-438, 1 Jan.-March 2022, doi: 10.1109/TCC.2019.2944367.

[24] Chaudhary, D. S. . (2021). ECG Signal Analysis for Myocardial Disease Prediction by Classification with Feature Extraction Machine Learning Architectures. Research Journal of Computer Systems and Engineering, 2(1), 06:10. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/12.

[25] J. Niu, X. Li, J. Gao and Y. Han, "Blockchain-Based Anti-Key-Leakage Key Aggregation Searchable Encryption for IoT," in IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1502-1518, Feb. 2020, doi: 10.1109/JIOT.2019.2956322.

[26] S. Khan et al., "ABKS-PBM: Attribute-Based Keyword Search With Partial Bilinear Map," in IEEE Access, vol. 9, pp. 46313-46324, 2021, doi: 10.1109/ACCESS.2021.3068194.

[27] Natalia Volkova, Machine Learning Approaches for Stock Market Prediction , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[28] K. Gu, W. Zhang, X. Li and W. Jia, "Self-Verifiable Attribute-Based Keyword Search Scheme for Distributed Data Storage in Fog Computing With Fast Decryption," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 271-288, March 2022, doi: 10.1109/TNSM.2021.3123475.