ACCESSING AND SHARING SECURED HEALTH-CARE FILES OVER CLOUD BY IMPLEMENTING BLOCKADING

Dr.K.Ketzial Jebaseeli[1]
Assistant Professor[1]
Department of Information Technology[1]
School of Computing Science[1]
KPR College of Arts Science and Research[1]
ketzialjebaseeli.k@kprcas.ac.in[1]

Abstract

Curtailing the overload usage of cloud by incorporating several methodologies which will also assist in the sustaining of the records safely is being deliberated skillfully. Especially in the field of medical management, convenient and proper coordination of data could be agreed upon by practicing the schemes that are codified here. The principal intention is to take down the time and expenditure appropriated heretofore. In an enormous league where the data is quite extensive as in health service institutions, preserving the delicate information amongst a group of working staffs is quite challenging. Highly fortified security system is the radical imperative of the today's novel world. In this configuration, outsourcing of data in cloud is insured with tightened security by categorizing the files with data individually and aggregating the key, this could be done by following the procedure of ensemble signature. A lightweight data preserving model using ensemble signature scheme to the outsourced health files in cloud is employed here for the protection of files. This will mitigate the time taken to decrypt the data that is encrypted and conserved. The grouped files containing the user information separately has to be scrutinized in order to find the required material, the process of utilizing the search scheme acknowledged as k-vertex is integrated as the following methodology of Accessing dynamic health records using K-Vertex search scheme model towards hierarchical users in cloud servers. BMSA the blockade maneuver sequence amplification is assimilated to faultlessly contrive or schematize the warranted healthcare files are laboured for an effective application and usage in this research work.

Key Words: Cloud ,Encryption Decryption, K-Vertex, BMSA, Security
DOI Number:10.14704/nq.2022.20.8.NQ44470 NeuroQuantology 2022; 20(8): 4368-4378

I.INTRODUCTION

The safety concerns regarding the stored files by the data owners pressurize them as there are ample numbers of users across the globe. Cloud computing has made to be conspicuous amidst others in the secure functioning of the outsourced files. This is conceivable with a highly immune system of encryption procedure where the data could never be exploited in any way. The misappropriation of the

information midway is imaginable in the contemporary setup which in turn results in the excessive consumption of time where deciphering the document are a regular process. The achievement of the desired proceeds is rendered by discounting the time take for decryption. The deployment of the data is performed by fabricating a group with the authenticated users with the provision of signatures with which the access of the documents is made viable. The ensuing project entities ensure a detailed knowledge of no trouble access to the secured document that is outsourced.

2. RELATED WORK

Liang and D.S. Wong, 2013 adduced certain solutions to surmount confrontations arising while piling up data in cloud. Symmetrical keys mutilated to form a tree structure in indiscriminate cyclic and acyclic extending archetype. This approach enabled the accession of files by deflating encryption time and file ingression interludes by the use of tree structure. R. Canetti and S. Hohenberger, 2014 discussed exceptional information in cryptography by using sensible applications as email and storage dispersion.

A competent configuration is made by referring bilinear Diffie-Hellman model.J.F.Wang and X.F. Chen, 2015 demonstrated a technology that consumes no wires as it becomes groundwork for the wireless and sensor based technology. From these, heterogeneous environment that is wireless is enumerated in order to formulate it as cost efficient, resourceful and flexible. An additional integrity scheme has been proposed by using homomorphism marks and BLS signature. Storing in cloud has been made more reliable by the use of this wireless data transmission. Malicious data providers are also accessed to gain specific information without any threats. O.William Grut, 2016 proceeded to deal with the Eistenian-espace, an authority to be dealt with the space organization that budges guard time technologies. This system depicts how a block chain is ingressed into guard time that bestows private network to citizens and provides permission to users to check into each file for accession. Each user updates a file into the access or that further formulates into authentication.

3. RESEARCH METHODOLOGY

In the below figure 1 advocating methodology which incorporates three found facets that are highly provisioned with tight security to the data provided. Organizing the data in necessary groups is effected which assisted in reducing the time considerably and also has enhanced the safety of the underlying data to a great extent.

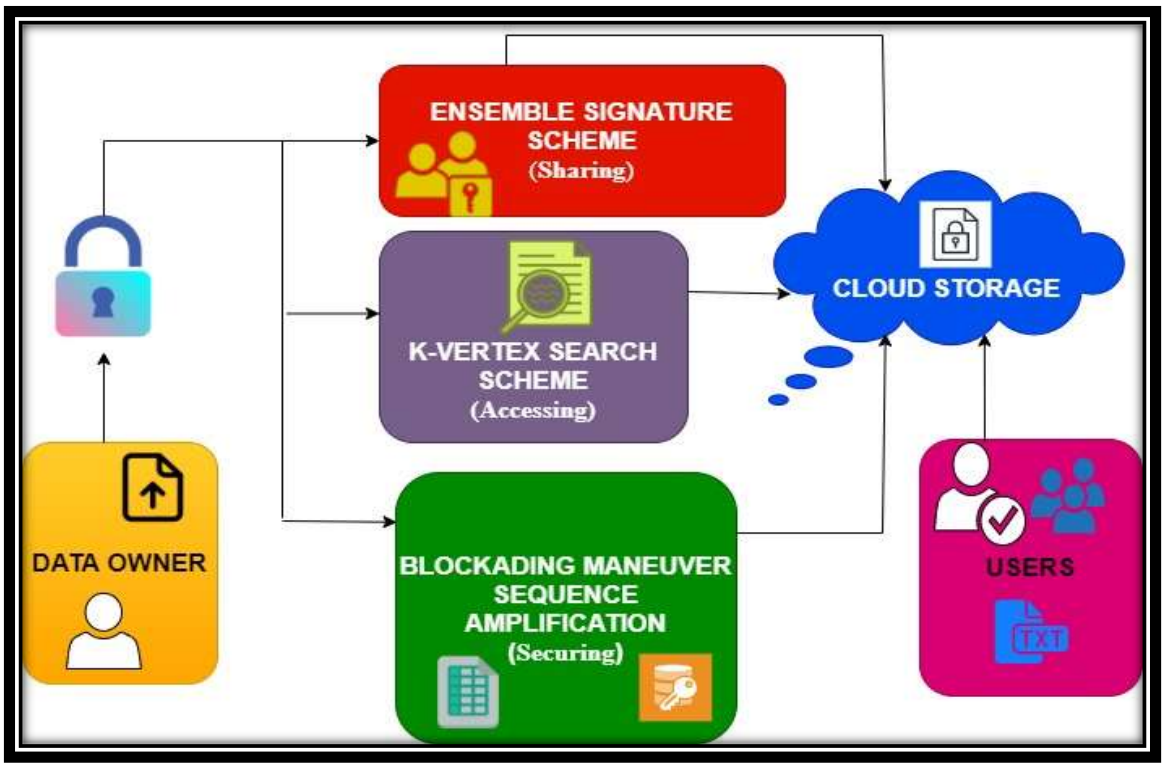

Figure 1 Architecture Diagram-Phases

3.1 Phase I ENSEMBLE SIGNATURE SCHEME

The safe keeping of the documents is intensified by the embodiment of the Attribute based Encryption approach in this stage. Aligning the members in groups with the help of ring signatures has been a distinguished function in maintaining the data security. Instituting an aggregate key along with the edging in of files in a hierarchical structure has maintained the safety of the data in a comfortable way. The users are accredited with the ring signatures through the involvement of multiple key usage and Cryptosystem, which clinches a shielded hashing and hierarchy setup for the data owner. The radical action of this research scheme is that it lessens the multiple decryptions into one which supports the cutback of the time taken for decryption along with the computational costs.

3.2 Phase II K-VERTEX SEARCH SCHEME

This proposed model enhances an element called k-vertex that performs primary aspect in accessing each file. This technique use files accession to be encrypted that is of user-desired file access. The k-vertex search scheme works out with an arrangement that is descending in order to perform file security at the time of decryption. Multi-keyword search in cipher text policy hierarchical encryption is represented in terms of TF*IDF illustration, whereas TF denotes term frequency and IDF as inverse document frequency. Encryption is formulated by AES algorithm for enhanced and secluded data storage. The competent data provides enhanced automation for the purpose of trap door generation. Vector erection builds up the query efficiency in accordance with the hierarchical arrangements that are made. This system enables flexible usage to abrupt data abuser and searches for even a single data and not

always multiple data.

3.3 Phase III BMSA

BMSA is a feature where the files are split into blocks for encryption. It allows in two configurations, the content in each block are displayed and users are consented to read entire block. The data stored in the files are ingressed out two at a time. These two records of classification lead to access of files and splitting into blocks. Each key generated is formulated by threshold value (Ti) and number of lines to be counted (Li) as Li/Ti. Blockading maneuver sequence amplification endows claimant item set (Ci) and recurrent item set (Ri) from where the entity conforms to token generation. Whenever a value is passed in the recurrent set, if equals enters into non-matched item set in the temporary cache. Files that are separated into blocks are accessed and decrypted in a secured way thereby lowering its time period and cost reduction even more. Aggregate value of one block is enumerated for the value obtained in the absolute block.

4. EXPERIMENTAL RESULTS

The proposed investigate work segregates into three modules where the data stored in cloud are encrypted in a secluded manner. Each data into the file are accessed for decryption to enumerate the resultant decrypted data file. Files are accessed of user's desire and secured highly through blockading partitioning (BMSA).The results are illustrated below in Table 1 and Figure 2.

Technique	Health Records _10_ Files in seconds	Health Records _40_ Files in seconds	Health Records _70_ Files in seconds	Health Records _100_ Files in seconds	Health Records _200_ Files in seconds	Health Records _300_ Files in second	Health Records_500_ Files in seconds
File Hierarchy Attribute based Encryption (FH-ABE)	110	540	860	1287	2574	3861	6435
Ensemble Signature Scheme	120	570	810	1200	2400	3600	6000
K-Vertex Search Scheme	115	250	335	550	1100	1650	2750
Blockading Maneuver Sequence Amplification(BMSA)	**125**	**250**	**305**	**500**	**1000**	**1500**	**2500**

Table I: Overall Decryption Seconds of FH-ABE, Ensemble Signature Scheme, K-Vertex Search Scheme, BMSA

*e*ISSN1303-5150 www.neuroquantology.com

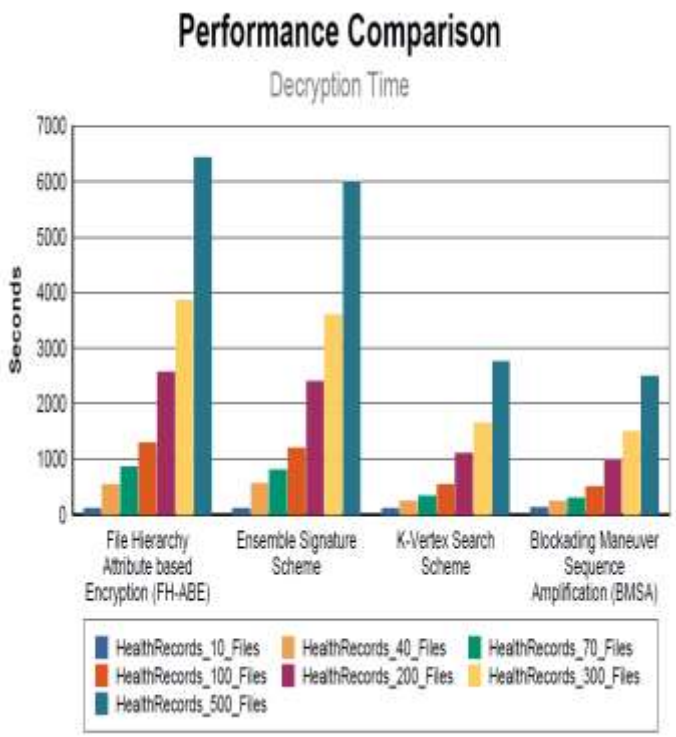

Figure 2. Comparison of performance in decryption time

Table 1 is the comparison of decryption seconds undertaken by each methodology for file hierarchy in health records respectively. Each technique has lessened its decryption time to the number of files accessed. Performance is higher in BMSA as it has an abrupt reduction in its decryption time when compared to the other above techniques encompassed. From figure 1 it is evidently proved that BMSA provides the least number of seconds as 125s and for large files as 2500s. BMSA has the least decryption time because blockading partition has been undergone by each file that is to be accessed for encryption. The files are splitting up into blocks that further leads to ingression through blockading maneuver. Additional results are shown in Table 2.

Technique	**Health Records _10_ Files in Bytes**	**Health Records _40_ Files in Bytes**	**Health Records _70_ Files in Bytes**	**Health Records _100_ Files in Bytes**	**Health Records _200_ Files in Bytes**	**Health Records _300_ Files in Bytes**	**Health Records _500_ Files in Bytes**
File Hierarchy	185,042	740,169	1,295,296	1,850,424	3,700,848	5,551,272	9,252,120

Attribute based Encryption (FH-ABE)							
Ensemble Signature Scheme	145,042	580,169	1,015,296	1,450,424	2,900,848	4,351,272	7,252,120
K-Vertex Search Scheme	72,521	290,084	507,648	725,212	1,450,424	2,175,636	3,626,060
Blockading Maneuver Sequence Amplification(BMSA)	**70,021**	**280,084**	**490,148**	**700,212**	**1,400,424**	**2,100,636**	**3,501,060**

Table 2: Decryption Memory Comparison of FH-ABE, Ensemble Signature Scheme, K-Vertex Search Scheme, BMSA

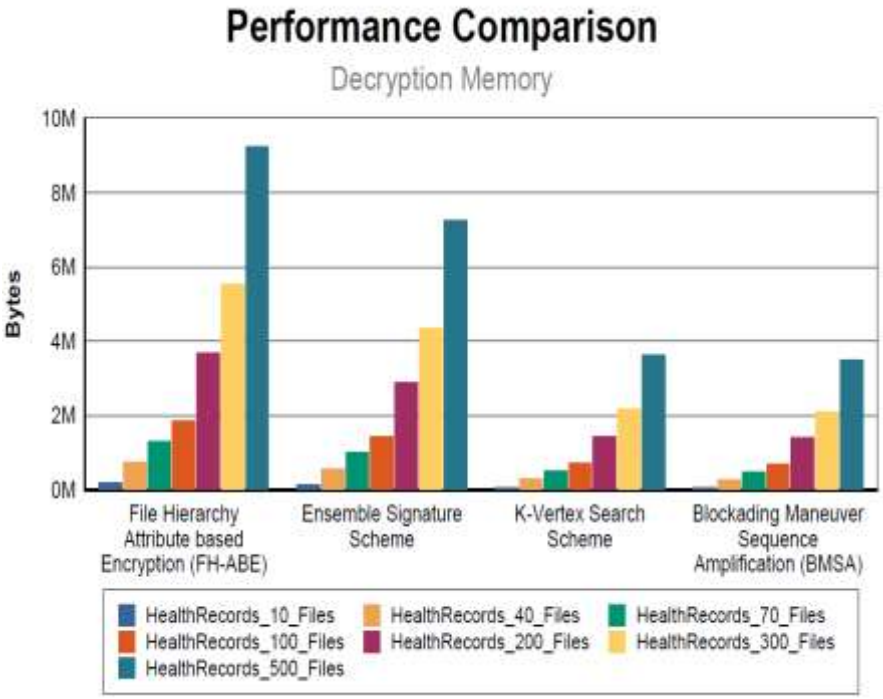

Figure 3. Performance comparison of Decryption memory

It is clearly assumed form Table 2 that the memory stored is randomly differed in health records to 100 files in decryption memory. Each technique is varied in storing memory preceding afterwards its decryption. The least memory is 50% while drastic storage of 90% of its memory is stored in BMSA. From the above figure 2, each technique is processed into comparison from file hierarchy including ensemble signature and BMSA the memory stored is contrasted and put in performance where the large lead to FH-ABE and accurate storage in BMSA as it infers file storage and file partition into blocks as well. On comparing the techniques with storage, reduction cost and memory, BMSA practically checks out and passes all the categories than others. It is quite impossible and impractical to store the most amounts of memories in CP-ABE rather accumulating in BMSA. Table 3 depicts the results at the time of retrieval in four major techniques.

Technique	**Health Records _10_ Files in %**	**Health Records _40_ Files in %**	**Health Records _70_ Files in %**	**Health Records _100_ Files in %**	**Health Records _200_ Files in %**	**Health Records _300_ Files in %**	**Health Records _500_ Files in %**
File Hierarchy Attribute based Encryption (FH-ABE)	5%	20%	35%	50%	55%	57%	60%
Ensemble Signature Scheme	7%	26%	45%	55%	62%	67%	70%
K-Vertex Search Scheme	9%	34%	59%	62%	68%	72%	85%
Blockading Maneuver Sequence Amplification (BMSA)	**9%**	**38%**	**66%**	**70%**	**73%**	**85%**	**95%**

Table 3: File Retrieval Result of FH-ABE, Ensemble Signature Scheme, K-Vertex Search Scheme, BMSA

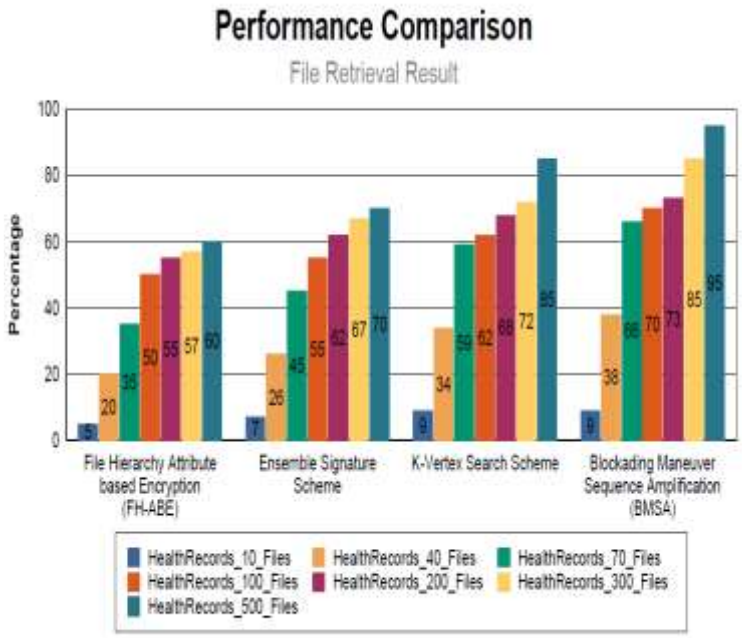

Figure 4. Performance comparison of File retrieval result

5. CONCLUSION

The decryption time and cost decrease differ when comparing each technique individually. Time required for decryption varies depending on the mechanism used when files are accessed for encryption and stored in the cloud after encryption. The method under consideration offers an effective and efficient use in a variety of industries, particularly healthcare, despite the fact that the technique under consideration has an inefficient feature. The earlier approaches are not used as frequently and cannot defeat the BMSA strategy that has been eventually proposed. A significant benefit in file encryption methods has been deduced from splitting files into blocks and then gaining access to them for decryption.

REFERENCES

1. K. Liang, Q. Huang, R. Schlegel, D. S. Wong, C. Tang, “A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release,” In Proc. Information Security Practice and Experience, pp. 132-146, Springer Berlin Heidelberg, 2013.
2. R. Canetti and S. Hohenberger, “Chosen-Ciphertext Secure Proxy Re-Encryption,” in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS ’07). ACM, 2007, pp. 185–194.
3. J. F. Wang, X. F. Chen, J. Li, J. L. Zhao, and J. Shen, “Towards achieving flexible and verifiable search for outsourced database in cloud computing” Future Generation Computer Systems, vol. 67, February2017,pp. 266-275.
4. J.Hur,”Improving Security and Efficiency in attribute-based data sharing”, IEEE Transaction on Knowledge and Data Engineering, vol.25, no.10, pp.2271-2282, August 2013.
5. K.Ketzial Jebaseeli,V.G.Rani, ”A Lightweight Data Preserving model using Ensemble Signature scheme to the Outsourced health files in

cloud", Journal of Advanced Research in Dynamical and Control Systems, ISSN 1943-023X,Vol 11, No.02-Special Issue, March 2019. pp. 253-261.

6. Ketzial Jebaseeli, V.G.Rani, "Accessing Dynamic Health Records Using K-Vertex Search Scheme Model towards Hierarchical Users mod Obscure Servers", International Journal of Recent Technology and Engineering, ISSN: 2277-3878, Vol 8, Issue-3, September 2019. pp 3474-3479. DOI: 0.35940/ijrte.C5237.098319
7. K.Ketzial Jebaseeli, V.G.Rani "Schematizing Insured Healthcare Dossiers in Cloud using Blockading Maneuver Sequence Amplification (BMSA)", International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Vol 9, Issue-2, December 2019. pp 252-258. K.Ketzial Jebaseeli, V.G.Rani, "Survey on Techniques of Encryption for Cloud Storage Security", International Journal of Creative Research Thoughts, ISSN: 2320-2882, Vol 6, Issue 2, April 2018. Pp.652-655.
8. K.Ketzial Jebaseeli, V.G.Rani, "Implementation of File-Hierarchy Attribute Based Encryption (FH-ABE) For Fine Grained Access Control of Medical Managemet in Cloud System", Journal of Emerging Technologies and Innovative Research, ISSN-2349-5162,Vol 6,Issue 3,March 2019.pp 75-80.DOI: http://doi.one/10.1729/Journal.20064.
9. K.Ketzial Jebaseeli, V.G.Rani, "Security Incursion and Cryptography Quick Fix for Data Accumulated in Cloud Storage", Journal of Emerging Technologies and Innovative Research, ISSN-2349-5162, Vol 6, Issue 3, March 2019.pp 345-350.
10. K.Ketzial Jebaseeli, V.G.Rani,"Formulation of Aggregate key in cloud by Cipher Text storage Reduction for data outsourcing in healthcare", **IEEE Digital Xplore** ISBN:978-1-7281-1261-9, Published in the proceedings of International Conference on Communication and Electronics Systems(ICCES) 2019,pp 828-833
DOI: 10.1109/ICCES45898.2019.9002035

Bibliography

Dr.K.Ketzial Jebaseeli MCA, Ph.D, Assistant Professor, Department of Information Technology, School of Computing Science, KPR College of Arts Science and Research, She has completed her doctorate in the department of computer science at Sri Ramakrishna College of Arts & Science for women. She has published many papers in journals and at national and international conferences. Her publications include **IEEE, SCOPUS, and UGC.** She has received the **BEST PAPER AWARD** at the national conference on Emerging Trends and Advancements in Intelligent Computing. She also received the BEST USER AWARD for her e-learning platform. She has one year of industry & 6 years of teaching experience in computer science and she has worked as a Technical Trainer for the ICT Academy. She was provided with the opportunity to perform as a

research assistant for projects funded by ICCSR-Impress. She has a keen interest in information security and cloud computing. She has been selected as one of the Top 50 Internationally Distinguished "**YOUNG SCIENTISTS**" awarded by the International Multidisciplinary Research Foundation. She received an International Star Excellence Award at the Global Web Conference on Multidisciplinary Research and Development. She has received the **BEST WOMAN PERFORMER AWARD IN RESEARCH AND DEVELOPMENT** from the GISR Foundation in February 2022.

*e***ISSN**1303-5150 www.neuroquantology.com