Asia-pacific Journal of Convergent Research Interchange
Vol.10, No.2, February 29 (2024), pp.35-42
http://dx.doi.org/10.47116/apjcri.2024.02.04

Digital Forensics Security for Communications Transmission by Encrypting and Decrypting Characteristics with One-Time Key Authorization

Hye-jin Kim[1], Yong-wan Ju[2], JunHo Hong[3]

[1] *Ph.D. Student, Busan University of Foreign Studies, South Korea, 20225432@office.bufs.ac.kr*
[2] *Professor, Industry-University Cooperation Foundation, Gangneung-Wonju National University, South Korea, ywju@gwnu.ac.kr*
[3] *General Director, Ph.D., Korea Information Security Industry Association, South Korea, hjh@kisia.or.kr*

Corresponding author: JunHo Hong

Abstract: Information can be secretly coded to conceal its actual meaning through the process of encryption. In computers, encrypted data is referred to as ciphertext and unencrypted data is also called plaintext. Data encryption guards against data loss, alteration, and compromise. However, the decryption key needs to be kept private and shielded from unwanted access in order to guarantee that data is kept safe. In this study, the One-Time Key Authorization (OTKA-AED) framework is built to guarantee that message exchange is safe between owners and requesters of cloud data. Additionally, it obtains the OTKA-AED framework that obtains the encryption and decryption method for every session number based on the bilinear mapping transformation and reverse bilinear mapping transformation. In this study, to provide the public key and secret key, the OTKA-AED framework first used the one-time key generation function. This reduced the key generation time and hence, increased cloud security. Finally, permission tag-based encryption and decryption was carried out under the authorization tag, which ensured authorization by effectively reducing communication and storage overhead. The proposed One-Time Key Authorization (OTKA-AED) architecture further ensures message processing within the cloud environment by increasing the security of message communication by encrypting key attributes shared among cloud users.

Keywords: Urban Green Spaces, Sustainability, Equity, Policies, Strategies, Future Generations

1. Introduction

Both the academic and business worlds have given the cloud environment much attention. Firms can easily and securely share various services using Cloud Computing (CC). The personal information of the cloud data owner is transferred to the cloud servers via numerous middlemen, where it is shared at any time with other cloud data requesters. The cloud environment allows users to access the data anytime, from any location[1-3].

CC is an on-demand network access used to assess the information and resources on the internet. The CC services can secure the outsourcing of data security, data privacy, and service availability to third parties. The owners of cloud data can send their messages securely message securely at a high level. However, CC uses attribute encryption to ensure the protected message communication while leaving the authorization factor unresolved[4].

Received: October 30, 2023; 1st Review Result: December 02, 2023; Accepted: January 25, 2024

The OTKA-AED architecture is suggested as a solution to the aforementioned constraint to improve message security and speed up key generation. The public and secret keys are generated between the cloud data owners and servers through the third party during each session using the one-time key generation function. Using the generated public key and secret key, Authorization Tag-based Attribute Encryption is meant to encrypt the key attributes through the authorization tag and produce cypher text with a lower computational cost. Executing the Authorization Tag-based Attribute Decryption[5], which decrypts the cypher text and retrieves the original message, will enable protected message communication in cloud service provisioning.

2. Literature Review

A previous study developed a secure data share method based on dynamic groups to carry out key distribution and data sharing[6]. A secure data-sharing mechanism is first created to share the key securely without using a communication channel. Users can access their private keys using the group manager without needing certificate authorities according to user authentication[7].

The Searchable Symmetric Encryption Scheme with Rankings was developed[8] to facilitate the effective usage of Cloud-based remote storage of encrypted data. Ranking search significantly improves system usability and, as a result, the accuracy of file retrieval by enabling the relevance rating of search results. It is crucial to carefully consider ranked search techniques such as relevance scoring, ranked search solution authentication, and command transfer from one to a number to correctly to correctly maintain the sensitive score data.

A Key Policy Attribute Based Encryption (KP-ABE) approach was presented[9] to offer a higher level of security for CC supply. Additionally, the KP-ABE system enables senders to encrypt messages in the attributes, groups, and private keys that are connected based on access structures that specify which type of cypher texts the key holder is permitted to decrypt. By utilizing the deliverables identity-based broadcast encryption system, the KP-ABE approach creates a constant cypher text size. This makes it possible to express the access strategy with any form of repetitive access structure[10]. The amount of bilinear pairing is regarded as constant while cypher text size is self-governing to the number of cypher text attributes.

3. Proposed Work

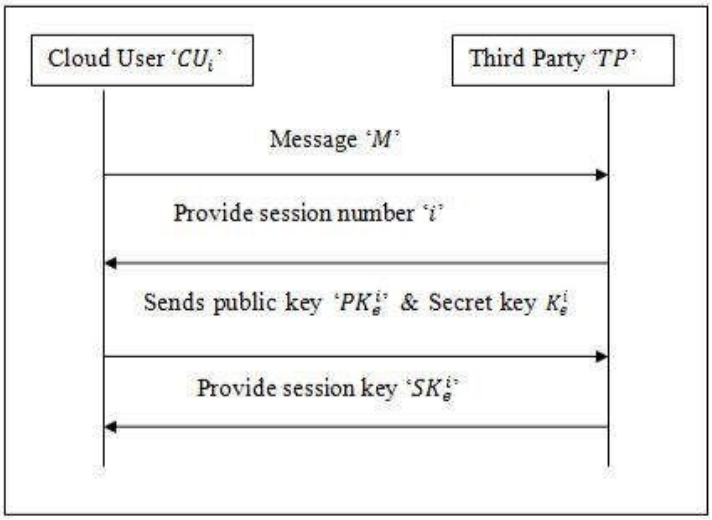
The OTKA-AED framework is developed to safely outsource the secret message across cloud servers while employing a third party and key generation[11][12]. The Cloud Service Provider (CSP) and cloud users (i.e., cloud data owners and data requesters) are described by the OTKA-AED architecture as providing the session key and public keys for achieving message exchange in a secure way. This reduces the storage and communication costs associated with provisioning cloud services.

In this study, the security factor “SK” was considered when designing the suggested OTKA-AED framework. By selecting the two multiplicative cyclic groups “G1” and “G2”, the bilinear map “f: G1* G1→ G2” may be constructed. The cloud users were formed by assuming that the cloud data owners were “DOi=DO1, DO2,..., DOn” and the cloud data requesters were “DRi=DR1, DR2,...DRn”. The cypher text was created after the plain text, represented by the symbol “M”, has been encrypted. The encryption and decryption were carried out by a third party, or “TP” and were recorded in a matrix with attributes set as “α={attr1, attr2, attrn}” respectively.

3.1 One-Time Key Generation

One-time key generation problems must be considered while implementing the attribute encryption

approach in the cloud. The centralized cloud storage is occupied by cloud data, which causes key generation time to be nonlinear and increase file size[13]. In the suggested OTKA-AED framework, secured message communication is achieved by using the One-Time Key Generation function, which generates the through a third party, cloud users can exchange public key and private key. Both the Public Key (PK) and Secret Key (K) are used in every session as the parameters for encryption and decryption. The session key SKI with the ith session for the eth cloud user is represented as the message transmission 'M' together with the cypher text that contains the message to be encrypted.

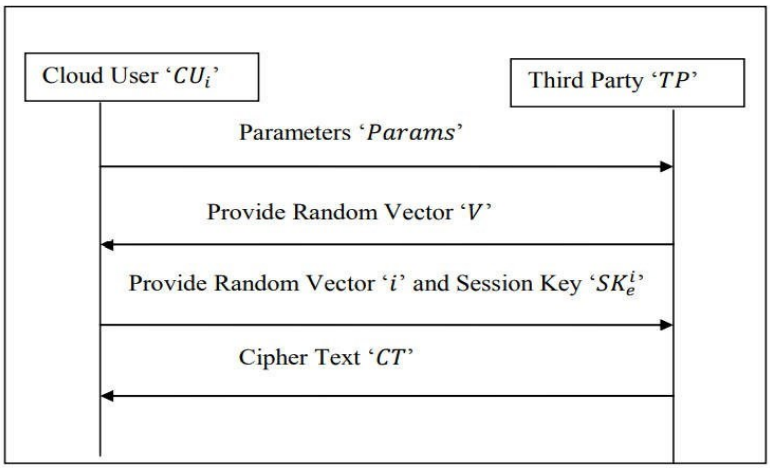


[Fig. 1] One-Time Key Generation

The suggested OTKA-AED framework serves as the foundation for the one-time key generation function diagram depicted in [Fig. 1].

3.2 Encryption of attributes Based on Authorization Tags

The proposed OTKA-AED uses attribute encryption to communicate the message of the cloud data owner with other requesters using the authorization tag provided by the cloud data owner. Messages delivered through cloud data owners generate the authorization tag "AT" during message broadcasting. After evaluating the authorization tag "AT" provided by cloud users using the suggested OTKA-AED architecture, encryption is carried out.



[Fig. 2] OTKA-AED Architecture

The Tag-based Attribute Encryption's activity diagram is shown in [Fig. 3] and is based on the OTKA-AED framework that is suggested below. [Fig. 2] shows how to implement message encryption using the data owner and authorization tag-based attribute encryption. It is assumed that the message “M”, the secret key “K”, the matrix “MAT”, the order “m*n”, and ‘α’ all denote the rows of the matrix "MAT.” The Measure of Key Generation Time is shown in [Fig. 2].

The time needed to generate the public key and the secret key to enable secure message transmission among cloud users by a third party is referred to as key generation time in the proposed OTKA-AED framework. The following is a mathematical formulation of key generation time.

KG_{time}=Size of the attributes*Time(public key)*Time(secrete key)

In the given equation, KG_{time} is the key generation time, which is taken into account while determining the size, public key, and secret key that must be created for a cloud user.

It is quantified in milliseconds (ms). The process is said to be more effective when key generation takes less time as shown in the [Table 1].

[Table 1] Tabulation for Key Generation Time

Filesize (KB)	Key Generation Time (ms)			
	OTKA-AED	Existing SecureData Sharing	Existing KP-ABE	Existing Ranked Searchable SymmetricEncryption
10	0.031	0.043	0.058	0.075
20	0.037	0.05	0.064	0.081
30	0.041	0.053	0.068	0.085
40	0.039	0.052	0.067	0.084
50	0.044	0.057	0.072	0.089
60	0.047	0.06	0.075	0.092
70	0.046	0.059	0.074	0.091
80	0.054	0.067	0.081	0.098
90	0.058	0.072	0.086	0.103
100	0.061	0.075	0.089	0.106

[Table 1] compares the key generation times for current methods such as the KP-ABE by Changji Wang and Jianfa Luo and the ranked searchable symmetric encryption scheme by Wang et al. (2012) and the secure data sharing scheme by Zhu and Jiang (2016) with the proposed OTKA-AED framework (2013). The range of file sizes used for conducting experiments is 10 to 100. According to all approaches have longer key generation times as file sizes grow. When compared to current approaches, the proposed OTKA-AED system, however, dramatically reduces the time required for key generation. [Fig. 3] shows the graph, which is produced based on the data in [Table 2].

The proposed OTKA-AED framework's key generation time is depicted in [Fig. 3.6] and compared to the state-of-the-art approaches, such as the secure data sharing scheme developed by [14], the ranked searchable symmetric encryption scheme developed by [15], and the KP-ABE developed by [16-19]. The chart shows that, in comparison to current methods, the key generation time is significantly shorter. This is because only the key characteristics are addressed by the One-Time Key Generation method, and for each key attribute, the generation of the public key and the secret key is calculated concerning the time, increasing the files’ ability to be read remotely. As a result, the suggested OTKA-AED framework for secure message exchange can be used in the cloud with confidence. Also, the proposed OTKA-AED framework's key generation time was decreased by 23%, 38%, and 44%, respectively.

[Fig. 3] Measure of Key Generation Time

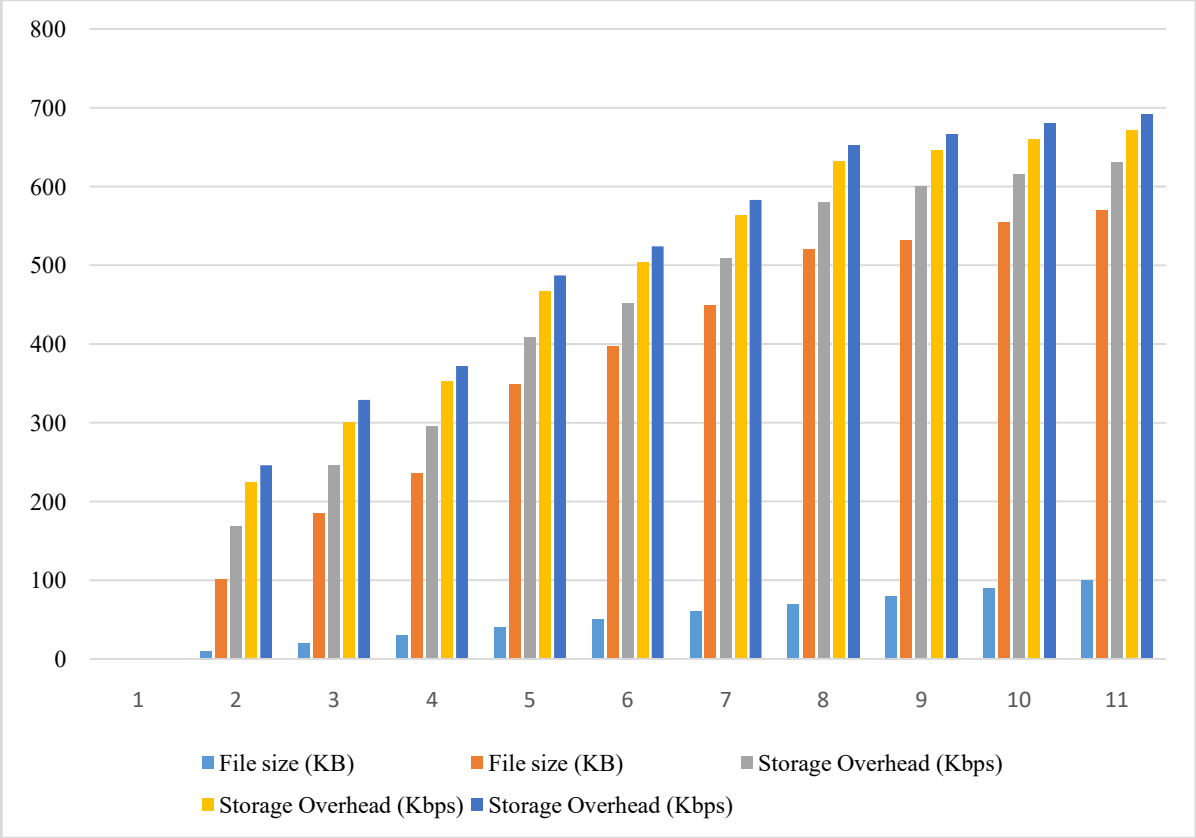
3.5.1 Measure of Storage Overhead

The size of the files is between 10 and 100. According to the table, storage overhead increased for all techniques as file size increases. However, it was much diminished in the OTKA-AED system.

[Table 2] Tabulation for Storage Overhead

File size(KB)		Storage Overhead (Kbps)		
	ProposedOTKA-AED	Existing SecureData Sharing	ExistingKP-ABE	Existing Ranked Searchable Symmetric Encryption
10	101	168	225	246
20	185	245	300	329
30	235	295	352	372
40	349	409	467	487
50	397	452	504	524
60	449	509	563	583
70	520	580	632	652
80	532	600	646	666
90	554	615	660	680
100	570	630	671	691

[Fig. 4] shows the measure of storage overhead for the proposed OTKA-AED framework compared with the current approaches, including the secure data sharing scheme by Zhu & Jiang (2016), and the ranked searchable symmetric encryption.



[Fig. 4] Measure of Storage Overhead

Additionally, utilizing the OTKA-AED architecture, the message is only encrypted when the permission tag is accepted by both parties.

4. Conclusion

The proposed OTKA-AED framework was built to guarantee safe message exchange between owners and requesters of cloud data. Additionally, the OTKA-AED framework obtained the encryption and decryption method for every session number based on the bilinear mapping transformation and reverse bilinear mapping transformation. To provide the public key and secret key, the OTKA-AED framework first used the one-time key generation function. This reduced the key generation time and hence increased cloud security. Finally, permission tag-based encryption and decryption were carried out by the authorization tag, which ensured authorization by effectively reducing communication and storage overhead. The proposed OTKA-AED architecture further ensures message processing within the cloud environment by increasing the security of message communication by encrypting key attributes shared among cloud users.

Additionally, the effectiveness of the suggested OTKA-AED framework was evaluated using the following metrics for cloud service provisioning, including key generation time, storage overhead, and communication overhead. The simulation findings showed that the proposed OTKA-AED framework, when compared to state-of-the-art works, decreased key generation time by 35%, storage overhead by 24%, and communication overhead by 14%. However, simply verifying cloud data is insufficient. To provide an optimum cloud service provider, the proposed Fuzzy K-Means and K-Medoids algorithms were created. Additionally, the algorithms for fuzzy K-Means and K-Medoids, greatly reduce the encryption time in CC by authenticating the cloud data.

5. Acknowledgments

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP-2024-2020-0-01825) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation) and This research was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea Government (MSIT) and Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist) and This work was supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT)(IITP-2024-RS-2023-00260267).

References

[1] B. P. Doppala, S. NagaMallik Raj, E. Stephen Neal Joshua, N. Thirupathi Rao, Automatic determination of harassment in social network using machine learning, Lecture notes in networks and systems, (2021), pp.245-253.
DOI: 10.1007/978-981-16-1773-7_20

[2] E. Morioka, M. S. Sharbaf, Digital forensics research on cloud computing: An investigation of cloud forensics solutions, 2016 IEEE Symposium on Technologies for Homeland Security (HST), (2016), pp.1-6.
DOI: 10.1109/THS.2016.7568909.

[3] S. N. J. Eali, N. T. Rao, K. Swathi, K. V. Satyanarayana, D. Bhattacharyya, T. Kim, Simulated studies on the performance of intelligent transportation system using vehicular networks, International Journal of Grid and Distributed Computing, (2018), Vol.11, No.4, pp.27-36.
DOI: 10.14257/ijgdc.2018.11.4.03

[4] E. S. N. Joshua, D. Battacharyya, B. P. Doppala, M. Chakkravarthy, Extensive statistical analysis on novel coronavirus: Towards worldwide health using apache spark, Healthcare Informatics for Fighting COVID-19 and Future Epidemics, (2022), pp.155-178.
DOI: 10.1007/978-3-030-72752-9_8

[5] S. Verma, A. Kumar, S. Pandey, P. Negi, Blockchain and cloud computing used in preservation of crime scene evidences, 2023 2nd International Conference on Edge Computing and Applications (ICECAA), pp.7-11, (2023)

[6] E. S. N. Joshua, D. Bhattacharyya, M. Chakkravarthy, H. Kim, Lung cancer classification using squeeze and excitation convolutional neural networks with grad cam++ class activation function, Traitement Du Signal, (2021), Vol.38, No.4, pp.1103-1112.
DOI: 10.18280/ts.380421

[7] Joshua, E. S. N., Chakkravarthy, M., & Bhattacharyya, D. (2021). Lung cancer detection using improvised grad-cam++ with 3D CNN class activation, Lecture notes in networks and systems, (2021), pp.55-69.
DOI: 10.1007/978-981-16-1773-7_5

[8] E. S. Neal Joshua, N. T. Rao, D. Bhattacharyya, Managing information security risk and internet of things (IoT) impact on challenges of medicinal problems with complex settings, Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems, (2022), pp.291-310.
DOI: 10.1016/B978-0-323-90032-4.00007-9

[9] E. S. Neal Joshua, N. Thirupathi Rao, D. Bhattacharyya, The use of digital technologies in the response to SARS-2 CoV2-19 in the public health sector, Digital innovation for healthcare in COVID-19 pandemic: Strategies and solutions, (2022), pp.391-418.
DOI: 10.1016/B978-0-12-821318-6.00003-7

[10] Domingues, Patrício, Luís Andrade, and Miguel Frade, A digital forensic view of windows 10 notifications, Forensic Sciences 2, (2022), No.1, pp.88-106.
DOI: 10.3390/forensicsci2010007

[11] X. Li, B. Li, H. Wang, J. Zhang, H. Yang, J. Liu, A novel violation tracing model for cloud service accountability, 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.744-750, (2020)

[12] N. T. Rao, E. S. Neal Joshua, D. Bhattacharyya, An extensive discussion on utilization of data security and big data models for resolving healthcare problems, Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems, (2022), pp.311-324.
DOI: 10.1016/B978-0-323-90032-4.00001-8

[13] A. Barros, R. Almeida, T. Melo, M. Frade, Forensic analysis of the bumble dating app for android, Forensic Sci, (2022), Vol.2, No.1, pp.201-221.
DOI: 10.3390/forensicsci2010016

[14] S. N. J. Eali, D. Bhattacharyya, T. R. Nakka, S. Hong, A novel approach in bio-medical image segmentation for analyzing brain cancer images with U-NET semantic segmentation and TPLD models using SVM, Traitement Du Signal, (2022), Vol.39, No.2, pp.419-430.
DOI: 10.18280/ts.390203

[15] S. Bhushan, A novel digital forensic inspection model for XSS attack, Soft Computing: Theories and Applications, (2022), Vol.425, pp.747.

[16] B. Coronel, P. Cedillo, K. Campos, J. Camacho, A. Bermeo, A systematic literature review in cyber forensics: Current trends from the client perspective, IEEE Third Ecuador Technical Chapters Meeting (ETCM), (2018), pp.1-6.

[17] Y. Khan, S. Varma, Development and design strategies of evidence collection framework in cloud environment, Social Networking and Computational Intelligence, (2020), Vol.100, pp.27.

[18] M. Michel, D. Pawlaszczyk, R. Zimmermann, AutoPoD-mobile—semi-automated data population using case-like scenarios for training and validation in mobile forensics, Forensic Sci, (2022), Vol.2, pp.302-320.
DOI: 10.3390/forensicsci2020023

[19] E. S. N. Joshua, D. Bhattacharyya, M. Chakkravarthy, M. Lung nodule semantic segmentation with bi-direction features using U-INET, Journal of Medical Pharmaceutical and Allied Sciences, (2021), Vol.10, No.5, pp.3494-3499.
DOI: 10.22270/jmpas.V10I5.1454