ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(11), DOI: 10.17485/ijst/2016/v9i11/88453, March 2016* ISSN (Online) : 0974-5645

Optimal Integrity Policy for Encrypted Data in Secure Storage using Cloud Computing

P. Senthil Kumari[1*] and A. R. Nadira Banu Kamal[2]

[1]Department of Master of Computer Applications, The Thassim Beevi Abdul Kader College for Women, Kilakarai, Ramanathapuram -623517, Tamil Nadu, India; senthilmathimca@gmail.com }
[2]Department of Computer Science, The Thassim Beevi Abdul Kader College for Women, Kilakarai, Ramanathapuram – 623517, Tamil Nadu, India; nadirakamal@gmail.com

Abstract

Objectives: We want to provide effective integrity verification for encrypted data which is transferred and provide high security. We want to retrieve the results with lesser memory consumption and lesser latency. **Methods:** The proposed approach combines Attribute Based Cryptography with bilinear mapping to enhance the data security. Simulation model validates the security issues related to the efficient key derivation and Message Authentication Code verification process. We compare our policy with existing techniques on the performance parameters such as encryption time, computational overhead and average lifetime to generate/derive keys. The performance analysis confirms the effectiveness of our policy. **Findings:** The chief drawbacks of the existing ABE schemes were expensive pairing operations and increase in the complexity and overhead of the admission policy. The time needed to decipher the cipher text was high, due to the great size of the cipher text. Hence, in order to overcome these limitations, this paper proposes an Optimal Integrity Policy for enhanced data security and integrity in the cloud. In secret key generation, we use AND, EXOR and hashing operarations to improve the security. MAC verification process is used to monitor the integrity of the data. An Optimal Integrity Policy confirmed the effectiveness of encryption time over existing CP-ABE methodologies based on the performance measures. The comparative analysis on the parameters such as computational overhead, average life time for generation/derivation of keys shows the better performance in OIP than the EPPDR, subset cover and pseudo random key generators. By enhancing the secret key generation, the data security is also enhanced. The experimental results achieves minimum overhead for both communication and computation. **Applications/Improvements:** The decryption time is slow for low end devices since it requires modular exponentiation. Hence, the future work shall be extended to speed up the decryption time.

Keywords: Attribute Based Encryption, Encrypted Data, Optimal Integrity Policy, Secret Key, Secure Storage

1. Introduction

Our modern society is increasingly relying on the collection, processing and sharing of digital information. Enabled by the rapid developments in the sensor, wireless and networking technologies, communication and networking are becoming more and more pervasive and ad hoc. Driven by the explosive growth of hardware and software capabilities, computation power is becoming a public utility and information is often stored in the centralized servers which facilitate ubiquitous access and sharing. The information handled by the system is usually sensitive and of high value, while various security breaches could compromise the confidentiality of the system. Thus there is an urgent need to develop security and privacy mechanisms to protect the authenticity, integrity and confidentiality of the collected data and to control the disclosure of private information.

In achieving that, there lacks the centralized trusted parties in pervasive networking; the remote data servers

* *Author for correspondence*

tend not to be trusted by the system users in handling their data. They make existing security solutions developed for traditional networked information systems unsuitable. Cloud computing is built on the virtualization, parallel and distributed computing and service-oriented architecture. The significant features of the cloud computing are high operational efficiency, scalability, flexibility and minimum capital cost. Users provide data to the cloud service provider for storage and business operations. Moreover, the entrepreneurs will face the critical consequences, if their confidential data is disclosed to their business competitors or public. Many data security techniques are developed to mitigate the security issues in the cloud. Current data security approaches focus only on data security in which cryptographic solutions are followed by the random key generation processes. But, the prevailing security technique suffers minimum data integrity. Loss of key in the conventional cryptographic techniques crash the original data provided by the data owner. Figure 1 shows the system model of the key encryption process.

The Attribute-Based Encryption (ABE) is a public key encryption technique that allows users to encrypt and decrypt messages, based on the user attributes. In the ABE scheme, the cipher texts are not encrypted for a particular user.

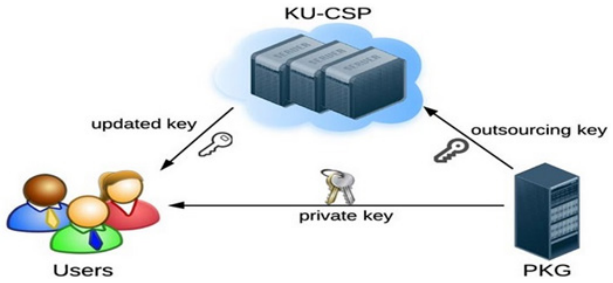

Figure 1. System model of the key encryption process.

Rather, both the cipher texts and decryption keys are associated with a set of attributes or a policy over attributes. The user can decrypt a cipher text only during the proper matching between the decryption key and the cipher text. ABE schemes are classified into Key Policy based ABE (KP-ABE) and Cipher Text-Policy based ABE (CP-ABE). The KP-ABE scheme is based on the association of the attributes and decryption keys of the user. The CP-ABE scheme is based on the association of Cipher Text Policy and decryption keys of the user. In the KP-ABE scheme, a cipher text relates to the set of attributes. The decryption key of the user is associated with a monotonic tree access structure. The user can decrypt the cipher text only when the user attribute related with the cipher text satisfies the tree access structure. The CP-ABE technique is extended to Hierarchical Attribute Set Based Encryption (HASBE) in order to design the scalable, flexible, fine grained access control. The HASBE operation includes several processes such as system setup, domain authority grant validation and file creation. The setup algorithm is used to setup the system public key parameters and master key parameters. The trusted authority domain verifies the new top level domain authority, when it requests to join the system. The administrative domain authority verifies the new joined domain authority whether it is valid or not. The new encrypted file creation is based on the needs of the owner. The complexity of the new file creation depends upon the size of the domain authority data file. The HASBE technique increases the efficiency of user revocation in multiple value assignment environments. The key escrow problem induced in HASBE technique is considered by Multi Authority Attribute Based Encryption (MA-ABE). The main drawback of the ABE technique is the increase in the computational cost for key generation and encryption. To overcome this problem, this paper proposes an Optimal Integrity Policy (OIP) to ensure data security and integrity in the cloud services. The proposed technique focuses on a robust secret key generation process and Message Authentication Code (MAC) verification process.

2. Related Works

This section describes the conventional encyrption techniques for the cloud computing applications. [1]Proposed a Hierarchical Attribute-Set-Based Encryption (HASBE) technique for the scalable, flexible and fine-grained access control of the outsourced data in the cloud computing. The proposed scheme achieves the scalability and flexibility due to the hierarchical structure. The proposed scheme was efficient and flexible in dealing with the access control of the outsourced data in the cloud computing. [2]Proposed an efficient and privacy-protective auditing protocol for supporting the data dynamic operations in the cloud storage systems. The proposed protocol supports batch auditing for the multiple owners and clouds, without requiring any trusted organization. The efficiency and security of the proposed auditing protocols were improved, while reducing the computation cost of the auditing process.

[3]Suggested a set of data access control mechanisms for the Personal Health Record (PHR) stored in the semi trusted servers. The PHR file of the patient was encrypted, by using the Attribute-Based Encryption (ABE) techniques. Each user in the PHR system was divided into multiple security domains to reduce the complexity in the key management for the data owners and users. The analytical and experimental results had shown the efficiency, security and scalability of the proposed scheme. [4]Proposed a secure cloud storage system for the simultaneous privacy-protective public auditing of the multiple users. The security and performance analysis had described that the proposed schemes were secure and highly efficient. [5] Suggested a flexible auditing mechanism for the cloud storage, by using the homomorphic token and distributed erasure-coded data. The proposed mechanism was resistant against various failure and malicious attacks. Fast data error localization was achieved, without any increase in the communication and computation cost.

[6]Proposed a Sec Cloud protocol for associating the secure storage and computation auditing in the cloud by using the Designated Verifier Signature (DVS), batch verification and probabilistic sampling techniques. The effectiveness and efficiency of the proposed Sec Cloud were improved. [7]Suggested the combination of the digital signature and Diffie-Hellman key exchange with the Advanced Encryption Standard (AES) algorithm to enable the protection of the data confidentiality in the cloud. The three-way mechanisms of the proposed architecture had made it more difficult to crash the security system. [8]Presented an attribute-based keyword search scheme for independently encrypting and outsourcing data of the multiple owners to the cloud server. The owner-enforced access policy on the index of each file had achieved fine-grained search authorization. The proposed scheme was efficient and secure against the keyword attack.

[9]Presented a clock-based proxy re-encryption scheme that enables the sharing of a secret key by the data owner and the cloud. The cloud has automatically performed re-encryption of data based on the internal clock, without receiving any command from the data owner. The proposed scheme had achieved scalable user revocation and fine-grained access control in the unreliable clouds. [10]Suggested the utilization of the Cipher Text Policy based ABE technique to encrypt and decrypt the Electronic Health Record (EHR). The flexibility and scalability of the proposed approach were realized using the preliminary experimental results. [11]Proposed a distributed access control in the cloud algorithm to support the user revocation without the need for redistribution of the keys to all the cloud users. The computation, communication and storage overheads were reduced by the proposed approach.

[12]Designed an access control framework with efficient attribute revocation method to match with the dynamic change in the access privileges of the users in large-scale systems. The proposed scheme was efficient and secure in the random oracle model. [13]Proposed a hierarchical encryption scheme combining the identity-based encryption and Cipher Text Policy based encryption systems, to achieve fine-grained access control. The access rights were efficiently revoked from the users, by applying proxy and lazy re-encryption techniques to the proposed scheme. [14]Proposed a revocable Identity-Based Encryption (IBE) scheme for deploying a hybrid private key for each user. The efficiency and security of the proposed scheme were improved, while achieving reduction in the key generation complexity.

[15]Proposed a novel verifiable attribute-based keyword search scheme for the outsourced encrypted data. The performance evaluation had depicted that the proposed scheme was practical and deployable.[16]Proposed a proxy re-encryption technique based on attribute and Cipher Text Policy, constructed in the composite order bilinear group. The proposed technique integrated the dual system encryption technology with a selective proof technique. [17]Presented a Multi-message Cipher Text Policy ABE technique for sharing scalable media based on the attributes of the data users. The scheme was efficient and flexible, while achieving reduction in the computational complexity of the cloud servers. [18]Proposed a novel attribute-based encryption scheme to generate different class security keys for the users. The proposed scheme was simple, efficient and secure by using the hierarchical keys resulting from the one-way function chain. [19]Proposed Authorized Private Keyword Search (APKS) solution that enables the delegation and revocation of search capabilities. Efficient multi-dimensional keyword search was achieved by the proposed solution. [20]Presented an efficient time-based access control encryption scheme for the cloud services. The effectiveness and security of the encryption scheme were improved by using the cryptographic integer comparison. The traditional key based encryption scheme

such as Efficient Privacy-Preserving Demand Response Scheme (EPPDR) achieves the privacy preservation of demand, adaptive key evolution and the forward secrecy. The problem in EPPDR is more computational overhead compared to other encryption methods. Hence, an alternative technique is required to minimize the computational overhead in security applications.

Proposes HASBE by extending Cipher Text Policy Attribute-set-Based Encryption with a hierarchical structure of users.[21]The security of HASBE based on security of the CP-ABE scheme is proved by and its performance and computational complexity are analyzed. Yongdong Wu et al. presents a novel Multi-message Cipher Text Policy Attribute-Based Encryption (MCP-ABE) technique and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes rather than an explicit list of the consumers' names. The scheme is efficient and flexible[22] because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one cipher-text.

[23]Defines and enforces access policies based on data attributes and allows the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. The proposed scheme has salient properties of user access privilege confidentiality and user secret key accountability. [24]Proposes a scheme with the following achievements: (1) The key escrow problem could be solved by escrow-free key issuing protocol. (2) Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

[25]Propose efficient Blind Key Extraction protocol for an anonymous Identity Based Encryption which is conceptually simpler. It supports predicates defined by vectors from a large domain instead of bit vectors and allows retrieval of multiple items in one invocation. A Two-Round Searchable Encryption (TRSE) scheme[26] is used to eliminate the leakage of data. The approach supports top-*k* multi-keyword retrieval. Homomorphic encryption and vector space model are employed in the TRSE method. Sufficient search accuracy is provided by the vector space model. Majority of the computing work is performed on the server side by operations on cipher text. The approach eliminates data leakage and ensures data security.

[27]Introduce Attribute Set Based Encryption (ASBE) scheme for realizing scalable, flexible and fine-grained access control. ASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. [28]Develops a new cryptographic framework to secure data and related processing in the cloud so as to enable users to enjoy the tremendous benefits of cloud computing while ensuring their data remains protected.

In authors' previous work, a searchable index is generated for the data that has to be outsourced to the cloud. Encryption of data is performed using Pairing Based Cryptography (PBC)[29]. The encrypted data is wrapped with the index and then outsourced. The searched result is ranked by the cloud server according to Robust Searchable Symmetric Encryption (RSSE) ranking criteria in order to enhance the document retrieval accuracy. This approach provides high security by using PBC. In authors' previous work, a secure scheme with multi keyword search is proposed for encrypted cloud data. This paper introduces a novel Association Based Cryptography (ABC)[30] and multiple keyword semantics approach for secure search of the cloud data. The major advantages of the proposed ABC are high security in cloud data, effective integrity verification for data transferred, lesser memory consumption and lesser latency.

Akshaya et al. proposes ABBE (Attribute Based Broadcast Encryption) which is an enhancement of ABE (Attribute Based Encryption) which uses ABE to encrypt the data (AES key) and then broadcasts the cipher in order to provide fine grained access. This also avoids collusion and excess key generation[31]. In addition to this multiple data owner scenario scheme, the whole system is divided into multiple domains. ABBE has minimized implementation complexity and less effort with respect to computation when compared to that of ABE. Shanthi et al. proposes HABE along with Group Key mechanism for better security and scalability of sharing data over cloud from mobile devices[32]. With this the data are stored securely in cloud and the system is scalable for group communication. To reduce the computational overhead during revocation, Proxy re-encryption technique is used. It also improves the performance of the mobile users by leveraging the process of regenerating the keys onto the server side.

The chief drawbacks of the existing ABE schemes were expensive pairing operations and increase in the

complexity and overhead of the admission policy. The time needed to decipher the cipher text was high, due to the great size of the cipher text. Hence, in order to overcome these limitations, this paper proposes an optimal Integrity Policy for enhanced data security and integrity in the cloud.

3. Optimal Integrity Policy

This section describes the proposed OIP for improving the data security and data integrity in the cloud. The proposed technique mainly focuses on the key security for the outsourced data in the cloud servers. The key generation algorithm provides secure access control mechanism and data access policies.

3.1 Secret Key Generation Process

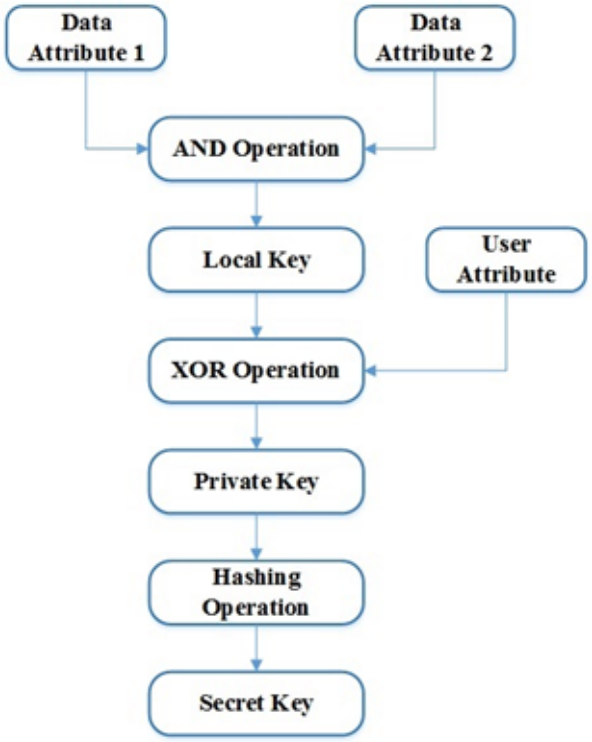

Figure 2. Flow diagram for the secret key generation process.

Initially, the extraction of the data and user attributes are performed. Then, any two attributes are randomly selected. The AND operation is performed on the selected attributes. The resultant value of the AND operation is the local key. The exclusive OR (XOR) operation is performed with the local key and user attribute and a private key is generated. Then, the Hashing operation is performed to convert the private key into a secret key. When the users need to retrieve data, their request is transferred to the data owner by the third party provider. The data owner sends the secret key directly to the user. Using this secret key, the user can decrypt the cipher text obtained from the cloud, to get the original plain text. Figure 2 shows the flow diagram for the secret key generation process.

3.2 ABE Process

The ABE process defines an access control policy so that the user can access the data, if the data attributes and user attributes satisfy the defined policy. The attribute-set-based encryption prevents the combination of the attributes across the multiple sets. The user access control policy is defined on the basis of corresponding attributes of the users. Initially, the users have to send the request to the key authority to access a service. The key authority performs computation using the user attributes and private key issues. Then, the key authority issues the public parameter to the service provider to encrypt the service response.

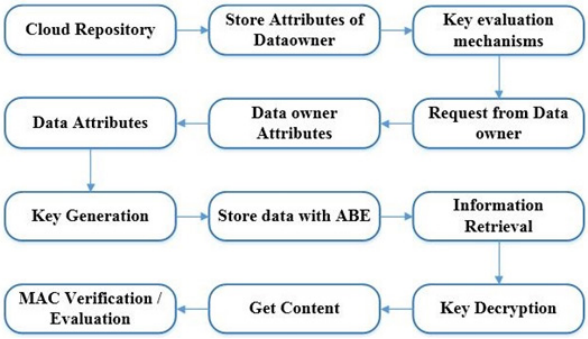

Figure 3. Flow diagram of the ABE and MAC verification process.

A key defines the unique labels for each attribute in the structure. The depth of the key structure is the level of recursions in the set. The members at depth 1 are either attribute elements or sets and members at depth 2 will be attribute elements. For key structures of depth 2, an index of the sets at depth 2 is sufficient to uniquely identify the sets. Thus, if there are 'n' sets at depth 2, then a unique index u_i, where $1 \leq u_i \leq n$ is assigned to each set. The combination of attribute name and label defines the unique label to the individual attribute. In the proposed

method, local key is generated using the user attributes. For example, let us consider the file name, file size and file extension as the attributes of the user. Then, the private key is generated by using the user and data attributes. Figure 3 shows the flow diagram of the encryption process and MAC verification process.

3.3 Secret Key Generation Algorithm

The key generation algorithm depends upon the two issues such as a secret key and the attributes of the user. The attribute authority receives the master key 'y'. Let w0* and w1* be the two data attributes. Local key W* is generated by the intersection of w0* and w1*. The private key is generated using the Ex-or operation of the W* and w3*. The secret key SK* is generated by hashing the private key. Cost function is performed using the secret key and selected file. Finally, the encryption key is generated. The encryption key can be viewed as the form of kF; p = H0 (H1 (F), KP) $\oplus$ H2 (F), where H0, H1 and H2 are all cryptographic hash functions. The file F is encrypted with another key k, while k will be encrypted with kF; p. Following algorithm shows the secret key generation process.

Secret Key Generation Algorithm
Input Parameters: Fs, Fn, w*, sk
Output: kF = KeyGen CE (Hash (Pk*))
Step 1: Start
Step 2: SEND DataAttr (fs, fn, fext)
Step 3: RECEIVE DataAttr (fs, fn, fext)
Step 4: Generate LocalKeyGen (w0* intersect w1*)
Step 5: Generate PrivateKeyGen (w* Exor w3*)
Step 6: KF = KeyGen CE (Hash (Pk*))
Step 7: CF = Enc CE (KF, F)
Step 8: STORE CF into cloud
Step 9: REQUEST for File Download
Step 10: DF = DEC (KF, F)
Step 11: GET Cost (DF), Mutil
Step 12: Stop

3.4 MAC Verification Process

The MAC verifies the data integrity by using a secret key shared between the data owner and user. Different hash values are generated to indicate the unawareness of the secret key of the data owner. The MAC standard defines the cryptographic check sum, which is obtained from passing the data through a message authentication algorithm along with the user attributes. The MAC utilizes a session key to detect both accidental and intentional data modifications. The outsourced data file F consists of a finite ordered set of blocks S_1, S_2….S_m. A direct way to ensure data integrity is pre-computation of the MACs for the entire data file. The data owner pre-computes MACs of the file using a set of secret keys and stores them locally, before data outsourcing. For each time during the auditing process, the data owner reveals a secret key to the cloud server and requests for a fresh keyed MAC for verification. MAC verification process enables high data integrity, since it covers all data blocks.

The algorithm to implement MAC verification is as follows:

MAC verification
Input Parameters: key, message
Output: Hash concatenation
Step 1: Start
Step 2: Check the size of keys greater than block size
Step 3: Calculate the hash function; otherwise add the zero pads to the hash function.
Step 4: Calculate the underlying hash function for within the block and XOR function
Step 5: Calculate the concatenated hash output
Step 6: Stop

The MAC utilizes a session key and message to detect both concatenated data modifications in hash function. The data owner pre-computes MACs of the file using a set of secret keys and stores them locally before data outsourcing. For each time during the auditing process, the data owner reveals a secret key to the cloud server and requests for a fresh keyed MAC for verification. MAC verification process enables high data integrity, since it covers all data blocks.

4. Results and Discussion

This section presents the comparative analysis of the performance parameters such as computational time, computational overhead and average time to derive the keys with the optimization techniques and average time to generate the keys with optimization on the proposed OIP with the CP-ABE, EPPDR and pseudo random key generation subset cover.

4.1 Encryption Time

The time required to complete the encryption process

is termed as computational time. When the number of attributes involved in the process increases, it increases the encryption time. The encryption time computed with ten key attributes is listed in the Table 1.

It shows the variations of the encryption time with the number of attributes involved. The time for encryption increases to the maximum value in the traditional CP-ABE methods. The proposed OIP provides the minimum time required for the encryption process for different number of attributes.

Table 1. Encryption time vs. attributes

Attributes	Computational Time (sec)	
	CP-ABE	OIP
1	0.5	0.2
2	0.8	0.5
3	1.1	0.8
4	2.7	1
5	3.1	1.3
6	3.4	1.5
7	3.9	1.6
8	4.3	1.8
9	4.5	2.3
10	5.5	2.9

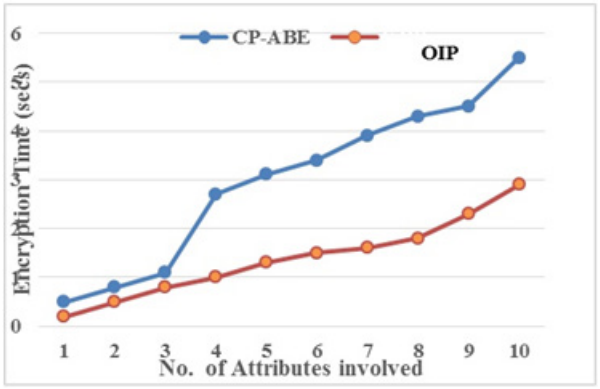

Figure 4. Encryption time vs. no. of attributes.

Figure 4 describes the relationship between the computational time with the number of attributes respectively. The proposed OIP algorithm provides the minimum computational time than the traditional CP-ABE approach.

4.2 Computational Overhead

The measure of the capability of the network to withstand the emulation attackers is called the computational overhead. When the number of attackers increases, the overhead is limited to achieve the authentication. The computational overhead is mathematically represented as follows:

Computational Overhead = Generated Keys + Encrypted Keys

The computational overhead computed with ten session keys is listed in the Table 2. It shows the variations of the computational overhead with the number of session keys involved. The overhead increases to the maximum value in the traditional EPPDR methods. The proposed OIP provides the minimum overhead.

Table 2. Computational overhead vs. session keys

Session Keys	Computational Overhead (ms)	
	EPPDR	OIP
1	10	9
2	19	15
3	25	21
4	34	27
5	43	39
6	46	40
7	47	41
8	59	42
9	74	45
10	90	49

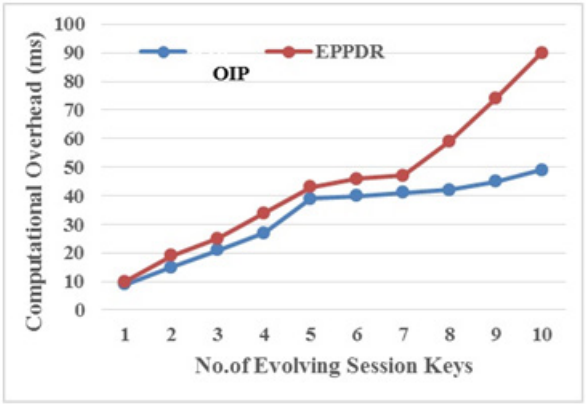

Figure 5. Computational overhead vs. no. of evolving session keys.

The relationship between the computational overhead and the number of session keys is described in Figure 5. The number of session keys is increased and the network capability in terms of the computational overhead is

computed. The proposed OIP algorithm provides the minimum overhead compared to existing EPPDR approach.

4.3 Average Lifetime to Derive Keys

The life time is the important parameter in the design of the network. The speed of the packet transmission depends upon the life time to derive the keys of the data transmission when the network is in high traffic. The interval for key update increases, then the average lifetime to derive the keys is computed using the existing pseudo random key generation algorithm and the proposed OIP algorithm. The simulation results confirm the effective increase in the lifetime. The average lifetime to derive the keys computed with ten different key update intervals is listed in the Table 3.

Table 3. Average lifetime for key derivation vs. key update interval

Key Update Interval	Average Lifetime (ms)	
	Pseudo Random	OIP
1	234	200
2	274	208
3	434	256
4	466	341
5	500	490
6	530	504
7	561	541
8	714	547
9	939	638
10	993	684

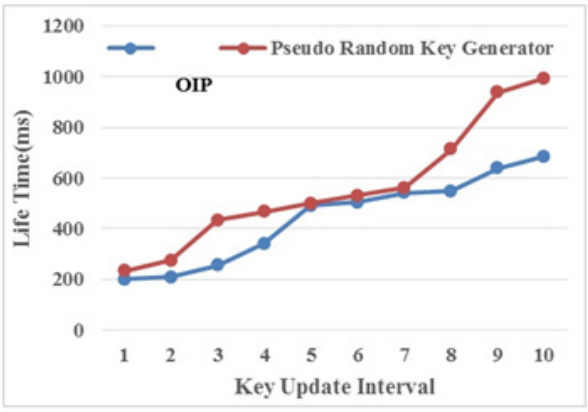

Figure 6. Average lifetime vs. key update interval.

It shows the measures of the average lifetime for key derivation with the key update interval. The interval for updating process is more than the average lifetime for derivation of keys. But, using the proposed OIP algorithm provides the minimum average lifetime compared to the pseudo random key generation algorithm.

The interval for key update is increased in the network that leads to the high network traffic. The measure of the traffic is expressed as the lifetime of the users. The relationship between the key update interval and lifetime are depicted in Figure 6. The proposed method provides the minimum lifetime compared to the pseudo random key generators.

4.4 Average Lifetime to Generate Keys

The key is the important parameter in the design of the network. The time to generate the keys depends upon the key update interval. The interval for key update increases, then the average lifetime to generate keys is computed using the subset cover and the proposed OIP algorithm. The simulation results confirm the effective increase in the average lifetime. The average lifetime to generate the keys computed with ten different intervals is listed in the Table 4.

Table 4. Average lifetime for key generation vs. key update interval

Key Update Interval	Average Lifetime (ms)	
	Subset Cover	OIP
1	200	112
2	260	217
3	314	290
4	400	315
5	402	390
6	415	398
7	469	397
8	503	302
9	508	380
10	510	300

It shows the measures of the average lifetime for key generation with the key update interval. The interval for updating process is more than the average lifetime for derivation of keys. But, using proposed OIP algorithm provides the minimum average lifetime compared to subset cover.

The increase in the generated keys leads to high network traffic. The measure of traffic is expressed as lifetime of the users. The relationship between the key update interval and lifetime are depicted in Figure 7.

The proposed method provides the minimum lifetime compared to the subset cover.

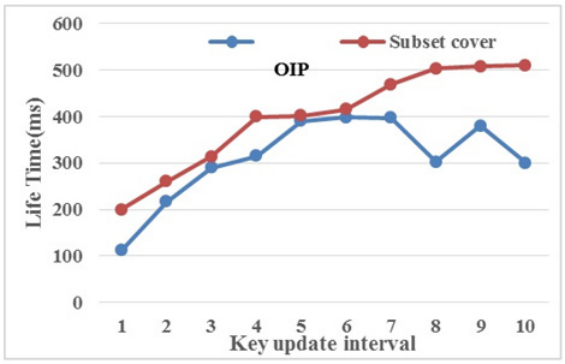

Figure 7. Average lifetime vs. key update interval.

5. Conclusion

In this paper, an Optimal Integrity Policy is proposed to ensure high data security and integrity in the cloud for secure data transmission. In secret key generation, MAC verification process is used to monitor the proper security key. An Optimal Integrity Policy (OIP) confirmed the effectiveness in the areas of security over the existing CP-ABE methodologies based on the performance measures. The comparative analysis on the parameters such as computational overhead, average life time for generation/derivation of keys and encryption time shows the better performance in OIP than the CP-ABE, EPPDR, pseudo random key generator and subset cover. At the user side, the decryption accelerates significantly. The decryption time may be still slow for low end devices since it requires modular exponentiation. Hence, the future work shall be extended to provide an alternative approach to speed up the decryption time for low end devices.

6. Referenes

1. Wan Z, Liu JE, Deng RH. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security. 2012 Apr; 7(2):743–54.
2. Yang K, Jia X. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Transactions on Parallel and Distributed Systems. 201 Sep3; 24(9):1717–26.
3. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems. 2013 Jan; 24(1):131–43.
4. Wang C, Chow SS, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers. 2013 Feb; 62(2):362–75.
5. Wang C, Wang Q, Ren K, Cao N, Lou W. Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing. 2012 Apr-Jun; 5(2):220–32.
6. Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y. Security and privacy for storage and computation in cloud computing. Information Sciences. 2014 Feb; 258:371–86.
7. Rewagad P, Pawar Y. Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. 2013 International Conference on Communication Systems and Network Technologies (CSNT); Gwalior. 2013 Apr 6-8. p. 437–9.
8. Sun W, Yu S, Lou W, Hou Y T, Li H. Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. 2014 Proceedings IEEE INFOCOM; Toronto, ON. 2014. p. 226–34.
9. Liu Q, Wang G, Wu J. Clock-based proxy re-encryption scheme in unreliable clouds. 41st International Conference on Parallel Processing Workshops (ICPPW); Pittsburgh, PA. 2012 Sep 10-13. p. 304–5.
10. Alshehri S, Radziszowski SP, Raj RK. Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. IEEE 28th International Conference on Data Engineering Workshops (ICDEW); Arlington, VA. 2012 Apr 1-5. p. 143–6.
11. Ruj S, Nayak A, Stojmenovic I. Dacc: Distributed access control in clouds. IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); Changsha. 2011 Nov 16-18. p. 91–8.
12. Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security; 2013. p. 523–8.
13. Wang G, Liu Q, Wu J, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers and Security. 2011 Jul; 30(5):320–31.
14. Li J, Chen X, Jia C, Lou W. Identity-based encryption with outsourced revocation in cloud computing. IEEE Transactions on Computers. 2015 Feb; 64(2):425–37.
15. Zheng Q, Xu S, Ateniese S. Vabks: Verifiable attribute-based keyword search over outsourced encrypted data. 2014 Proceedings IEEE INFOCOM; Toronto, ON. 2014. p. 522–30.
16. Liu Q, Wang G, Wu J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences. 2014 Feb; 258:355–70.
17. Wu Y, Wei Z, Deng R. Attribute-based access to scalable media in cloud-assisted content sharing. IEEE Transactions on Multimedia. 2013 Jun; 15(4):778–88.
18. Xu D, Luo F, Gao L, Tang Z. Fine-grained document sharing using attribute-based encryption in cloud servers. 2013

Third International Conference on Innovative Computing Technology (INTECH); London. 2013 Aug 29-31. p. 65–70.
19. Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing. 2011 31st International Conference on Distributed Computing Systems (ICDCS); Minneapolis, MN. 2011 Jun 20-24. p. 383–92.
20. Zhu Y, Hu H, Ahn G-J, Huang D, Wang S. Towards temporal access control in cloud computing. 2012 Proceedings IEEE INFOCOM; Orlando, FL. 2012 Mar 25-30. p. 2576–80.
21. Tomy D, Dhanalakshmi S, Karthik S. Implementing HASBE Scheme for setting up access controls in out-sourced data clouds. International Journal of Sceince, Engineering and Technology Research. 2013 Apr; 2(4):877–80.
22. Wu Y, Wei Z, Deng RH. Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks. IEEE Transactions on Multimedia. 2013 Jun; 15(4):778–88.
23. Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable and fine-grained daa access control in cloud computing. INFOCOM 2010 Proceedings of the 29th Conference on Information Communications; San Diego, CA. 2010 Mar 14-19. p. 534–42.
24. Hur J. Improving security and efficiency in attribute-based data sharing. IEEE Transactions on Knowledge and Data Engineering. 2013 Oct; 25(10):2271–82.
25. Lin H, Chow SSM, Xing D, Fang Y, Cao Z. Privacy-preserving friend search over online social networks. IACR Cryptology ePrint Archive; 2011. p. 1–11.
26. Yu J, Lu P, Zhu Y, Xue G, Li M. "Toward secure multikeyword Top-k retrieval over encrypted cloud data. IEEE Transactions on Dependable and Secure Computing. 2013 Jul-Aug; 10(4):239–50.
27. Radhika T, Vasumathi Kannagi S. Survey on user revocation and fine grained access control of PHR in cloud using HASBE. International Journal of Computer Science and Mobile Computing. 2014 Jan; 3(1):452–6.
28. Yadav S, Kalaskar K. Security of data and processing in cloud computing. Sai Om Journal of Science, Engineering and Technology. 2014; 1(2):1–7.
29. Senthil Kumari P, Nadira Banu Kamal AR. Effective search of cloud data depending on PBC based cryptography and multiple keyword semantics. National Conference on Recent Trends in Conference on Recent Trends in Communication Engineering, Organized by Sree Sastha College of Engineering, Chennai. 2014; 1:13–8.
30. Senthil Kumari P, Nadira Banu Kamal AR. An effective search of cloud data using ABC based cryptography and multiple keyword semantics. International Journal of Innovative Computing, Information and Control. 2015 Aug; 11(4):1257–67.
31. Akshaya B, Sudha C, Suvedha B, Shanthi P, Umamakeswari A. Efficient ABBE for improving cloud security in a dynamically changing user environment. Indian Journal of Science and Technology. 2015 May; 8(S9):306–11.
32. Shanthi P, Saranya Devi B, Shruthi S, ThivyaRajeswari S, Umamakeswari A. secure data sharing in scalable mobile cloud environment using HABE with re-encryption. Indian Journal of Science and Technology. 2015 May; 8(9):340–5.