IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. II (Jan.- Feb. 2018), PP 44-55
www.iosrjournals.org

An Emprical Study on Secured Cloud Storage Techniques

P Jayasree [1], Dr.V.Saravanan [2]
Ph.D Research Scholar,Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India [1].,
Head & Associate Professor, Department of Information Technology(PG),Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India [2].
Corresponding Author: P Jayasree

Abstract: *Cloud computing is a large-scale distributed computing paradigms for Information and Communications Technology because of promising vision. Cloud computing presents an incredible convenience for organizations to store the data in cloud. The key advantage of cloud storage is ubiquitous user accessibility and virtually unlimited data storage capability. Data integrity is preservation, assurance of accuracy and consistency of data over its complete life-cycle. It is an essential feature to design, execution and usage of system that stores, processes, or retrieve data. Cloud data auditing is an essential for securing the cloud storage as it allocates the cloud users to authenticate the integrity of outsourced data in efficient manner. However, the existing techniques failed to improve the data integrity rate and reduce the data accessing time. Our main objective is to improve the security of cloud storage by considering cryptographic techniques.*

Keywords: *Cloud computing, Cloud data auditing, Cloud storage, Information and Communications Technology, Data integrity*

Date of Submission: 25-01-2018 Date of acceptance: 15-02-2018

I. Introduction

Cloud computing is a revolutionary method to enterprise the hardware and software design. Cloud computing increased the advantages to the cloud clients like costless services, resource elasticity and easy access via internet. Cloud user is disinclined to place confidential or sensitive data such as personal health records, emails and government sensitive files. When data are stored in cloud datacenter, the client lost the direct control over data sources.

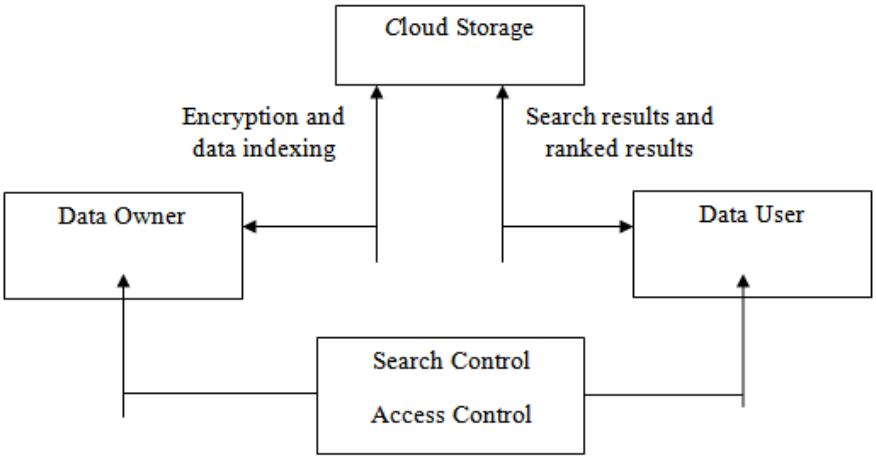

Figure 1 Secured Cloud Storage Process

In figure 1, the process of secured cloud storage is described. Cloud Service Provider (CSPs) guarantees the data security over the stored data of cloud clients through techniques like firewalls and virtualization. The sensitive data encryption before storing the data merits data privacy and confidentiality against CSP. An essential problem with encryption scheme is addressed that it is not practical due to

communication overhead over cloud access patterns. The cloud required the secure technique to storage and management for preserving the data confidentiality and privacy. The cloud computing not provided the control over the stored data in cloud data centers. The cloud service providers have control over the data and perform malicious tasks like copy, demolishing, changing, etc. The features of cloud computing are virtualization. The multi tenancy has many possibilities of attacks than generic cloud model.

This paper is organized as follows: Section II discusses the review on different secured cloud storage techniques, Section III portrays the study and analysis of the existing secured cloud storage techniques, Section IV describes the possible comparison of existing techniques. In Section V, the discussion and limitations of the existing secured cloud storage techniques are studied and Section VI concludes the paper.

II. Literature Survey

A novel construction of identity-based (ID-based) RDIC protocol was designed in [1] with key-homomorphic cryptographic primitive to lessen complexity and cost for creating as well as controlling the public key authentication framework in PKI-based RDIC systems. However, the designed protocol failed to provide the assurances for accessibility of each repository in cloud server. In [2], an efficient public integrity auditing scheme was introduced by secure group user revocation using vector commitment and verifier-local revocation group signature. But, the designed scheme was not secure against the collusion attacks in cloud storage server as well as revoked group users in user revocation.

A new proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography called IDentity-base Proxy-oriented data Uploading and remote data Integrity Checking in public cloud (IDPUIC) was introduced in [3]. But, the hashing process was not carried out for integrity checking using IDPUIC. A Cellular Automata based secure distributed storage scheme with Integrity Proof called CAD-IP was introduced in [4]. CAD-IP controlled the threshold based storage service for increasing the confidentiality of user private data. But, the designed storage scheme failed to present the security for the large files.

A new Data Access Control for Multi-Authority Cloud Storage (DAC-MACS) scheme called NEDAC-MACS scheme was introduced in [5] to resist two attacks for guaranteeing secure attribute revocation. Though the communication and computation overhead was reduced, authentication was not carried out using DAC-MACS scheme. An identity-based data outsourcing (IBDO) scheme was introduced in [6] with essential features in securing the outsourced data for addressing the integrity issues. IBDO scheme allocates user to allow the proxies for uploading the data to the cloud storage server. But, the storage complexity was not reduced using identity-based data outsourcing scheme. A key updating and authenticator-evolving mechanism was introduced in [7] with zero-knowledge privacy of stored files for secure cloud data auditing. But, key updating and authenticator-evolving mechanism consumed large amount of time for performing the secure cloud data auditing as it undergoes integrated verification process.

A new public auditing scheme was introduced in [8] for secure cloud storage using the dynamic hash table (DHT). The designed scheme is a two-dimensional data structure at third parity auditor (TPA) to record data property information for dynamic auditing. However, the data confidentiality rate was not improved using the public auditing scheme. For addressing the key management problems in cloud data auditing, an identity-based cloud data integrity checking protocol (ID-CDIC) [9] reduced the certificate management in traditional cloud data integrity checking protocols. Though the computation cost was minimized, hash value was not generated in RSA which reduced the data integrity in ID-CDIC protocol.

III. Secured Cloud Storage Techniques

Cloud computing is the delivery of computing and storage capacity as service to users. Cloud storage is an essential one with the networked online storage and data is stored in virtualized pools of storage. Access control mechanism is an important one that protects the complex IT environment that supports the separation and integrity of different levels or categories of information belonging to multiple parties. Access controls failed to stand on their own as they are maintained by additional security capabilities. Access control is based on identity management capability that addresses the requirements for the implementation.

3.1 Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage

A new identity-based (ID-based) RDIC protocol was introduced by using key-homomorphic cryptographic primitive to lessen the system complexity and cost for public key authentication framework in PKI-based RDIC techniques. In an ID-based signature scheme, anyone with the access to signer identity verify signature of signer. In ID-based RDIC protocols, the person knowing cloud user identity verifies data integrity for the cloud user. Public verifiability is advantageous than private verification in ID-based RDIC for resource constrained cloud users. The property of zero-knowledge privacy is important for the data confidentiality in ID-

based RDIC protocols. The key objective is to formalize the security model of zero knowledge privacy against TPA in ID-based RDIC protocols at first time.

A concrete ID-based RDIC protocol is a new construction that is different from existing by using the idea of new primitive called asymmetric group key agreement. The challenge-response protocol is a two party key agreement between TPA and cloud server where challenged blocks were used when generating the shared key from the TPA by cloud server. The security proofs of protocol with the soundness and zero-knowledge privacy of the stored data are described. The security proofs are employed in generic group model. It is the first correct security proof of the ID-based RDIC protocol. The new security proof method is independent interest.

The data owners themselves observe the integrity of cloud data using two-party RDIC protocol. The auditing result from data owner or cloud server is biased in two-party scenario. The RDIC protocols with public verifiability audits the integrity of outsourced data. For description of the publicly verifiable RDIC protocols, there exit third party auditor (TPA) who has the capabilities for performing the verification work. Four entities namely KGC, cloud user, cloud server and TPA are used in the system. KGC generates the secret keys for all users consistent with their identities. The cloud user comprises many number of files stored on cloud without local copy. The cloud server comprises storage space and computation resources with data storage services for cloud users. TPA has expertise and capabilities where the cloud users failed to check the integrity of cloud data for cloud user upon request. Each entity has own obligations and advantages respectively. The cloud server are self-interested with own benefits to preserve good reputation. The cloud server hides the data corruption incidents to the cloud users. The cloud server does not have incentives to expose the hosted data to TPA due to the regulations and financial incentives. TPA performs the data integrity checking on behalf the cloud user.

3.2 Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud

A new proxy-oriented data uploading and remote data integrity checking model is introduced in identity-based public key cryptography termed as identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC). The designed ID-PUIC protocol is efficient as the certificate management is removed. ID-PUIC is a new proxy-oriented data uploading and remote data integrity checking model in public cloud. The formal system model and security model are given for ID-PUIC protocol. Depending on the bilinear pairings, concrete ID-PUIC protocol was introduced. In random oracle model, the designed ID-PUIC protocol is secure. With the original client authorization, designed protocol recognizes the private checking, delegated checking and public checking.

A concrete ID-PUIC protocol includes five processes, namely Setup, Extract, Proxy-key generation, TagGen, and Proof. Initially, setup is carried out and the system parameters are generated. Depending on the generated system parameters, the other process is carried out. In phase Extract, when entity identity is input, KGC creates the entity private key. It creates the private keys for the client and proxy. In Proxy-key generation, the original client generates warrant and helps proxy generate the proxy key. In TagGen when data block is input, the proxy creates the block tag and uploads the block-tag pairs to PCS. In phase Proof, original client cooperates with the PCS. Through interaction, original client verifies their remote data integrity.

3.3 Cellular automata based secure distributed storage scheme with integrity proof

A Cellular Automata based secure Distributed storage scheme with Integrity Proof called CAD-IP is introduced. CAD-IP uses the threshold based storage service to increase the confidentiality of user private data. Homomorphic hashing is used in CAD-IP scheme that employs the verifier to check the integrity of data on servers. A sampling strategy minimized the computation and communication cost. The designed scheme improved the confidentiality and unforgeability to identify the alteration or deletion of file shares. With the implementation and pseudorandom behavior, cellular automata are used in cryptography. The schemes are not optimal solutions for distributed cloud storage that failed to present the integrity proof. The threshold storage of file guarantees the confidentiality and robustness. In addition, it undergoes the Byzantine failures where storage server failed in random manner.

3.4 On the Security of Data Access Control for Multiauthority Cloud Storage Systems

Data access control are demanding problem in cloud storage systems. The two attacks are given DAC-MACSs and EDAC-MACSs revocation security that are not guaranteed through the cryptanalysis. A new extensive DAC-MACS scheme called NEDAC-MACS is introduced to address the two attacks and manages the secure attribute revocation. The two attacks are constructed on vulnerabilities of revocation security in DAC-MACS and EDAC-MACS. By the first attack, the revoked user attains the other users Key Update to update their Secret Keys. In addition, it attains proper Token to decrypt secret information as nonrevoked user. By second attack, the revoked user interrupts the Ciphertext Update Key to recover their ability to decrypt secret information as nonrevoked user.

DAC-MACS algorithms are changed and executed the essential cipher-text update communication between cloud server and attribute authority (AAs) with secure algorithms. NEDAC-MACS scheme comprises two enhancements on DAC-MACS at Secret Key Generation phase and Attribute Revocation phase. The designed scheme functions correctly consistent with the correctness proof of NEDAC-MACS. Formal cryptanalysis of NEDAC-MACS is explained to establish that NEDAC-MACS guarantee the collusion resistance, secure attribute revocation, data confidentiality and provable security against corruption of authorities depending on the random oracle model. The performance analysis of NEDAC-MACS are carried out through comparing the efficiency among CP-ABE schemes to show NEDAC-MACS is security-enhanced one without minimizing the efficiency. The overhead of decryption is securely outsourced to cloud server, storage overhead, communication and computation of NEDAC-MACS are superior to DACC and similar to DAC-MACS.

3.5 Implementation of searchable symmetric encryption for privacy preserving keyword search on cloud storage

A privacy preserving data storage and retrieval system was introduced in cloud computing. The scopes include the utilization of searchable encryption algorithms to search for keywords within the encrypted content to download the database and decrypt the contents before searching. The designed solution delegates the searching on encrypted data to CSP with the privacy preservation. For searchable encryption algorithm, secure Searchable Symmetric Encryption-2 (SSE-2) scheme is introduced. The SSE-2 scheme presents simple and efficient method to enable searching over encrypted data while preserving the data privacy. The reason behind choosing the private/symmetric key for execution reduced the computational overhead when compared to public/asymmetric key counterpart and suitable for mobile devices.

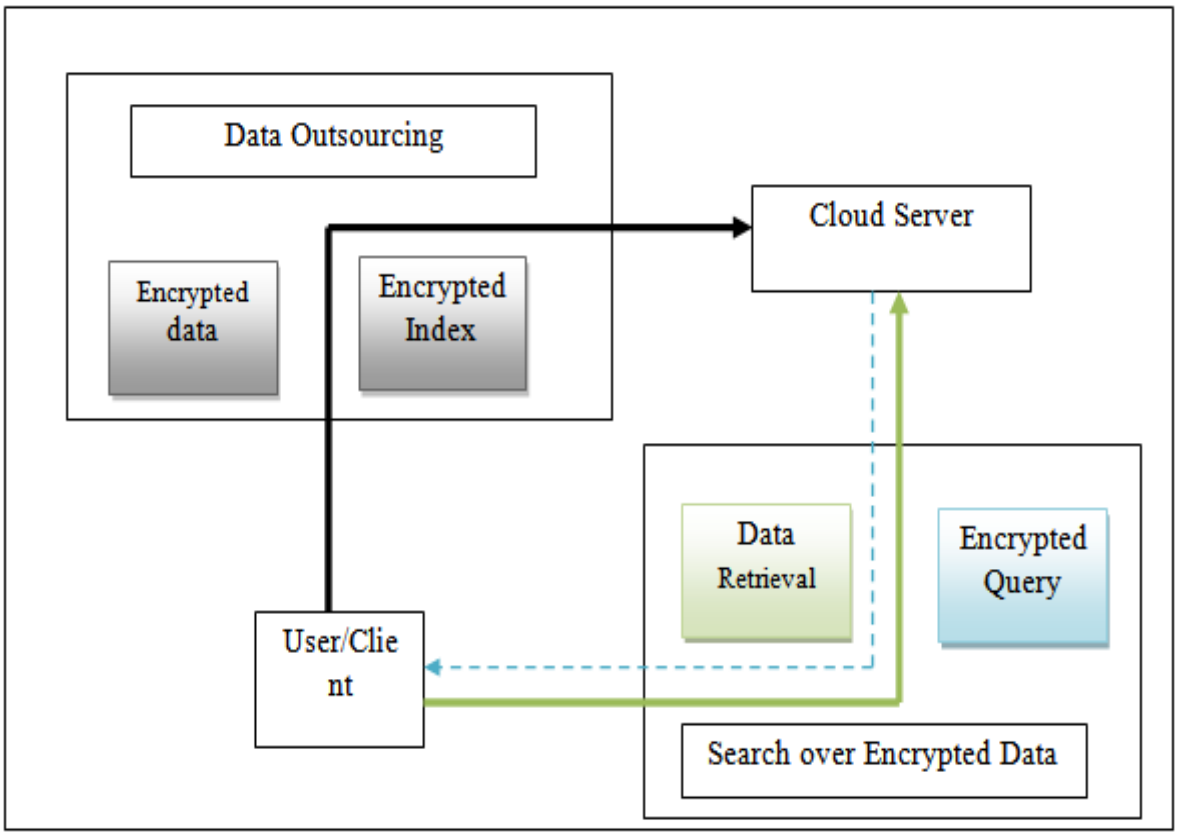

Figure 2 Privacy Preserving Data Storage and Retrieval System

From figure 2, the user 'U' encrypts the collection of data and creates encrypted index file 'I' with 'm' encrypted keywords extracted from the dataset 'D'. For searching over encrypted data, user 'U' outsources the index 'I' and encrypted dataset 'D' to cloud server. During the search, U generates an encrypted query and sends it to the server. Cloud server considered the encrypted query as the input and employed the encrypted index located at server to retrieve the pointers to document with searched keyword. When the search result is achieved, the encrypted document with searched keyword is returned to the client.

3.6 Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds

Cloud storage system presented the file storage and sharing services for the distributed clients. For improving the integrity, outsourcing and auditing on outsourced files, an identity-based data outsourcing (IBDO) scheme equipped with desirable features in securing the outsourced data. IBDO scheme authenticates the proxies to upload the data to the cloud storage server. The company authorizes employees to upload the files in company cloud account. The proxies are identified with recognizable identities that eliminate difficult certificate management in secure distributed computing systems. IBDO scheme is used for auditing. The designed scheme allocates the integrity auditing for protecting outsourced data and audit information on data origin, type and outsourced files consistency. An identity based data outsourcing and secure IBDO scheme allowed the file-owner to delegate the outsourcing capability to proxies. The authorized proxy process and outsource the file in support of file-owner. The file origin and file integrity are verified through a public auditor.

3.7 Cloud data integrity checking with an identity-based auditing mechanism from RSA

Cloud computing is a kind of large-scale distributed computing models for Information and Communications Technology. Many cloud data auditing schemes are introduced but majority is depending on Public Key Infrastructure (PKI). It is essential to verify the validity of public key certificates before any public key that creates the verifier incur expensive computation cost. Complex certificate management makes protocol ineffective. For addressing the key management problems in cloud data auditing, an identity-based cloud data integrity checking (ID-CDIC) protocol is introduced. ID-CDIC protocol eliminates the complex certificate management in traditional cloud data integrity checking protocols. The designed concrete construction from RSA signature supported the variable-sized file blocks and public auditing. A formal security model for ID-CDIC is introduced under RSA assumption with large public exponents in random oracle model.

3.8 Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

Cloud storage is an application of cloud computing that present on-demand outsourcing data services for organizations and individuals. The users not trust the cloud service providers (CSPs) where it is not easy to decide whether CSPs meet legal expectations for data security. It is significant to an efficient auditing method to support data owners trust and confidence in cloud storage. A new public auditing scheme was introduced for secure cloud storage depending on dynamic hash table (DHT). The designed scheme is new two-dimensional data structure at third parity auditor (TPA) to record data property information for auditing. The designed scheme shifted the authorized information from CSP to TPA and minimized the computational cost and communication overhead. The designed scheme increased updating efficiency. The designed schemes are used for privacy preservation by joining the homomorphic authenticator depending on public key with random masking generated by TPA and attain batch auditing using aggregate BLS signature technique.

3.9 Dynamic remote data auditing for securing big data storage in cloud computing

An efficient remote data auditing (RDA) technique is introduced for securing the big data storage in cloud computing using algebraic signature. The signature allocates the auditor to verify the data possession in cloud storage and incurs the lesser computational overheads on auditor and server in comparison to the homomorphic cryptosystem. The data auditing method is introduced through data structure that allows auditor to execute the dynamic data update operation with minimum computational overhead on client and cloud server. An efficient RDA is introduced for data storage depending on algebraic signature. The scheme reduced the lesser computational and communication costs on auditor and server side. A new data structure called Divide and Conquer Table (DCT) is constructed to support dynamic data operations like insert, append, delete, and modify. With new data structure, the designed method is used for the frequent update of large-scale data with minimal computational cost on auditor and server.

IV. Comparison Of Secured Cloud Storage Methods & Suggestions

To compare various parameters such as space complexity, data integrity rate, security level of data access, privacy preserving rate, average individual auditing time, computation cost and for the security providence of multimedia digital data using various techniques such as Identity-based (ID-based) RDIC protocol, identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC), Cellular Automata based secure Distributed storage scheme with Integrity Proof (CAD-IP), new extensive DAC-MACS scheme, Searchable Symmetric Encryption-2 (SSE-2) scheme, identity-based data outsourcing (IBDO) scheme, identity-based cloud data integrity checking (ID-CDIC) protocol, dynamic hash table with third parity auditor (DHT-PA) and remote data auditing (RDA) technique.

4.1 Space Complexity

Space complexity is defined as the amount of time taken for storing the number of data blocks of cloud user. It is measured in terms of megabytes (MB). The space complexity is mathematically formulated as,

$$Space\ Complexity = number\ of\ data\ blocks * space\ consumed\ for\ one\ block$$

When the space complexity is lesser, the method is more efficient.

Table 1 Tabulation of Space Complexity for Different Secured Cloud Storage Techniques

Number of data blocks (Number)	Space Complexity (MB)		
	ID-based RDIC protocol	IDPUIC Model	CAD-IP Scheme
10	25	35	41
20	28	38	44
30	32	40	46
40	35	42	47
50	37	43	49
60	40	45	52
70	41	46	55
80	44	47	58
90	46	49	61
100	49	52	64

Table 1 describes the space complexity of different secured storage techniques with respect to number of data blocks ranging from 10 to 100. Space complexity of Identity-based (ID-based) RDIC protocol, identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC) and Cellular Automata based secure Distributed storage scheme with Integrity Proof (CAD-IP) are explained. The graphical representation of space complexity is described in figure 3.

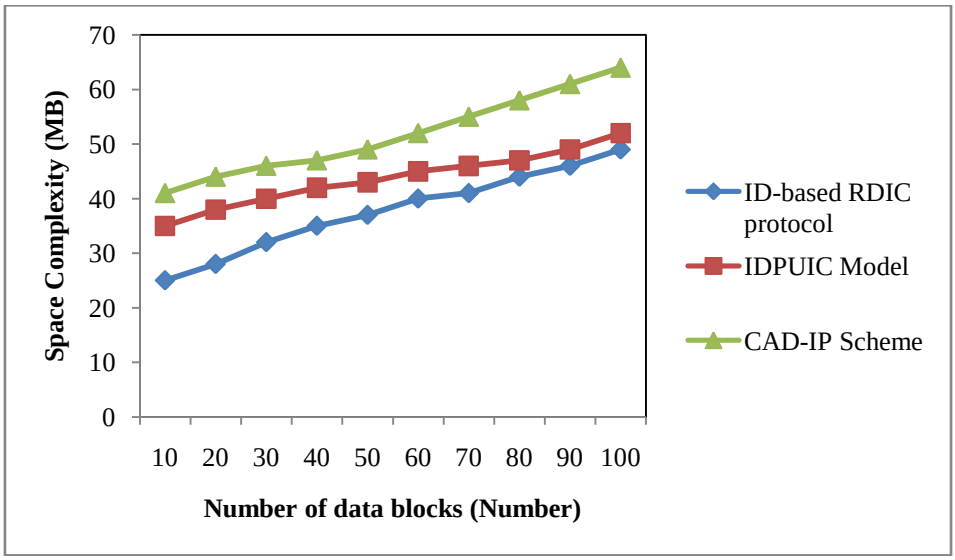

Figure 3 Measurement of Space Complexity for Different Secured Cloud Storage Techniques

From figure 3, space complexity based on different number of data block is explained. It is clear from figure 3 that space complexity of ID-based RDIC protocol is lesser than that of identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC) and Cellular Automata based secure Distributed storage scheme with Integrity Proof (CAD-IP). This is because of key-homomorphic cryptographic primitive to minimize the complexity and cost for establishing as well as for managing the public key authentication framework. The space complexity of ID-based RDIC protocol is 15% lesser than identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC) and 28% lesser than Cellular Automata based secure Distributed storage scheme with Integrity Proof (CAD-IP).

4.2 Data Integrity Rate

Data integrity is defined as the maintenance of and assurance of accuracy as well as data consistency over its entire period. Data integrity is measured in terms of percentage (%).

Table 2 Tabulation of Data Integrity Rate for Different Secured Cloud Storage Techniques

Number of data blocks (Number)	Data Integrity Rate (%)		
	ID-based RDIC protocol	IDPUIC Model	CAD-IP Scheme
10	61	69	75
20	64	72	78
30	66	75	81
40	68	77	82
50	71	79	83
60	75	81	85
70	79	83	87
80	81	86	89
90	83	88	91
100	85	90	94

Table 2 describes the data integrity rate with respect to number of data blocks ranging from 10 to 100. The data integrity rate is compared using Identity-based (ID-based) RDIC protocol, identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC) and Cellular Automata based secure Distributed storage scheme with Integrity Proof (CAD-IP). The graphical representation of data integrity rate is described in figure 4.

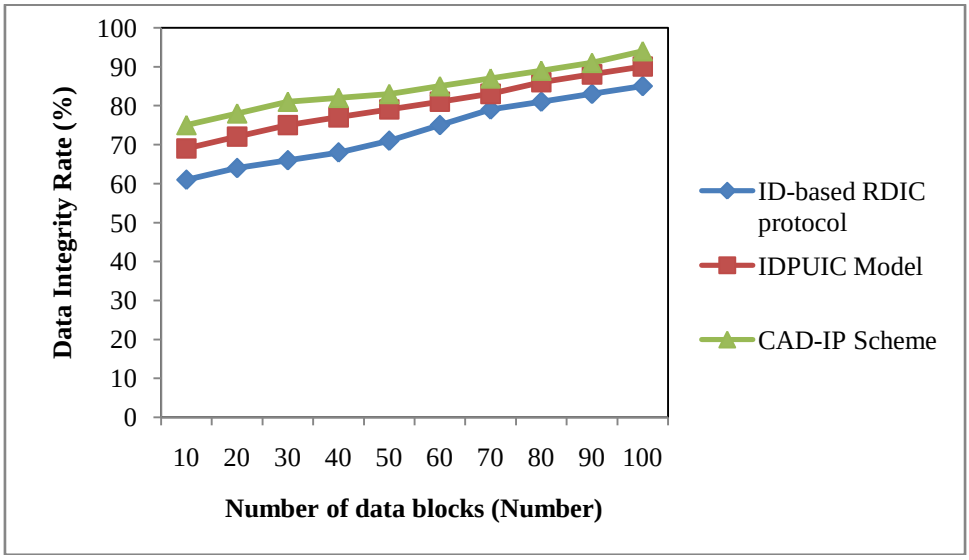

Figure 4 Measurement of Data Integrity Rate for Different Secured Cloud Storage Techniques

From figure 4, data integrity rate based on different number of data block is described. It is clear that data integrity rate of Cellular Automata based secure Distributed storage scheme with Integrity Proof (CAD-IP) scheme is higher than identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC) and ID-based RDIC protocol. This is because of Homomorphic hashing is used in CAD-IP scheme by verifier to check the integrity of data on servers. The data integrity rate of CAD-IP scheme is 6% higher than identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (IDPUIC) and 16% higher than ID-based RDIC protocol.

4.3 Security level of Data Access (SL)

The security level of data access is defined as the preserving ability of data during the access. It is measured in terms of percentage (%). The mathematical formula of security level of data access is given by,

$$SL = Packets\ stored - Packet\ accessed$$

When the security level is higher, the method is said to be more efficient.

Table 3 Tabulation of Security level of Data Access for Different Secured Cloud Storage Techniques

Number of data blocks (Number)	Security level of Data Access (%)		
	NEDAC-MACS scheme	SSE-2	IBDO Scheme
10	74	81	62
20	77	83	65

30	78	85	67
40	81	88	68
50	83	91	71
60	85	92	74
70	87	94	77
80	90	95	78
90	91	96	81
100	92	97	83

Table 3 describes the security level of data access with respect to number of data blocks ranging from 10 to 100 using three different techniques, namely new extensive DAC-MACS scheme, Searchable Symmetric Encryption-2 (SSE-2) scheme and identity-based data outsourcing (IBDO) scheme. The graphical representation of data access security level is described in figure 5.

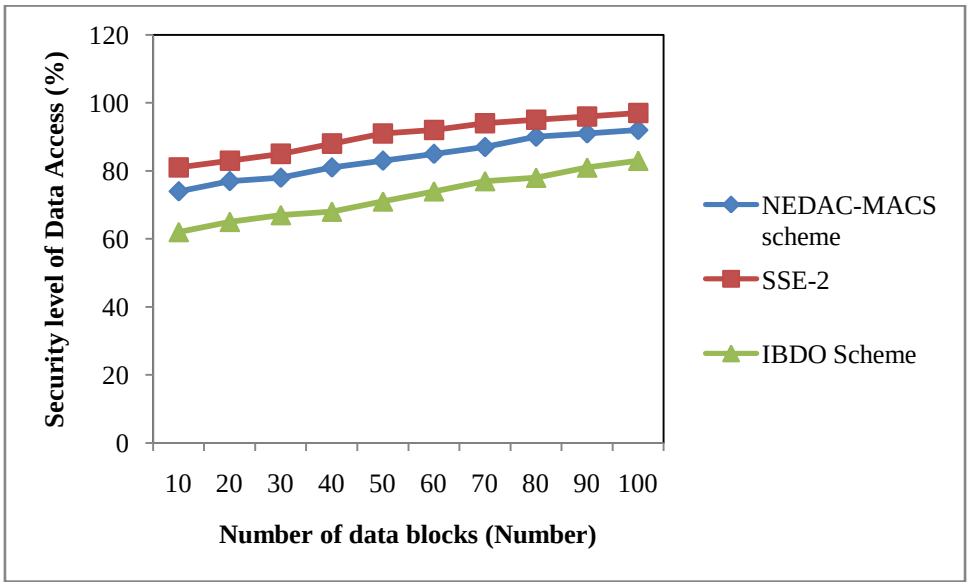

Figure 5 Measurement of Security Level of Data Access for Different Secured Cloud Storage Techniques

From figure 5, security level of data access based on different number of data block is described. It is clear that security level of Searchable Symmetric Encryption-2 (SSE-2) scheme is higher than new extensive DAC-MACS scheme and identity-based data outsourcing (IBDO) scheme. This is because that Re-Stream assigned the tasks by energy-efficient heuristic and critical path scheduling mechanism depending on architectural needs. The security level of Searchable Symmetric Encryption-2 (SSE-2) scheme is 16% higher than new extensive DAC-MACS scheme and 25% higher than identity-based data outsourcing (IBDO) scheme.

4.4 Privacy Preserving Rate

Privacy preserving rate is defined as the amount of data preserved from the unauthorized access. It is measured in terms of percentage (%). When the privacy preserving rate is higher, the method is said to be more efficient.

Table 4 Tabulation of Privacy Preserving Rate for Different Secured Cloud Storage Techniques

Number of data blocks (Number)	**Privacy Preserving Rate (%)**		
	NEDAC-MACS scheme	**SSE-2**	**IBDO Scheme**
10	61	73	82
20	63	75	84
30	65	76	85
40	68	78	86
50	69	80	87
60	71	82	89
70	73	83	91
80	76	86	92
90	77	87	93
100	79	89	95

Table 4 compares the privacy preserving rate with respect to number of data blocks ranging from 10 to 100 using three different techniques, namely new extensive DAC-MACS scheme, Searchable Symmetric

Encryption-2 (SSE-2) scheme and identity-based data outsourcing (IBDO) scheme. The graphical representation of privacy preserving rate is explained in figure 6.

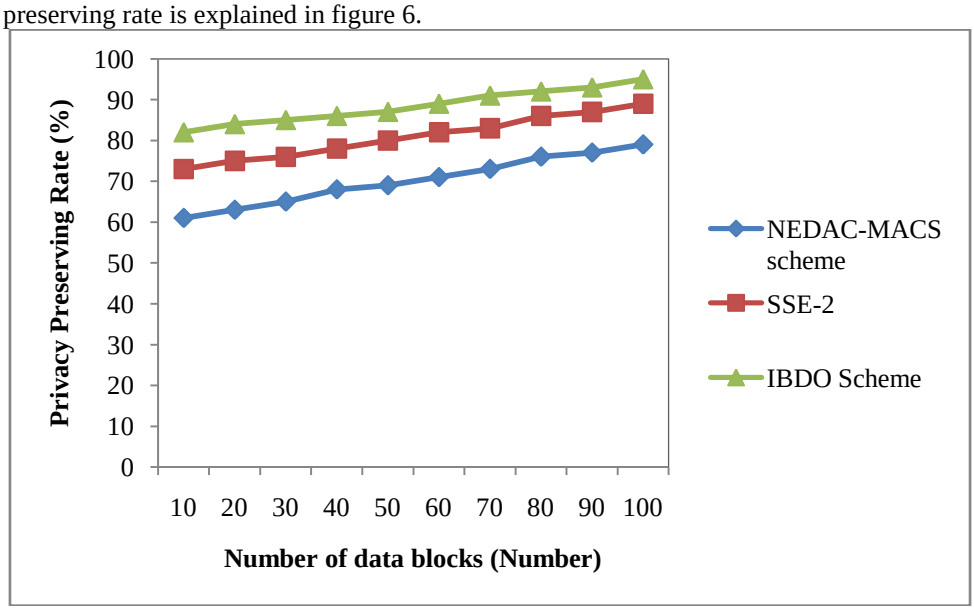

Figure 6 Measurement of Privacy Preserving Rate for Different Secured Cloud Storage Techniques

From figure 6, privacy preserving rate with respect to different number of data blocks is described. It is clear that privacy preserving rate of identity-based data outsourcing (IBDO) scheme is higher than new extensive DAC-MACS scheme and Searchable Symmetric Encryption-2 (SSE-2) scheme. This is because IBDO scheme permits the regular integrity auditing for securing the outsourced data and allowed to audit information on data origin, type and consistence. The privacy preserving rate of identity-based data outsourcing (IBDO) scheme is 26% higher than new extensive DAC-MACS scheme and 9% higher than Searchable Symmetric Encryption-2 (SSE-2) scheme.

4.5 Average Individual Auditing Time

Average Individual Auditing Time (AIAT) is defined as the amount of time consumed by third party auditor for auditing the data. It is measured in terms of milliseconds (ms). AIAT is mathematically formulated as,

$$AIAT = Ending\ time - Starting\ time\ of\ individual\ auditing$$

When the average individual auditing time is lesser, the method is said to be efficient.

Table 5 Tabulation Of Average Individual Auditing Time For Different Secured Cloud Storage Techniques

Number of auditing tasks (Number)	Average Individual Auditing Time (s)		
	ID-CDIC protocol	DHT-PA	RDA technique
25	1.41	0.81	1.26
50	1.42	0.82	1.26
75	1.43	0.82	1.27
100	1.43	0.83	1.28
125	1.43	0.84	1.28
150	1.43	0.84	1.29
175	1.44	0.86	1.29
200	1.44	0.86	1.30
225	1.45	0.86	1.30
250	1.45	0.87	1.30

Table 5 describes the average individual auditing time with respect to number of auditing tasks using identity-based cloud data integrity checking (ID-CDIC) protocol, dynamic hash table with third parity auditor (DHT-PA) and remote data auditing (RDA) technique. The graphical diagram of average individual auditing time is described in figure 7.

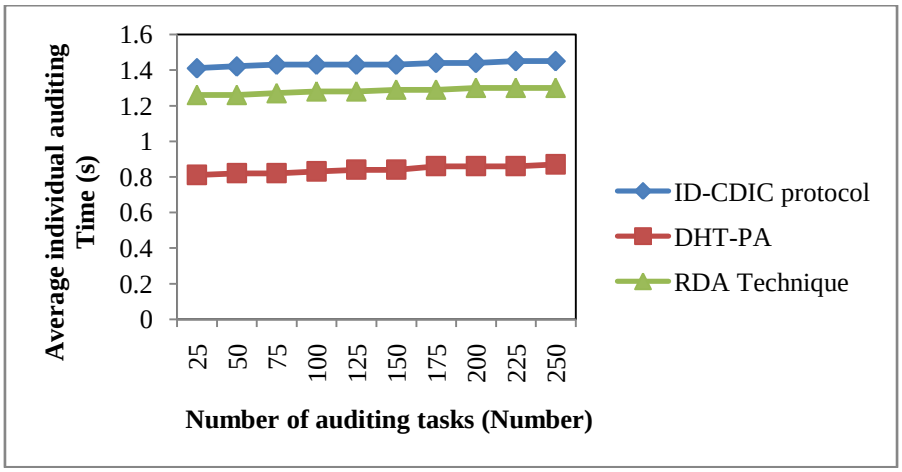

Figure 7 Measurement of Average Individual Searching Time for Different Secured Cloud Storage Techniques

From figure 7, average individual searching time with respect to different number of auditing tasks is described. It is clear that average individual searching time of dynamic hash table with third parity auditor (DHT-PA) scheme is lesser than identity-based cloud data integrity checking (ID-CDIC) protocol and remote data auditing (RDA) technique. This is because DHT-PA scheme shifted the authorized information from CSP to TPA and minimized the average individual searching time as well as computational overhead. The average individual searching time consumption of DHT-PA scheme is 41% lesser than identity-based cloud data integrity checking (ID-CDIC) protocol and 34% lesser than remote data auditing (RDA).

4.6 Computation cost

Computation cost is defined as time taken to perform integrity validation with respect to the file size. It is measured in terms of milliseconds (ms). Computation cost is mathematically evaluated as,

$$Computation\ cost = File\ size * time\ taken\ for\ integrity\ validation$$

When the computation cost is lesser, the method is said to be more efficient.

Table 6 Tabulation of Computation Cost for Different Secured Cloud Storage Techniques

File Size (GB)	Computation cost (ms)		
	ID-CDIC protocol	DHT-PA	RDA Technique
1	0.11	0.16	0.19
2	0.12	0.16	0.19
3	0.14	0.17	0.20
4	0.15	0.18	0.21
5	0.17	0.19	0.22
6	0.18	0.20	0.22
7	0.18	0.20	0.23
8	0.19	0.21	0.24
9	0.19	0.21	0.24
10	0.20	0.23	0.24

Table 6 explains the computation cost with respect to different file size ranging from 1 to 10 using different schemes, namely identity-based cloud data integrity checking (ID-CDIC) protocol, dynamic hash table with third parity auditor (DHT-PA) and remote data auditing (RDA) technique. The graphical diagram of computation cost is described in figure 8.

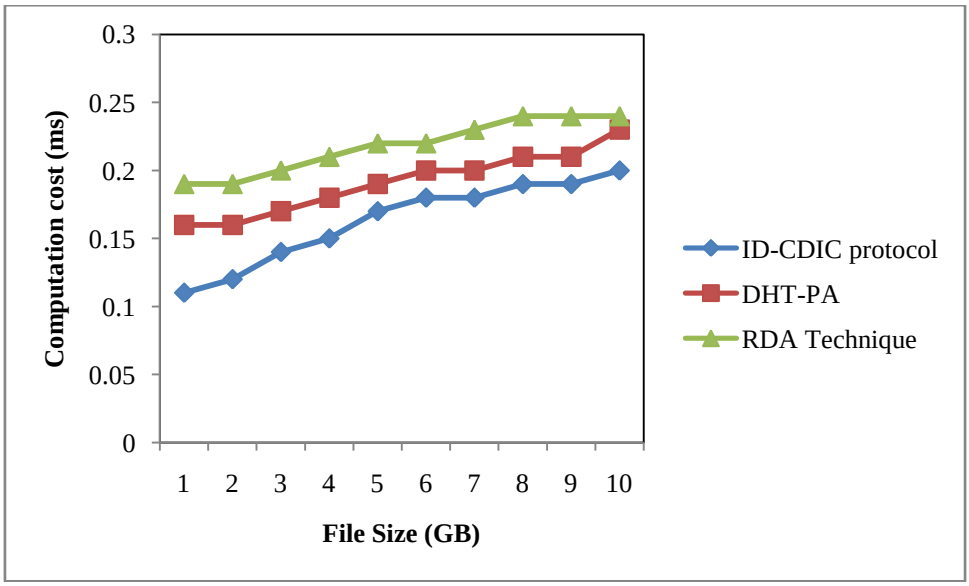

Figure 8 Measurement of Computation Cost for Different Secured Cloud Storage Techniques

From figure 8, computation cost with respect to different file size is described. It is clear that computation cost of identity-based cloud data integrity checking (ID-CDIC) protocol is lesser than dynamic hash table with third parity auditor (DHT-PA) scheme and remote data auditing (RDA) technique. This is because eliminating the complex certificate management in traditional cloud data integrity checking protocols. The computation cost of identity-based cloud data integrity checking (ID-CDIC) protocol is 15% lesser than DHT-PA scheme and 26% lesser than remote data auditing (RDA).

V. Discussion And Limitations On Secured Cloud Storage

A new construction of identity-based (ID-based) RDIC protocol was designed by key-homomorphic cryptographic technique to reduce system complexity for managing the public key authentication framework in PKI-based RDIC schemes. However, designed ID-based RDIC protocol failed to provide assurances for availability of every repository in cloud server. A new proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography called identity-based proxy-oriented data uploading and remote data integrity checking (IDPUIC) was designed in public cloud. But, the hashing process was not carried out for integrity checking using IDPUIC.

A Cellular Automata based secure Distributed storage scheme with Integrity Proof called CAD-IP was designed to leverage threshold based storage service with higher robustness and confidentiality of user private data. But, designed storage scheme failed to provide the security for large files. An identity-based data outsourcing (IBDO) scheme was introduced with desirable features in securing outsourced data for improving the integrity. However, the storage complexity was not reduced using identity-based data outsourcing scheme. An identity-based cloud data integrity checking (ID-CDIC) protocol was introduced to eliminate complex certificate management in traditional cloud data integrity checking protocols. Though the computation cost was reduced, hash value was not generated in RSA which reduced the data integrity in ID-CDIC protocol.

A new extensive DAC-MACS scheme (NEDAC-MACS) was designed to support secure attribute revocation by avoiding the attacks (DAC-MACS and EDAC-MACS). Though the communication and computation overhead was reduced, authentication was not carried out using DAC-MACS scheme. A new public auditing scheme was introduced for secure cloud storage using dynamic hash table (DHT). Data confidentiality rate was not improved using public auditing scheme. An efficient public integrity auditing scheme was introduced with secure group user revocation depending on vector commitment and verifier-local revocation group signature. The designed scheme was not secure against collusion attacks in cloud storage server and revoked group users in user revocation.

5.1 Related Works

An eXclusive-OR (XOR) homomorphism encryption scheme was introduced in [10] for secure keyword searching on encrypted data. A new data protection method was designed by encrypting the keyword and randomizing using the executing XOR operation with random bit-string for every session to preserve the access pattern leakage. But, the randomized session query and homomorphic evaluation key failed to control the data access against unauthorized user. A new secure k-NN query scheme was designed in [11] depending on the

encrypted cloud data. The designed approach increased the data privacy against cloud server (CS) where the encrypted database opposes the potential attacks of CS. But, the designed scheme failed to provide the secure analysis scheme on encrypted cloud data with additional realistic consideration such as protecting the data access patterns from CS.

A secure and efficient data collaboration scheme was introduced in [12] where fine-grained access control of ciphertext and secure data writing operation considering attribute-based encryption (ABE) and attribute-based signature (ABS) correspondingly. However, data synchronization guarantee process was not discussed in data collaboration. A privacy preserving keyword search was carried out in encrypted cloud data using Curtmola's Searchable Symmetric encryption scheme in [13]. The execution of privacy preserving data storage and retrieval system was carried out in cloud computing. But, index update process was static that failed to allow the addition of new files or updating files. The encryption module required large amount of time as it comprises conversion of documents into text file for keyword extraction process.

5.2 Future Direction

The future direction of secured data storage can be carried out using cryptographic techniques for increasing the security level and data integrity rate.

VI. Conclusion

A comparison of different existing secured cloud storage techniques is studied. From the study, it is observed that the existing techniques failed to improve the data integrity rate. The survival review shows that the existing eXclusive-OR (XOR) homomorphism encryption scheme failed to control the data access against unauthorized user. In addition, index update process was static that failed to allow adding of new files. The wide range of experiments on existing methods determines the performance of many secured cloud storage with its limitations. Finally, from the result, the research work can be carried out using cryptographic techniques for improving the performance of data integrity rate and data auditing time.

References

[1]. Yong Yu, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information Forensics and Security, Volume 12, Issue 4, April 2017, Pages 767-778

[2]. Tao Jiang, Xiaofeng Chen, and Jianfeng Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE Transactions on Computers, Volume 65, Issue 8, August 2016, Pages 2363 – 2373

[3]. Huaqun Wang, Debiao He and Shaohua Tang, "Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 6, June 2016, Pages 1165 – 1176

[4]. Yousheng Zhou, Feng Wang, Fei Tang and Xiaojun Wang, "Cellular automata based secure distributed storage scheme with integrity proof", Computers & Electrical Engineering, Elsevier, Volume 59, April 2017, Pages 291-304

[5]. Xianglong Wu, Rui Jiang, and Bharat Bhargava, "On the Security of DataAccess Control for Multiauthority Cloud Storage Systems", IEEE Transactions on Services Computing, Volume 10, Issue 2, March-April 2017, Pages 258 – 272

[6]. Yujue Wang, Qianhong Wu, Bo Qin, Wenchang Shi, Robert H. Deng and Jiankun Hu, "Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds", IEEE Transactions on Information Forensics and Security, Volume 12, Issue 4, April 2017, Pages 940 – 952

[7]. Yannan Li, Yong Yu, Bo Yang, Geyong Min and Huai Wu, "Privacy Preserving Cloud Data Auditing with Efficient Key Update", Future Generation Computer Systems, Elsevier, Volume 78, January 2018, Pages 789-798

[8]. Hui Tian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen and Jin Liu, "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", IEEE Transactions on Services Computing, Volume 10, Issue 5, September-October 2017, Pages 701 – 714

[9]. Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, Jian Shen, "Cloud data integrity checking with an identity-based auditing mechanism from RSA", Future Generation Computer Systems, Elsevier, Volume 62, September 2016, Pages 85-91

[10]. Shu Qin Ren, Benjamin Hong Meng Tan, Sivaraman Sundaram, Taining Wang, Yibin Ng, Chang Victor and Khin Mi Mi Aung, "Secure Searching on Cloud Storage Enhanced by Homomorphic Indexing", Future Generation Computer Systems, Elsevier, Volume 65, December 2016, Pages 102-110

[11]. Youwen Zhu, Zhiqiu Huang and Tsuyoshi Takagi, "Secure and controllable k-NN query over encrypted cloud data with key confidentiality", Journal of Parallel and Distributed Computing, Elsevier, Volume 89, 2016, Pages 1–12

[12]. Qinlong Huang, Yixian Yang and Mansuo Shen, "Secure and efficient data collaboration with hierarchical attribute based encryption in cloud computing", Future Generation Computer Systems, Elsevier, Volume 72, July 2017, Pages 239-249

[13]. Md Iftekhar Salam, Wei‑Chuen Yau, Ji‑Jian Chin, Swee‑Huay Heng, Huo‑Chong Ling, Raphael C‑W Phan, Geong Sen Poh, Syh‑Yuan Tan and Wun‑She Yap, "Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage", Human-centric Computing and Information Sciences, Springer, Volume 5, Issue 19, December 2015, Pages 1-16

P Jayasree "An Emprical Study on Secured Cloud Storage Techniques." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): PP 44-55.