I.J. Modern Education and Computer Science, **2014, 12, 26-33**
Published Online December 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.12.04

Information Interpretation Code For Providing Secure Data Integrity On Multi-Server Cloud Infrastructure

Sathiya Moorthy Srinivsan
Research Scholar, Manonmaniam Sundaranar University, Tamil Nadu, India Pin. 62701
sathiyamoorthy.srinivasan@gmail.com

Dr. Chandrasekar Chaillah
Asst. Professor, Periyar University, Salem, Tamil Nadu, India. 636011
ccsekar@gmail.com

Abstract—Data security is one of the biggest concerns in cloud computing environment. Although the advantages of storing data in cloud computing environment is extremely high, there arises a problem related to data missing. CyberLiveApp (CLA) supports secure application development between multiple users, even though cloud users distinguish their vision privileges during storing of data. But CyberLiveApp failed to integrate the system with certain cloud-based computing environments on multi-server. Environmental Decision Support Systems (EDSS) move away the technical load and focus mainly on decision-making activities. EDDS does not have a secure collaborative decision-making experience on cloud services. To integrate the security level for multi-server cloud infrastructure, Information Interpretation Code on Multi-Server (IICM-S) is proposed in this paper. To ensure the information with relevance to security on cloud-based computing environments, Information Interpretation Code (IIC) algorithm is initially developed. Thus, IIC guarantee that all information pertaining to cloud is in secured condition in order to prove the trustworthiness of data. In addition, the multi-sever cloud infrastructure in IIC provides access point for secure information recovery from cloud data server. The multi-server cloud infrastructure with IIC algorithm performs the recovery task on multi-server cloud infrastructure. The Multi-server Information (MI) scheme measures the integrity level with effective data recovery process. The integrity level on multi-server cloud infrastructure is ensured using two components, verifier and verify shifter. MI scheme proficiently check integrity using these two components so that not only the data integrity is provided as well as security is ensured in all cases using IICM-S. Experiment is conducted in the Cloudsim platform on the factors such as average integration time on multi-server, security level, recovery efficiency level.

Index Terms—Information Interpretation Code, Cloud Services, Security Level, Multi-server Information, Verifier, Data Integrity.

I. Introduction

With the increasing use of cloud-based computing environments, Information as a Service has emerged to meet the needs of the software users. The conventional method of using software has been replaced by the cloud environment to meet the higher demands of the software users. These paradigms provide different methods that enable efficient means for data, information sharing in cloud-based computing environments.

CyberLiveApp (CLA) [1] provided a secure application development for multiple users. Even though, the cloud users distinguish their privileges during data storing. A proxy-based filtering mechanism was used for delivering desktop operations to different users. Though the approach was flexible and provided the advantage of collaborative approach, the system failed to integrate with certain cloud-based computing environments on multi-server.

In [4], an efficient scheme called as the Provable Data Possession (PDP) was presented to provide scalability with the existence of multiple cloud service providers in existence. The advantage of using PDP remained cooperatively storing and maintains the clients' data by reducing the communication and computation overhead. Though scalability was achieved, it remained inefficient from the angle of cluster-based network model.

Personal Health Record [6] was designed to protect the personal health data of the patients that were stored on semi-trusted servers or cloud-based computing environments. The most sensitive personal health data of the patients was protected by applying an attribute-based encryption (ABE) mechanism to prove the scalability of the system. Though trustworthy and privacy of sensitive data was ensured, this attribute-based encryption mechanism was not suitable for other applications. In [13], regulatory frameworks were designed in order to protect the privacy of the sensitive cloud user data.

The usage of cloud-based computing environment in recent scenarios has had significant results from different angles ranging from life to economy. Cloud-based

computing environment is a method that enables access to network on-demand that in a way shares the pool of resources with minimal effort on the side of service provider. Environmental Decision Support Systems (EDSS) [2] concentrated mainly on activities related to decision-making. While the cost of the decision making process related to decision making was reduced drastically, it did not have a secure collaborative decision-making experience on cloud services.

The application of cloud computing leverages the customers possessing limited computational resources for outsourcing large-scale computations. But, providing security to the users' confidential data becomes a major security concern. In [7], a method that provided secure outsourcing model was designed in order to solve the linear equations in large-scale systems in cloud by increasing the security of users' confidential data. Application level security [16] and different types of security frameworks was introduced. However, providing security for web services remained unaddressed.

Cloud-based computing environment provides high level of scalability over the Internet on the basis of the needs and requirements of the cloud users'. One of the major features of cloud services is the processing of users' data in a remote manner in different machines where the users do not own or operate. Though the advantage of the system being convenience, lose of data control levy the cloud users' in the new emerging technology which again become one of the most felt drawbacks of many cloud services. In [3], a new method called as the decentralized information accountability using an object-based approach that kept track of the usage of the users' data in cloud environment was presented that provided the flexibility of users' control.

To provide flexibility and a secured model, multi tenancy was introduced in [17] for cloud computing environment. Though efficiency was achieved, it was not oriented towards user-centric and the time for achieving efficiency was high. To minimize the response time, a framework with multiple data centers was designed in [18]. However, users in different regions enjoyed good response time rather than those in the hybrid regions.

Though flexibility was addressed security a key concern was unaddressed. In [5], the significant task of assigning clients to a set servers with respect to cloud environment was designed in such a manner that size of clients allocated to a server was smaller than the achievable degree of the server while providing overall optimal throughput. But the computation cost involved was higher.

In this work, we endeavor to study the secure data integrity on multi-server cloud infrastructure and focus on addressing the complicate and challenging key security and recovery level. In order to prove the trustworthiness of data on a multi-server cloud infrastructure, we adopt Information Interpretation Code (IIC) as the main access point for secure information recovery during loss of data. Using Multi-server Information (MI) scheme, the integrity level is measured using two components namely Verifier component and Verify Shift component, which enables a cloud user to authenticate the information during recovery phase.

The remainder of the paper is organized as follows. In Section 2, the concept of secure data integrity model using information interpretation code on multi-server cloud infrastructure is designed with a neat block diagram. In Section 3, the implementation details of IICM-S are provided. In Section 4, simulations are conducted to evaluate IICM-S. Section 5 reviews related work on securing data integrity on multi-server. Finally, Section 8 concludes with a concluding remark.

II. A Secure Data Integrity Model Using Information Interpretation Code On Multi-Server

In this section, we present a scheme called as the Information Interpretation Code on Multi-server for cloud infrastructure. The main objective behind information interpretation code on multi-server is to check the security level of the cloud user information. The design of IICM-S includes two phases namely, information access phase and data recovery phase. These two phases are combined together to achieve a secure data integrity for user information on multi-server cloud infrastructure.

The first phase in IICM-S extracts all the user information. Then, the information entering into the cloud is measured using interpretation security method. In order to secure the user data on cloud infrastructure, Information Interpretation Code in the first phase uses the information that are added into the multi-server server area, i.e., both before and after the information is added into the multi-server server area. Ever data uploaded by the user in IICM-S model uses the Interpretation Code to measure the security level for both the client and server side. IIC maintain the security for the entire data exchange system using the interpretation signature on the multi-server cloud infrastructure. The data recovery process is performed in the second phase of IICM-S. With the information being secured, in the second phase, IICM-S model assure data integrity using Multi-server Information Scheme. The task of MI is to reduce the burden of the data owner by integrating data in the multi-server cloud infrastructure, without any information loss. The consistent (i.e.,) recover data in the cloud structure improves the security level by using two components namely, the verifier and verifier shift. The process of authentication in IICM-S is provided using the Verify component ensures the authorized information. Next, the component, Verify Shift provides authorization to access the recover information with the help of the Access Log File (ALF). The block diagram of IICM-S is explained as follows with the figure depicted in Fig 1.

Fig 1 illustrates the block diagram of IICM-S model with information access phase using Information Interpretation Code and data recovery phase using Multi-server Information scheme. According to the needs and requirements of the users, they send and receive cloud data. As depicted in the block diagram, the multi-server cloud infrastructure consists of many servers of different

configuration to store the information in cloud. The objective of IICM-S is to provide data flow (i.e., to and from the multi-server zone) with higher security level. The proposed IICM-S model consists of two phases such as information access phase and data recovery phase. The detailed description of the two phases is provided in the forthcoming subsections.

A. Information Access Phase

The first phase involved in the design of IICM-S is the information access phase. In the information access phase, the security of the cloud information is monitored using the Information Interpretation Code. The cloud users assure the information security in the cloud using the condition satisfaction.

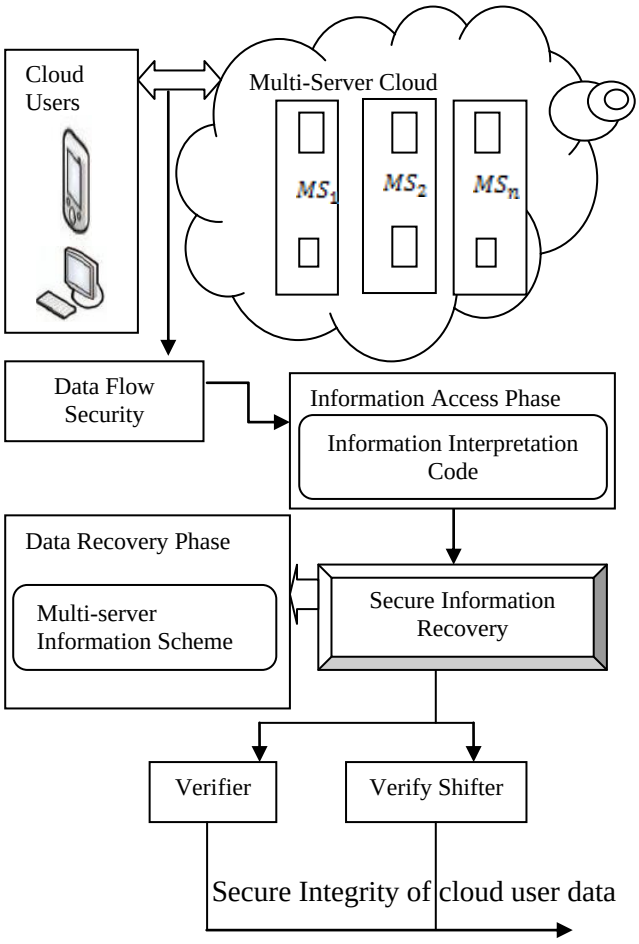


Fig. 1. Block Diagram of IICM-S model

Let us assume that particular size information is to be uploaded in multiple server cloud. Using IIC, the information is dividing into (n-1) parts, where 'n' is the no. of information counts in the cloud infrastructure. The information storage with security on server 'n' with count 'i' is denoted as,

$$\text{Secure Information } 'I' = \{n_i, n_{i+1}, \ldots . n_{i-1}\} \quad (1)$$

In order to confirm with the security of user information, the IIC always carries an interpretation signature in the cloud multi-server infrastructure. During uploading of client (i.e.,) cloud users information is provided to the server in IICM-S. In information access phase, while carrying out the upload operation to the server, 'n' signature is also appended with the user information.

The security of data is performed from the cloud user level using IICM-S before and after the information is being uploaded to the multi-server cloud infrastructure. Followed by this, the security level is verified using the information interpretation code on the client (i.e.,) users and server (i.e.,) multi-server side. The following equation part in IICM-S clearly explains about the security level checking.

$$N \in I, \quad Where\ N\ denotes\ 'IIC'\ and\ 'I'\ denotes\ cloud\ level\ Information \quad (2)$$

$$[N = \{i_c, i_{c+1}, i_{c+2} \ldots, i_{c-n}\} \quad (3)$$

The 'n' server with 'c' count of information is stored on the multi-server cloud infrastructure using IICM-S. The 'i' in the Eqn (3) specifies only the particular server on the multi-server cloud zone. To compute the relationship of security on multiple servers, Eqn (4) is presented as,

$$N = (R\{i_c, i_{c+1}, i_{c+2} \ldots, i_{c-n}\}, R_{i+1}\{i_c, i_{c+1}, i_{c+2} \ldots, i_{c-n}\} , \ldots, R_{i-n}\{i_c, i_{c+1}, i_{c+2} \ldots, i_{c-n}\}) \quad (4)$$

Where, R denotes different server divided into 'I' information with the interpretation signature on IIC multi-server cloud infrastructure. For the entire server 'i', the security verification process is explained with the help of algorithmic steps,

Begin
Input: 'I' information on server 'n', 'C Divided information count, 'R' Different servers in on Cloud infrastructure
Output: Secure Cloud Data information uploaded in 'R' servers
//Client Level Security
Step 1: If (n<=I) && (n==I)
Step 2: {
Step 3: For (i=0; i<=n; i++)
Step 4: Interpretation Signature =i
Step 5: Interpretation Signature++
Step 6: Else
Step 7: (n==R)
Step 8: n++
Step 9 :}
Step 10: End If Else
Step 11: End For
//Server Level Security
Step 12: Repeat step 1 to 11 on server side
End

The above algorithm describes the client and server level security computation using IICM-S. Similar client

level procedure is followed on the server level security verification also. The only difference being that the IIC code processing is performed in multi-server cloud infrastructure.

B. Data Recovery Phase

Once the uploaded information is provided security using the Information Interpretation Code, the data recovery phase is performed in IICM-S using the Multi-server Information (MI) scheme is carried out recover (i.e.,) sudden data lost in uploaded information. The design of IICM-S is based on provisioning of effective integrity of system without any information loss. MI Scheme compares the value of IIC with the current recovered value. The processing step followed in MI scheme helps to perform the secure integrity on the information and to recover the information during sudden lost.

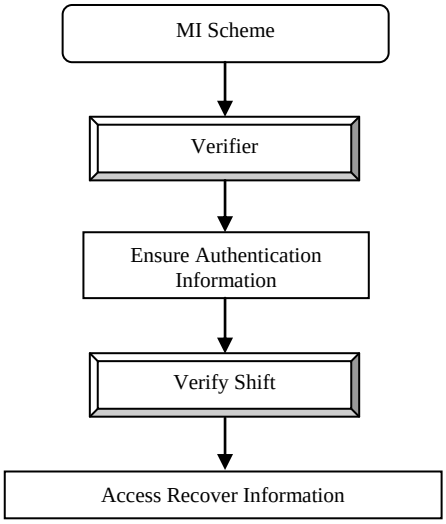


Fig. 2. Processing steps of MI Scheme

Fig 2 describes the processing step involved in the data recovery phase using MI scheme which is divided into two components, namely Verifier component and Verify Shift component. The MI scheme in IICM-S initially verifies and ensures the authentication of the information using the 'Verifier' component. The advantage of using MI Verifier component is that the information is recovered but does not allow retaining the information permanently.

The Verifier component in IICM-S model therefore authenticates the information using MI scheme. The cloud user information is then verified to provide access to the information.

The accessing of recovered information (i.e., in case of sudden data loss) is explained in the next subsection. The entity in the multi-server cloud infrastructure verifies the appended signature using the divided information parts, to easily authenticate the information with maximal integrity efficiency. The authentication on each access helps to improve the security on information integrity. With this, the access is granted and the information is made available to the different cloud users located at different location point.

The verified information in IICM-S then uses the 'Verify Shift' component to access the recovered information. The verifier shift performs the operation and provides access to recover the information. The verify shift hold the information and send the error corrected information to cloud users. The recovering work is computed as,

$$If\ (\sum_{i=0}^{n}[Interpretation\ Signature\ \ value] = \sum_{i=0}^{n} Current\ Value)\ then$$
$$Hidden\ \ information\ recovered$$
$$else\ Hidden\ information\ not\ recovered \quad (5)$$

Eqn (5) assess the interpretation signature with the current value to recover the hidden information from multi-server cloud infrastructure.

To guarantee security, record information is signed by entity using MI scheme. The signed information is checked to improve the integrity level. The MI scheme in IICM-S allows accessing at any time to recover the information. Information Interpretation Code on Multi-server mechanism (IICM-S) goal attained on security the information integrity operation on the multi-server cloud infrastructure.

III. Experimental Evaluations

Information Interpretation Code on the cloud multi-server infrastructure (IICM-S) using Cloudsim simulator performs the experimental evaluation. The experimental work is carried out in JAVA language for evaluating the security level. The particular toolkit has been preferred as a simulation platform as it contains the simulation structure in Cloud computing environments. To demonstrate the experimental work on the cloud simulator 8 GB of RAM and 1 TB of storage space is taken for the experimental work. Record Linkage Comparison Patterns Data Set from UCI repository is taken for the evaluation of the IICM-S mechanism.

The task compares the pattern and integrates the underlying records on the multi-server. IICM-SA mechanism compares the experimental result against the Existing CyberLiveApp scheme and Environmental Decision Support Systems (EDSS). IICM-S mechanism is compared on the factors such as average integration time on multi-server, recovery rate or recovery efficiency level, throughput, and security level.

Average integration time measures the time taken to perform the integral of over an interval (i.e., for multi-server) as given as

$$AIT = Time \int_{i=1}^{n} MS$$

Where MSrefers to the multi-server server in the range of i=1, 2, 3,….,n. Throughput in IICM-S measures the number of requests that a server can handle per second

which is measured in terms of %. The mathematical formula for throughput is given as

$$T = \frac{Number\ of\ cloud\ users * Number\ of\ active\ cloud\ users}{Request\ Rate} \quad (6)$$

The recovery efficiency level in IICM-S model measures the rate of recovery or the time taken to recover the information on multi-server infrastructure using eqn (5). The efficiency level of the recovery in IICM-S states that minimum the time taken to recover, the more efficient the recovery system. Security in IICM-S for the data flow is obtained by applying information interpretation code by using eqn (1).

IV. Results On IICM-S

In this section, certain simulations that were conducted to evaluate the secure data integrity using Information Interpretation Code on Multi-Server cloud infrastructure (IICM-S). Four performance aspects are analyzed namely, Average integration time on multi-server, recovery rate, throughput and security level.

The result analysis for providing secure data integrity using information interpretation code on multi-server cloud infrastructure is compared with existing CyberLiveApp (CLA) [1] and Environmental Decision Support Systems (EDSS) [2]. The table 1 represents the average integration time on multi-server using Cloudsim simulator and comparison is made with two other methods, namely CLA [1] and EDSS [2]. The simulation environment is shown in Fig 3.

Table 1. Average integration time on multi-server comparison with number of test made

Number of test made (c)	Average integration time on multi-server (ms)		
	IICM-S	CLA	EDSS
2	22	28	31
4	15	19	23
6	18	24	27
8	23	28	31
10	37	42	45
12	32	35	40
14	34	38	42

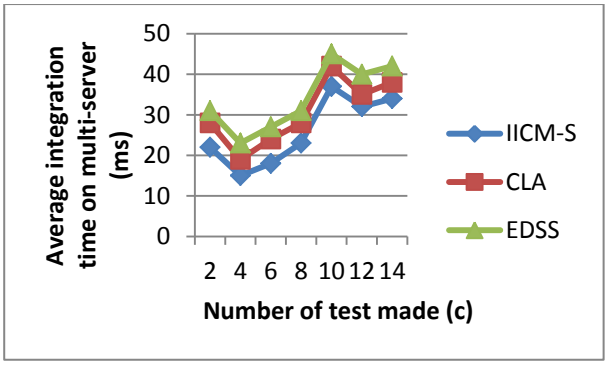


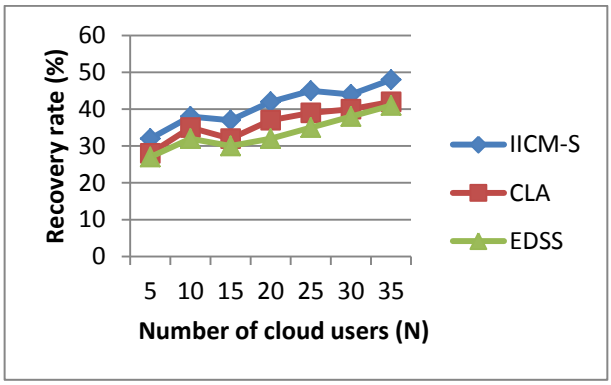
Fig. 3. Average integration time on multi-server for different tests

Fig 3 illustrates the average integration time on multi-server for different number of tests made. As illustrated in the Fig, the average integration time on multi-server does not increases or decreases linearly with the increasing number of tests made. This is because multi-server accepts any number of information from different cloud users which vary according to time. As a result, a test may include 5 cloud user or 3 cloud user and so on. But comparatively, the average integration time observed in IICM-S is less than the other two existing methods namely, CLA [1] and EDSS [2]. This is because by applying information interpretation code, in the information access phase, where 'n' server with 'c' count of information is stored on the multi-server cloud infrastructure using IICM-S. As a result, the average integration time is reduced by 9 – 33 % when compared to CLA and 21 - 50 % than EDSS.

Table 2. Recovery rate with different number of cloud users

Number of cloud users (N)	Recovery rate (%)		
	IICM-S	CLA	EDSS
5	32	28	27
10	38	35	32
15	37	32	30
20	42	37	32
25	45	39	35
30	44	40	38
35	48	42	41

The experimental results of recovery rate are illustrated in table 2. We can see that the three methods used are tested under same simulation environments with 7 cloud users taken into consideration for experiments.



Fig, 4. Recovery rate for different cloud users

Fig 4 illustrates the recovery rate for different cloud users (i.e. N). Comparison for recovery rate is made with two other methods, CLA [1] and EDSS [2] respectively. From the figure it is evident that the recovery rate using IICM-S is comparatively higher than other two existing methods over increased number of cloud users in the range 5 to 35 for experimental purpose. This is because of the Multi-server Information scheme carried out in the recovery phase of IICM-S which results in increase in

performance by 7 – 13 % when compared to CLA. Moreover, with the application of two components, Verify and Verify Shift in IICM-S, the recovery rate is improved by 14 – 23 % when compared to EDSS [2].

Table 3. Throughput level with different number of cloud users

Number of cloud users (N)	Throughput (%)		
	IICM-S	CLA	EDSS
5	65	62	60
10	68	66	63
15	71	68	66
20	69	65	64
25	73	69	66
30	75	72	69
35	74	70	66

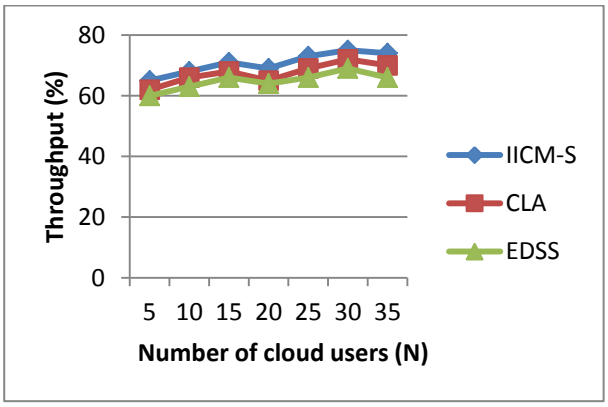


Fig. 5. Throughput level for different cloud users

Fig 5 shows the throughput level in multi-server cloud infrastructure for IICM-S, CLA [1] and EDSS [2] versus increasing number of cloud users from N = 5 to N = 35. The throughput improvement returned by security verification process over CLA and EDSS increases gradually as the cloud users gets increased. For example for N = 10, the percentage improvement of IICM-S compared to CLA is 2.9 percent and compared to EDSS is 7.35 percent, whereas for N = 15 the improvements are around 4.22 and 7.04 percent compared to CLA and EDSS respectively. The reason is that the security verification process evaluates client and server level security computation where similar client level procedure followed on the server level security verification increases the throughput by 2 – 5 % when compared to CLA and 7 – 10 % when compared to EDSS.

Table 4. Tabulation of Security Analysis

Methods	Security
IICM-S	85
CLA	72
EDSS	68

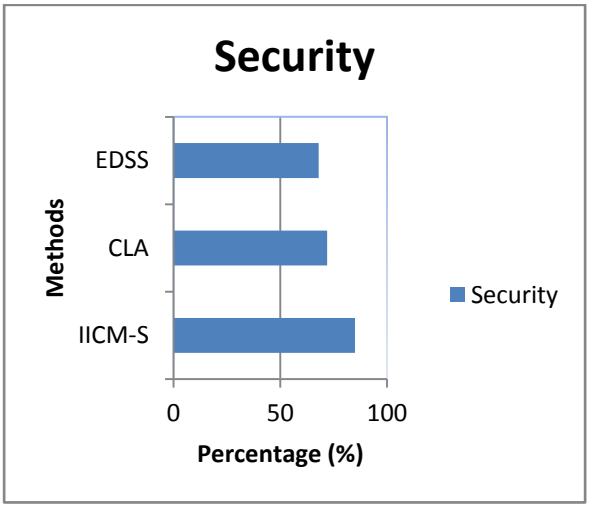


Fig 6 Security analysis chart

Table 4 and Fig 6 depict the security analysis chart for three methods IICM-S, CLA and EDSS. Apart from performance evaluation, the security of multi-server cloud infrastructure also plays the significant role for analysis. So it is highly required to evaluate the security involved in the process and it is also highly required to evaluate the performance of security level. As the proposed method IICM-S executes with respect to different number of cloud users executing different number of jobs for every configuration (i.e., multi-server), helps us in finding the best possible configuration for providing higher security levels to the cloud user.

From the figure, it is illustrative that the security level using IICM-S is high as the security level checking is performed for both single and multi-server resulting in the increase in level of 18 % when compared to CLA. In addition, the IICM-S maintain the security for the entire data exchange system using the interpretation signature on the multi-server cloud infrastructure the authentication on each access helps to improve the security on information integrity by 5 % when compared to EDSS.

V. Related Works

Cloud-based computing environment is a new paradigm that is purely based on distributed computing resources, virtualization, utility management and service-oriented architecture. The outsourced data in cloud environment used different method to achieve access control with the help of attribute-based encryption (ABE). But, most of the methods have the drawback of inflexibility while implementing complex access control policies.

In order to provide scalability, flexibility and provisioning of access control for outsourced data in cloud environment, Hierarchical Attribute-Set-Based Encryption (HASBE) [10] was designed. With the application of ABE, it achieved scalability and flexibility for compound attributes.

The storage of user data or information in cloud provides with a new solution in case of outsourcing the data or information in a remote manner. With this, the cloud provides the user with infinite amount of storage space for cloud user with the help of pay-and-use model. FADE [8], File Assured Deletion in cloud provides the cloud user with a secure cloud storage model and achieved access control based on the policy and assured deletion of the file by assuring value-added security. But certain issues related to arbitrary failure was unaddressed. Sharing of data in secured manner was addressed in [15] by considering privacy and confidentiality of data of arbitrary in nature.

With the increasing surge of Cloud Computing, a new development is the application of Internet with respect to computer technology. Ensuring data integrity was designed in [11] with the help of a third party auditor in Cloud Computing. The task of TPA is to verify the integrity of data using Merkle Hash Tree which proved to be highly efficient and scalable. Sometimes fraudulence in terms of prover may results in security breaches.

Interactive PDP protocol [12], provided efficient mechanism from fraudulence system using Diffie–Hellman assumption. Further, the data was leakage was also addressed using rewindable black-box knowledge extractor by minimizing the verification cost by efficiently detecting the abnormality. Though computation and communication overheads were reduced but at the cost of time. A Public Key Infrastructure [14], was deployed for assuring security in cloud environment using a trusted third party. The method ensured authentication, confidentially of data and data integrity from the point of view of cloud, but providing quality of services was not addressed.

Cloud-based computing environment, with its advantage of unlimited computation, storage of data storage and higher bandwidth level, is highly becoming choice for many business establishments. Self-adaptation [9], introduced a mechanism of decentralization using heuristic methods according to the market or user requirements by ensuring robustness and scalability. But the problem of collective adaptation was unsolved.

VI. Conclusion

In this paper, Information Interpretation Code on Multi-Server (IICM-S) is developed for multi-server cloud infrastructure. The proposed IICM-S ensures the trustworthiness of data by providing security for the user information. IICM-S also provides access point for secure information recovery from cloud data with the help of two components Verify and Verify Shift. With this, the integrity level with effective data recovery process is performed using Multi-server Information scheme. IICM-S model exploits both the security level and higher throughput level on multi-server cloud infrastructure. IICM-S derived an algorithm for security verification process to increase the security level. Simulation results demonstrate that the proposed IICM-S model outperforms two existing state-of-art models and results in increasing the security and throughput by reducing the average integration time on multi-server cloud infrastructure. The application of IICM-S model reduces the average integration time by 50 % when compared to the existing methods.

References

[1] Jianxin Li., Yu Jia., Lu Liu., Tianyu Woa., "CyberLiveApp: A secure sharing and migration approach for live virtual desktop applications in a cloud environment," Future Generation Computer Systems., Elsevier Journal., 2013.

[2] Alexander Sun., "Enabling collaborative decision-making in watershed management using cloud-computing services," Environmental Modeling & Software., Elsevier Journal., 2013.

[3] Smitha Sundareswaran, Anna C. Squicciarini, and Dan Lin," Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012.

[4] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Mengyang Yu," Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Sep 2012.

[5] Olivier Beaumont, Lionel Eyraud-Dubois and Hejer Rejeb," Heterogeneous Resource Allocation under Degree Constraints", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Oct 2012.

[6] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. X10, NO. 12, Oct 2012.

[7] Cong Wang, Kui Ren, Jia Wang, and Qian Wang," Harnessing the Cloud for Securely Outsourcing Large-scale Systems of Linear Equations", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Oct 2012.

[8] Yang Tang, Patrick P. C. Lee, John C. S. Lui, Radia Perlman," Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, Sep 2012.

[9] Vivek Nallur, Rami Bahsoon," A Decentralized Self-Adaptation Mechanism For Service-Based Applications in The Cloud", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, Mar 2012.

[10] Zhiguo Wan, Jun'e Liu, and Robert H. Deng," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[11] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.

[12] Yan Zhu, Hongxin Huc, Gail-Joon Ahnc, Stephen S. Yauc," Efficient audit service outsourcing for data integrity in clouds", The Journal of Systems and Software,Elsevier, Dec 2011.

[13] Nancy J. King, V.T. Raja," Protecting the privacy and security of sensitive customer data in the cloud",

computer law & security review, Elsevier, Feb 2012.
[14] Dimitrios Zissis, Dimitrios Lekkas," Addressing cloud computing security issues", Future Generation Computer Systems, Feb 2012.
[15] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo," Secure Data Sharing in the Cloud", Springer Jan 2014.
[16] Said Nabi, M. N. A. Khan," An Analysis of Application Level Security in Service Oriented Architecture", I.J. Modern Education and Computer Science, Feb 2014.
[17] Muhammad Fahad Khan, Mirza Ahsan Ullah, Aziz-ur-Rehman," An Approach Towards Customized Multi-Tenancy", I.J.Modern Education and Computer Science, Sep 2012.
[18] Ashraf Zia, M.N.A. Khan," A Scheme to Reduce Response Time in Cloud Computing Environment" I.J.Modern Education and Computer Science, July 2013.

Authors' Profiles

Mr. Sathiya Moorthy Srinivasan has degree MCA, M.Phil in computer Science (Data Mining), working in Oracle Solutions Services India Pvt., Ltd., as senior software engineer. And working in an oracle product like ERP, Retail products. Interested in Data migration concepts and cloud system. Having 8 years of software consulting experience and working on various data migration projects and implementations on Oracle ERP System.

Dr. Chandrasekar C is an Assistant professor in computer applications department at Periyar University, Salem. In teaching he has been focusing on networking and cloud concepts. Dr. Chandrasekar received his Ph.D in computer science (Network Technologies).