DOI: 10.21917/ijsc.2016.0194

PREVENTIVE SIGNATURE MODEL FOR SECURE CLOUD DEPLOYMENT THROUGH FUZZY DATA ARRAY COMPUTATION

R. Poorvadevi[1] and S. Rajalakshmi[2]
Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, India
E-mail: [1]poorvadevi@gmail.com, [2]srajalakshmi@kanchiuniv.ac.in

Abstract

Cloud computing is a resource pool which offers boundless services by the form of resources to its end users whoever heavily depends on cloud service providers. Cloud is providing the service access across the geographic locations in an efficient way. However it is offering numerous services, client end system is not having adequate methods, security policies and other protocols for using the cloud customer secret level transactions and other privacy related information. So, this proposed model brings the solution for securing the cloud user confidential data, Application deployment and also identifying the genuineness of the user by applying the scheme which is referred as fuzzy data array computation. Fuzzy data array computation provides an effective system is called signature retrieval and evaluation system through which customer's data can be safeguarded along with their application. This signature system can be implemented on the cloud environment using the cloud sim 3.0 simulator tools. It facilitates the security operation over the data centre and cloud vendor locations in an effective manner.

Keywords:

Cloud Vendor, Fuzzy Data Array, Cloud Server, Data Centre, Cloud Service Provider, Cloudsim, Signature Evaluator

1. INTRODUCTION

Cloud computing presently focuses on, a new approach to enhance the modern consumption and delivery model for IT services based on the internet. The major problems which is facing by the customer is, losing control over their confidential data. Even though, many security mechanisms and frameworks are deriving from distinguished developers still, there is a lack of consumer trust in cloud service providers. Many approaches cloud service providers are attempted to overcome the data safety problem due to compliance across the geographic boundaries. So, as an end user perception emphasizing the data protection is most important with the privacy control.

Cloud security is, the security principles applied to protect data, applications and infrastructure. Cloud security is, the security principles applied to protect data, applications and infrastructure associated within the cloud computing technology. Rising the joint venture between cloud service providers and security solution providers are mostly expected. Growing the emergence of cloud services are specifically focused on the security content solution providers. One of the major components in cloud security service is identity and Access management principles that can be used as an authenticity validation or recognition system.

1.1 IMPORTANCE OF CLOUD SECURITY

- Increasing the performance in the client level security system.
- Resolve the problem of vendor lock in.
- Monitoring and managing the huge resources across data centers.
- Improving the effective level of service access among the cloud vendors.

1.2 CHALLENGES OF DATA SAFETY

If people are discussing about cloud security that moment everyone knows that security is an end-user problem or issue. As a customer or cloud clients focal point security is lacking in the customer end only while using the resources from cloud. The major four distinguished challenges are given below:

- Focus on client level security issue
- Lack of awareness about cloud security
- Hardware and software span multiple trust domains
- Dynamism and fluidity of data
- Multi-tenancy services
- Inconsistent network connection issues
- Lack of proper cloud security standards

2. RELATED WORK

In traditional types, consumers are performed all their activities through shared, distributed approaches. There was a trade-off control between scalability and granularity components. Other approach is scalable and secure key updating mechanism for access hierarchies and attribute based signature scheme, it is described about the authentication process and its outcome sets through attribute dependency values. Another technique is, authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine- grained updates, this approach deals with the storage as a service as a big data storage phenomenon for proving the authorization of public auditing scheme[1]. Preventing anomaly based intrusion detection systems can also be applied for security solution [2]. Another approach is a secure cloud computing based framework for big data information management of smart grid. It was defined and developed a framework model designed for evaluating the huge data content management for smart grid services [3].

Multi-level privacy preserving cooperative authentication system in distributed environment, it was used for implementing the health care system activity [4]. Confidentiality preserving, *k*-nearest neighbour query model over encrypted data in cloud environment to secure the confidential content those are computed in cloud forums.[5,6]. Distinguished solutions are derived to migrate the virtual machines in a secured manner [7].

3. PROPOSED WORK

The proposed work will explicitly operate on how to secure the cloud user secret information and also authorizing the genuine users based on their service usage history, type of frequent resource request and so on. This proposed model will be applied into the mechanism of fuzzy data Array computation, cumulatively collecting the user's signature for proving the authenticity of cloud clients. So, we are considering the two major components.

- Signature retrieval
- Signature evaluator

This approach mainly used to ensure the unique features of each customer who belongs to the service in cloud platforms.

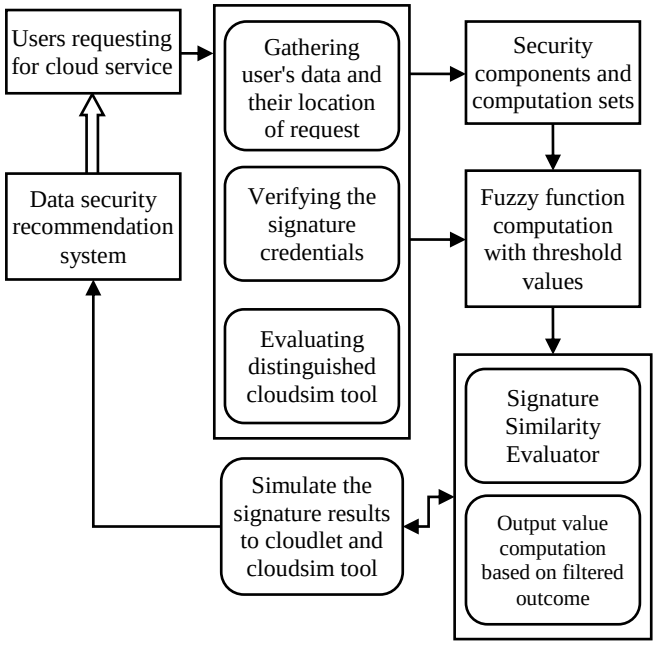

Fig.1. System Architecture

In system framework, shown in Fig.1 all the components are depicted as an activity or process. For finding an authentication process people are making uses of several methods like security key management, content hiding, text transfer via secured medium, encrypted data access control, secret key exchanges. Even customers are depending on the above services to apply for securing their own data still, lack of control over the customers end. The proposed work depicted in the system architecture to activate the several factors which proves the identity of users who is using the cloud service. Number of security factors and attribute sets are collected, identified and applied into the new framework.

3.1 IMPORTANCE OF FUZZY DATA ARRAY COMPUTATION

Fuzzy logic and techniques are approximate reasoning values based on the certainty principals. In this work, people are incorporating the signature or attribute packages into the fuzzy computation block to evaluate the content security.

Some approaches are considered in fuzzy computation as given below:

- Fuzzy rank ordering
- Fuzzy Lambda cut reasoning
- Fuzzy approximation
- Fuzzy elementary segments

Computation formula must be applied for signature identification system to evaluate the authorization outcome for consumers.

Total outcome = (*Service Utilization* + *Data center response* + *threshold value*) / *Efficiency* (%)

Fuzzy tools might be used to perform simulating the sample data set values along with the signature evaluator system.

3.2 PROCESS OF SIGNATURE RETRIEVAL SYSTEM

The process behind in this concept is validating the user authenticity based on the fuzzy data array computation element which can perhaps the various controlled elements during the verification process. The Fig.2 depicts the operation which is performed in signature recognition and comparison area.

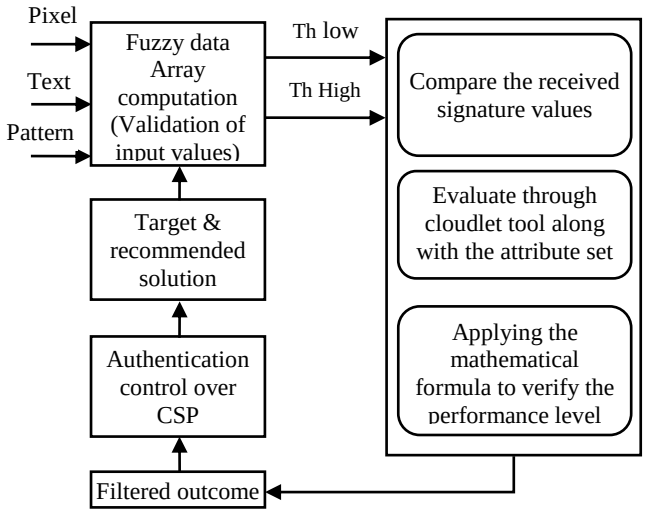

Fig.2. Depicting the process of signature retrieval modeling

The distinguished elements are configured into the various processing block and evolving the authenticity feature for the various users. The following levels can be applied into the proposed model and to evaluate the security performance, Efficiency and probability values. Let consider the following attributes which is used in this approach.

- Signature (Attributes collection)
- Signature Identifier and comparer
- Attribute set
  1.Pixel
  2.Text
  3.Audio / Video pattern
- Fuzzy data array computation
- Manipulation of user feature values
- Compare with the threshold values
  1.Th_{low}

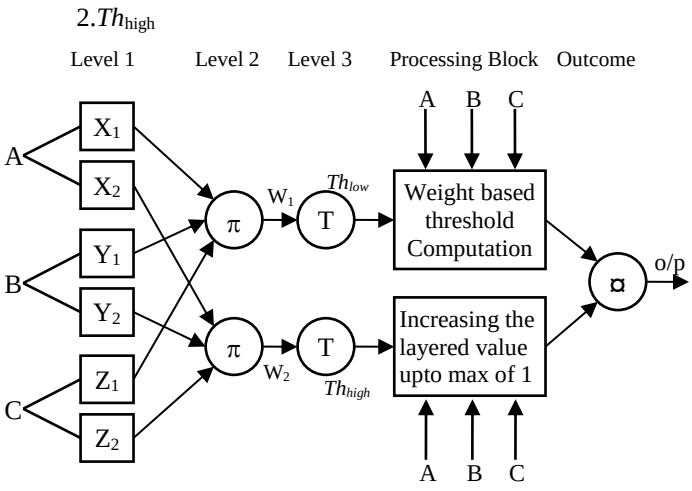

Fig.3. Manipulation of I/O process

In Fig.3 process, user is trying to achieve the authenticity outcome based on the level or layer approach.

In this Notations,

A - Pixel based input value

B - Text input value

C - Audio / Video pattern value

X_1, Y_1 – Attribute collection for pixel images.

Y_1, Y_2 – Attribute / Signature collection for Text frames.

Z_1, Z_2 – Audio track/ video play frames.

Th_{low} = less than 0.5 [Th = < 0.5]

Th_{high} = between 0.5 to 1 [Th > 0.5 < 1]

At finally, security solution can be obtained from the processing block. It is used to satisfy the user credentials and showing the similarity of images with cloud database.

3.3 PROCESS OF SIGNATURE EVALUATION SYSTEM

The concept of signature evaluation process is to determine the cloud users before they are getting the service from cloud provider. Service consumption is one part but, the major focus is how far customer's data are safe in a competitive environment.

So, for distinct set of cases number of research works is going about the protection data security and privacy and, which type of authentication service is suitable for distinguished cloud user services. This concept is elaborately explaining the similarity, features, applications of cloud clients attributes.

Threshold (T) = 0 to 1, // Threshold limit //

Marginally, setting the moderate authenticity value is 0.5, for the mid-range users. The following flowchart is used to describe the constraints based fuzzy data sets value. It has to be processed in the CSP location.

In flowchart in Fig.4 is configuring the various processes which are happening for user identification process. This can enables the computation through algorithmic principles and attribute selector and finder outcomes are passed to signature list or set.

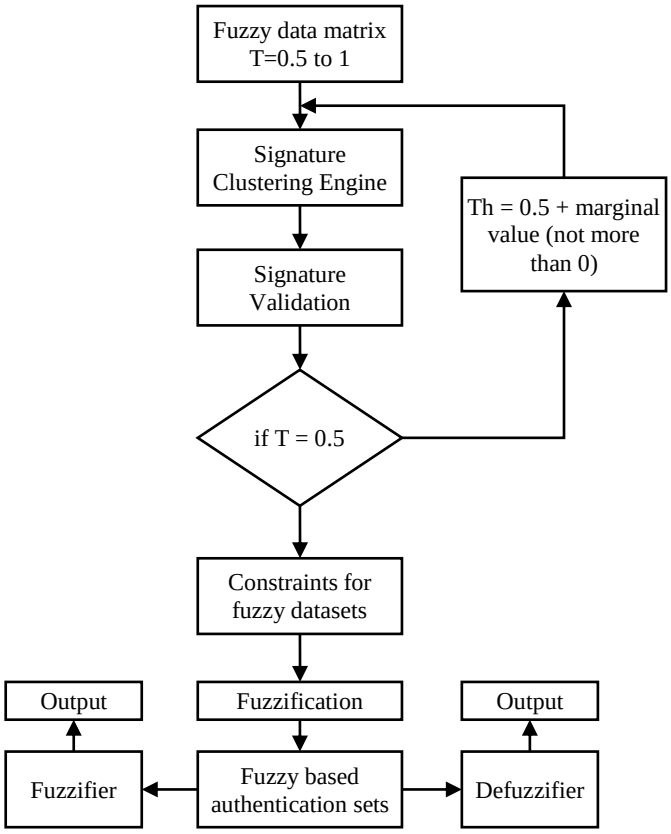

Fig.4. Flow chart for user attribute (signature) determining approach

3.4 COMPUTATIONAL STEPS USED

To regulate the process of secure cloud application deployment on the cloud platform, it is essential to propose a system, technology or an algorithm to implement the process. In this proposed work, the following computational steps are followed to prevent the cloud user confidential information and securing their application over the cloud vendors.

Step 1: Initial Threshold (T) =0;

Step 2: $X^r = X_S(K)$; // X_1, X_2 describes image data set

Step 3: $Y^r = Y^s(K)$; // Y_1, Y_2 describes Text data set

Step 4: $Z^r = Z^s(K)$; // Z_1, Z_2 describes pattern set

Step 5: While ($T > Th_{low}$) {

Step 6: While ($I < M/4$); // M-Marginal Value {

Step 7: $(X^d, Y^d) = (X^r, Y^r) + \Delta g\ (I+(K\text{-}1)M)/4$

Step 8: Attribute values = $convolve(X^d, Y^d)$;

Step 9: O/P for pixel, text, pattern (audio/video) values;

Step 10: While ($T < Th_{high}$) {

Step 11: $X^r = X^r + \Delta X(K)$;

Step 12: $I=I+1$;}

Step 13: $X_r = X_s$;

Step 14: $Y^r = Y^r + \Delta Y(k)$;

Step 15: $Z^r = (1\text{-}Z^r) + Th_{high}$;}

An algorithm is used to describe how to prevent the cloud user by using the signature based model system. Initially, the threshold set it as zero, and there are three major inputs are used

that is, image, text, pattern / Audio data set. These input values are validated by using the Th probability value. This value can be compared with the marginal set value. Finally, the decision is to be made based on the high, low or marginal threshold outcome. From this approach the security performance can be increased.

4. SIMULATION WORK

In order to compute the authenticity process the cloud secure application deployment need to be processed based on some sort of user attributes or property sets into the cloud simulator tool. The various set of cloud user input credentials are combined and pass into the cloud security system to make a suitable decision which related to the user service type, service request location and other service based transaction history.

Depends on these parametric values are implicated in the fuzzy system to find the certainty or uncertainty values. There are numerous cloud simulators available for processing the customer applications such as listed below:

Availability of different cloud tools:

- Workflow sim
- Simple workflow sim
- Dynamic work flow sim
- Cloud auction
- Cloud MIG xpress
- Cloud analyst
- Cloud let

There are three major types of security is available such as,

- Informational security
- Physical security
- Operational security

Parameters settings of simulations

Cloud sim 3.0.3 tar.gz - Bug fix release simulator tool name and before moving onto the simulation environment the possible factor considerations are listed below:

- Input fuzzy array approximation size
- Lines of code for computation (LOC)
- Input (or) source parameters list and unit samples.
- Fuzzy bi- signature clusters detector
- Bit size and string length
- Signature evaluation results set

For simulation work, java (JVM- sector) JDK 1.6.0 version was used with the latest version of cloud sim 3.0 tools along with its architectural components and all the input factors are applied into eclipse environment with jar file sequence, tar file locator.

To implement the cloud security offering services people may consider the different action flow and workflow in cloud environment service portals. It wills also perhaps the various functions to enable the feature of data security and user authentication component in cloud environment.

The Fig.5 depicts the operational performance of cloud security process. This approach is implemented in the cloud simulator platform to achieve the better authenticity provenance outcome.

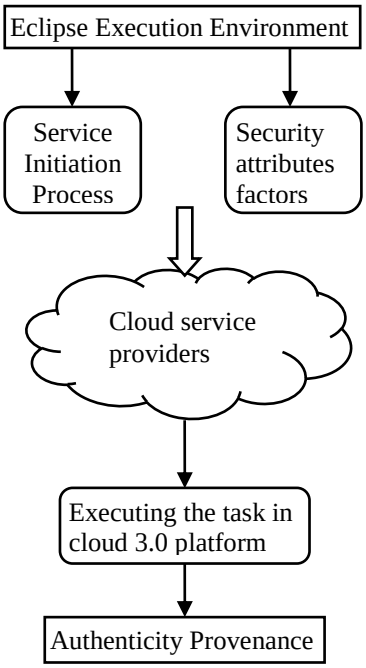

Fig.5. Illustrating Simulation Environment process

5. RESULTS AND DISCUSSIONS

The various activities are shown to prove the unique features of distinguished cloud users in the cloud platform; moreover all the applications are deployed into the cloud forum for getting the unlimited service access from the cloud providers.

Table.1. Signature retrieval process outcome

Type of cloud service	Signature Retrieval Sequence	Signature Evaluation Efficiency (%)	Fuzzy Data Array Value for Th_{low} and Th_{high}	
			Th_{low}	Th_{high}
Communication service	SEQ= 1.98	67.43	2.61	0.51
Security service	SEQ= 5.05	90.23	0.03	1.0
Platform service	SEQ=-3.21	54.23	0.132	0.67
Data service	SEQ=1.92	60.14	0.1	0.78
Network service	SEQ= 2.02	77.09	0.452	0.92
Storage service	SEQ= 2.08	73.20	0.120	0.56

5.1 SIMULATION PROCESS VALIDATION

Simulated results are obtained by using the cloud sim3.0 tool and service inhibition. Security is the one which may directs into different task computation to protect our customers data. It is also used to increase the customers interest to do more applications and task relevant application, enhancing the control the over the cloud service providers to prove the process information containers in a secured environment.

The Table.1 illustrates the approaches of signature identification and retrieval mechanisms through the two different values of low level and high level threshold ranges.

From the computed results in Table.2, the estimates results shows that, how the security services are reliable in customers end depends on the huge consideration of security based attributes.

Table.2. Computed Values of Authenticity Provenance

Cloud Let Tool Outcome	Fuzzy Bi-clusters Value	Authenticity Provenance Value
IAO = 1.1	FBC = Accept state value	APV = Full secured
IAO =0.7 to 0.91	FBC = Wait for another instance	APV= rise the attribute components into the next level
IAO = 0.41 >0.32	FBC = Idle state	APV=None process
IAO = 0.326	FBC = intermediate process response	APV= Process segregation

6. EXPERIMENTAL RESULT SET

Cloud is a connectivity portal between the cloud service providers and end users. So, this approach is mainly focused on increasing the data security performance for customer service resides on data center or virtual machine. This could be the phenomenon that is to be applied in a cloud environment for securing all the applications in cloud environment. The following results were obtained during the security analysis process in a simulated approach. The Fig.6 will explicitly specifies the distinct attribute threshold values for proving the cloud user authentication by considering the three different inputs such as pixel, text and pattern values. The result graph comparison – 1 will shows the high result value in the signature proving process.

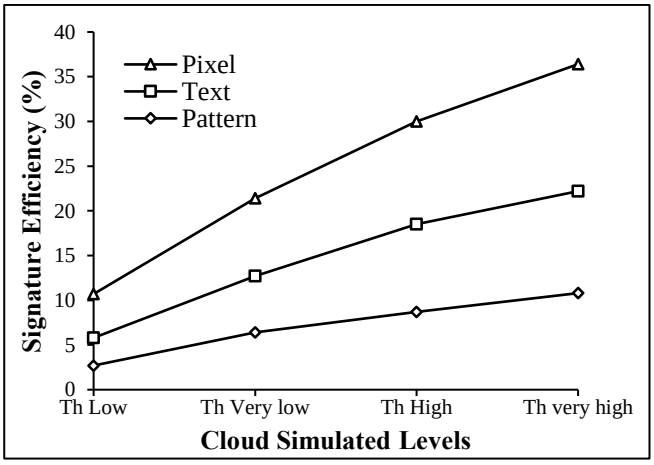

Fig.6. Attribute Threshold ranges based Graph Comparison-1

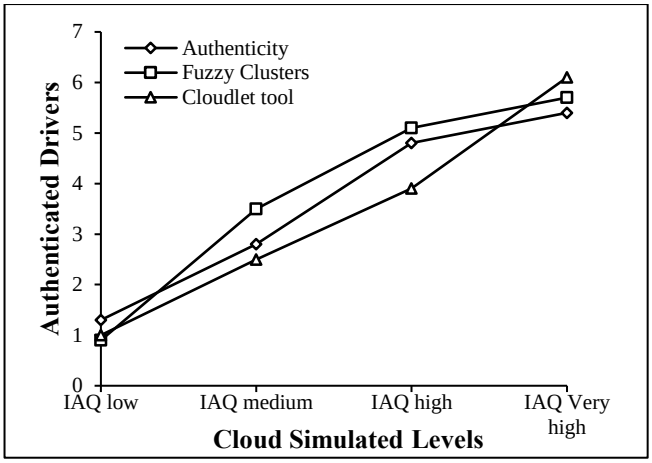

Fig.7. Cloud Authenticity Result based Graph Comparison-2

In Fig.7, the graphical results are obtained during the time of simulation. Finally, the obtained security efficient rate is, 90.23% in order to increase the security performance for huge cloud users.

7. CONCLUSION

From the implementation approach, users want to safe their confidential data, from the warms or distinguished hackers. People can apply efficient method to secure the secret information's in the cloud environment. This proposed model helps to, whoever consuming the cloud services, those can keep the data in a safe manner. Signature recognition is the traditional approach, but how can we perform the task of data safety to produce the authenticated output. Fuzzy data array computation is well suitable for finding the different forms of user signature to produce the authenticity of users to avoid the fearness in cloud area.

8. FUTURE ENHANCEMENT

In future cases, signature adaptation trend can be enhanced one. So, that user can apply their own security measurements by using the fuzzy modelling approaches from the hackers to protect the data.

REFERENCES

[1] Tram Truong-Huu and Chen-Khong Tham, "A Novel Model for Competition and Cooperation among Cloud Providers", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 251-265, 2014.

[2] Alain Tchana, et al., "A Self-Scalable and Auto Regulated request Injection Benchmarking Tool for Automatic Saturation Detection", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 279-291, 2014.

[3] Luis Tomas and Johan Tordsson, "An Automatic Approach to Risk-Aware Data Center Overbooking", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 292-305, 2014.

[4] Yang Wang and Wei Shi, "Budget-Driven Scheduling Algorithms for batches of Map Reduce Jobs in

Heterogeneous Clouds", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 306-319, 2014.

[5] Bei Guan, Yanjun Wu, Liping Ding and Yongji Wang, "CIV Scheduled Communication-Aware Inter-VM Scheduling Technique for Decreased Network Latency between Co-Located VM's", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, 2014

[6] Shanjiang Tang, Bu-Sung Lee and Bingsheng He; "Dynamic MR: A Dynamic Slot Allocation Optimization Framework for Map Reduce Clusters", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 333-347, 2014.

[7] B. Poornima and T. Rajendran, "Improving Cloud Security by Enhanced Hasbe using Hybrid Encryption Scheme", *Proceedings of World Congress on Computing and Communication Technologies*, pp. 312-314, 2014.

[8] Chang Liu, Jinjun Chen, Laurence T. Yang, Xuyun Zhang, Chi Yang, Rajiv Ranjan and Ramamohanarao Kotagiri, "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates Parallel and Distributed Systems", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 9, pp. 2234-2244, 2014.