Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# DESINING BIMATRIX GAME THOERY BASED NASH EQUILIBRIUM FOR INFORMATION SECURITY BASED ON RISK ANALYSIS IN CLOUD

**[1]V.VISWANATHAN, [2]Dr.S.P.SHANTHARAJAH, [3]Dr.P.NAVANEETHAM**

[1]Research Scholar, Department of Computer Science, Bharathiyar University, Tamilnadu, India

[2]Professor, Dept. of Computer Applications, Sona College of Technology, Salem, Tamilnadu, India.

[3] Professor, Department of Computer Applications, Velalar College of Engineering and Technology, Erode, Tamilnadu India.

E-mail: [1]viswanathan73@gmail.com, [2]spshantharaj@gmail.com, [3]pn_tham@yahoo.com

**ABSTRACT**

With the mushroom growth of Cloud Service Providers (CSPs) offering services of similar functionality, makes a challenge for cloud users to choose an appropriate service provider from cloud marketplace. This unique paradigm brings about new risk related issues in Cloud Computing (CC) environment. This is because it is indispensable from a customer's aspect to establish trust with a CSP with high risk of outsourced data to be misused. Though trustworthiness and competence to estimate risk of interaction and risk for customer's privacy were addressed in many research works, the way through which the risk of outsourced data/ file can be minimized in the presence of malicious service providers pose challenging issues. The challenging issue of handling risk in cloud environment is addressed in this work through Risk Evaluation using Nash Equilibrium-based Bi-Matrix Decision (RE-NEBMD) model. RE-NEBMD model studies the problem of ensuring security where the possible risk of outsourced data is brought to an absolute minimum in Cloud Computing in the presence of malicious CSPs. Nash Equilibrium-based Trust Evaluation model performs trust evaluation model on CSPs for outsourced data based on strategy and utility function. Next, risk evaluation is measured using Bi-Matrix Decision model on the evaluated trust and risk is measured accordingly. Extensive analytical and experimental results are presented which show minimized cost during risk analysis, computation overhead and improving true positive rate or detected threats of our proposed model.

**Keywords:** *Cloud Service Providers, Cloud Computing, Nash Equilibrium, Bi-Matrix, Decision Model.*

## 1. INTRODUCTION

Cloud computing facilitates better resource utilization by multiplexing the same physical resource among different cloud service providers. With different cloud service providers offering resources, it becomes tedious task for the cloud customer to decide upon CSP during data outsourcing.

A framework to facilitate selection of cloud service provider [1] through trustworthiness and estimating risk of interaction ensuring security was introduced. For example time series pattern for privacy protection on cloud using noise obfuscation was provided in [2]. However, auditability and storage security was much concerned which was addressed in [3] by allowing a third party auditor to verify data integrity on dynamic data stored in cloud. Outsourcing computations has received greater attention with the advent of cloud computing. In [4], a unifying trust framework was designed based on subkeys ensuring a secure solution. Another method to solve data integrity issues in cloud computing environment was addressed in [5] by applying an auditing process performed through third party auditor for multiple users simultaneously and efficiently.

In recent years, personal health record (PHR) has come up as a patient-centric methodology of health information exchange. In [6], an attribute-based encryption technique was introduced to enable dynamic modification of access policies ensuring security and scalability. To ensure cost effectiveness during privacy preserving, it is highly required to decide upon the factors like which dataset to be encrypted and which not. In [7], a privacy leakage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

upper bound constraint model was introduced to reduce the privacy preservation cost. A new insight into hybrid cloud model was introduced in [8]. A cloud computing architecture that analyzes the occupational risk involved was analyzed in [9].

In this paper, we propose a novel model to identify the trustworthiness of cloud service provider in order to design a risk analysis model in cloud computing environment. A trust evaluation model based on Nash Equilibrium is modeled with the aid of cloud security labs to analyze the trustworthiness of cloud service provider. As quantifying strategy and utility function of cloud service providers efficiently is challenging, we exploit a Nash Equilibrium-based Trust Evaluation algorithm to confine computation overhead. Based on such a constraint, we model the problem of minimizing the cost involved during risk analysis by introducing a Bi-Matrix decision model. Finally, we arrive at the risk and impact to identify and measure the risk involved during data outsourcing. Experimental results demonstrate that computation overhead and cost involved during risk analysis can be significantly reduced with our model over existing ones.

The rest of the paper is organized as follows. Section 2 presents a brief literature survey on other trust models used in cloud computing environment. Section 3 gives brief description to proposed RE-NEBMD model and its different modules. Validation and analysis of results based on experimental settings by our model have been done in Section 4. Finally, a conclusion is drawn in Section 5.

## 2. RELATED WORKS

Recently, much of growing interest has been pursued in the context of security and risk in cloud environment. Empirical analysis of cloud data center was presented in [10] using HBase and Cassandra to reduce the risk of data loss. Risk and safety of outsourced data was analyzed in [11] for complex network systems. From the view point of industrial security, sensor based system for computing and communication was presented in [12] for providing data sharing.

A fundamental step for the success in health care revolves around in in-depth understanding and the ensuring security and privacy in cloud computing environment. In [13], a security model with respect to health sector in cloud computing environment was presented in order to ensure information security process. A cloud computing adoption decision tool was designed in [14] to gather required information and provide user with valuable information to ensure security.

As already mentioned above the feature of the cloud computing environment make the business environment to immigrate to the cloud computing environment. However, the risk and security related cannot be overlooked. In [15], risk assessment methods were analyzed. Data coloring and software watermarking techniques was introduced in [16] provided means for multi-way authentication to the cloud users. With the objective of improving the performance of audit services, a method based on probabilistic query and periodic verification was introduced in [17]. In [18] multi attribute trustworthiness model for cloud service evaluation was presented using a novel service selection approach.

Linked to this, a mobile cloud computing survey was presented in [19] states that while the researchers and practitioners in the computer science community are making rapid strides in realizing cloud computing advantages in technological terms, an equally important discussion need to start from a business perspective with the risk associated. Thus, our research aims at contributing risk analysis in that perspective and, accordingly, the proposed model which is described in the next section follows this risk analysis model, based on the trust evaluation of cloud service provider through its main strategies of competitive improvement, via strategy and utility function.

## 3. RISK EVALUATION USING NASH EQUILIBRIUM-BASED BI-MATRIX DECISION

In this section, we describe our novel risk analysis model based on a security designed for cloud-based information security systems using trust evaluation and risk estimation. The main goal of our work is to design a risk analysis model in the presence of malicious cloud service providers. The key idea is to divide the model into cloud customer entity, cloud service provider entity and cloud security lab entity according to different cloud customer requirements. Figure 1 shows a three step process to perform risk analysis. They are (i) registering of cloud customer, cloud service provider and cloud security lab component in their corresponding registry, (ii) a trust evaluation model and (iii) risk evaluation model.

### 3.1 Security Model

In this work we consider the cloud service providers to be semi honest with the cloud customer having a risk of their outsourced data to be placed in the cloud service providers. As they are semi honest, the outsourced data of the cloud consumer is said to

Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

be at risk. The problem is defined as follows. Given cloud customers '$CC_i = CC_1, CC_2, \ldots, CC_n$' and cloud service providers '$CSP_i = CSP_1, CSP_2, \ldots, CSP_n$', the goal is to include a cloud security lab '$CSL$' that evaluates the trustworthiness of cloud service providers and measures the risk involved during data outsourcing on behalf of the cloud customer.

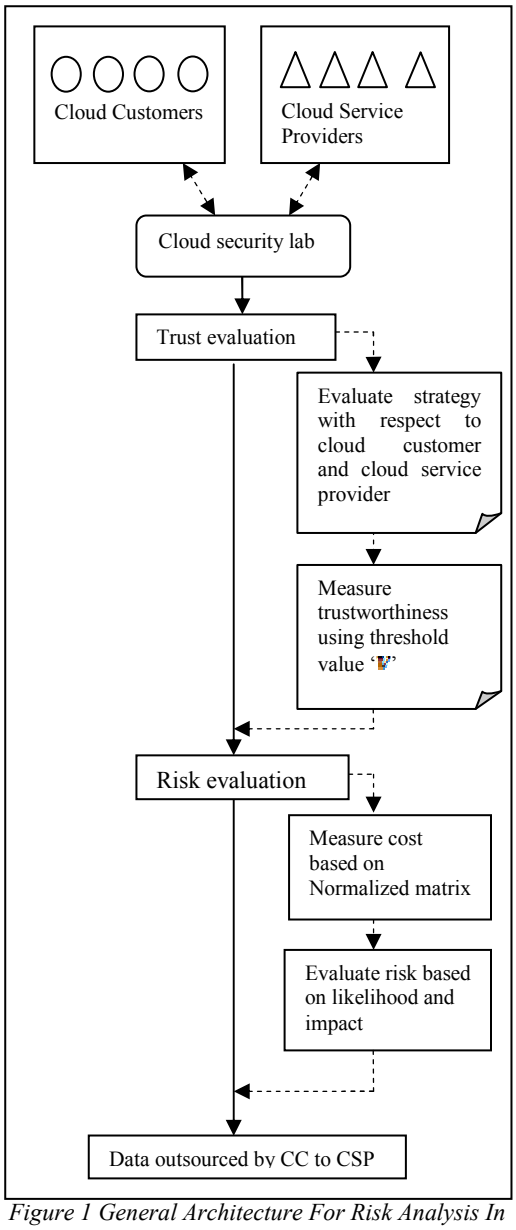


*Figure 1 General Architecture For Risk Analysis In Cloud Environment*

As shown in the figure, when a cloud customer has to outsource their data, there involves a possibility of risk. So in the proposed RE-NEBMD model, before sending the data, the cloud customer evaluates the trustworthiness of each cloud service provider using strategy and threshold value '$V$'. Next, the RE-NEBMD model performs risk analysis by measuring likelihood and impact through normalized matrix. The detailed explanation of RE-NEBMD model is described below.

### 3.2 Nash Equilibrium-based Trust Evaluation Model

Delegating data control to CSPs, invariantly results in the increase in the risk of data/file being compromised during data outsourcing as the data becomes highly accessible to an augmented number of parties. The proposed work constructs a trust evaluation model that minimizes the risk of outsourced data with the aid of three entities namely, Cloud Customer (CC), Cloud Service Provider (CSP) and Cloud Security Labs (CSL). The inclusion of the CSL provides higher rate of integrity to risk analysis making the results more homogenous for the CC. Figure 1 shows the relationship between three entities CC, CSP and CSL, a risk analysis model. Initially each entities register with their corresponding components.

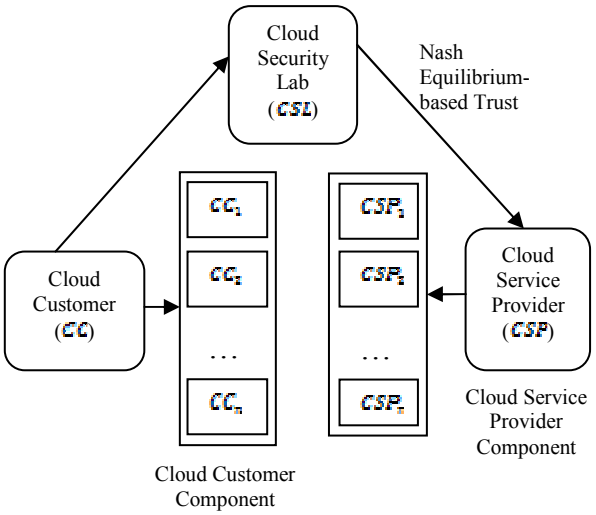


*Figure 2 Relationships between CC, CSP and CSL*

As shown in the figure, the cloud customers are registered with their cloud customer component and cloud service providers are registered with their cloud service provider component. The Cloud Security Labs (CSL) is an entity to ensure information security. On the other hand, the Cloud Customer (i.e. CC) is an entity that provides information in the cloud environment. Finally, the Cloud Service Provider (CSP) is an entity that provides services as requested by the CC. The proposed work with the aid of three entities uses a Bi-Matrix Game Theory model with the objective of performing a game between the CC and CSP through Bi-Matrix form. The Bi-Matrix Game Theory model in turn achieves security level agreement between the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CC and CSP by applying Nash Equilibrium algorithm, minimizing the risk of outsourced data in cloud environment.

Let us consider '$(S,F)$' with '$n$' cloud customers '$CC_i = CC_1, CC_2, \ldots, CC_n$', set of cloud service providers available to cloud customer be '$CSP_i = CSP_1, CSP_2, \ldots, CSP_n$' where '$S_j$'represents the strategy for cloud customer '$CC_j$'. Furthermore, '$S_{CC} = S_1, S_2, \ldots, S_n$' represents the strategy for cloud customers whereas '$S_{CSP} = S_1, S_2, \ldots, S_n$' represents the strategy for cloud service providers which belong to the strategy '$S$' and is formulated using Cloud Service Lab and is as given below.

$$CSL \rightarrow S_{CC}, S_{CSP} \in S \quad (1)$$

On the other hand the utility function is represented as '$u$' with '$u_{CC}$' as utility function for cloud customer and '$u_{CSP}$' as utility function for cloud service provider respectively and is formulated as given below. The utility function is obtained by the Cloud Security Labs (CSL) and is formulated as given below.

$$CSL \rightarrow u_{CC}, u_{CSP} \in F \quad (2)$$

From (1) and (2), with the arrived strategy and utility function for each cloud customer and clouds service provider, a service level between the cloud customer and clouds service provided is arrived at. A threshold value '$V$' is taken as the base to measure the trustworthiness of the cloud service provider over others. Let us further assume that the values used to measure the trust are ''.

$V = 1, very\ high, V = 0.5, medium, V = 0.25, low$ The mathematical function derived using the trust value is as given below

$$\forall i \in n, CSL = S : S_{CC}(CSP_1, CSP_2, \ldots, CSP_n) = v_i \quad (3)$$

$$\forall i \in n, CSL \neq S : S_{CC}(CSP_1, CSP_2, \ldots, CSP_n) \leq v_i \quad (4)$$

$$\forall i \in n, CSL \neq S : S_{CC}(CSP_1, CSP_2, \ldots, CSP_n) \leq v_i \quad (5)$$

Based on the resultant obtained through (3), (4) or (5), the trustworthiness of cloud service provider is obtained through which risk analysis is measured. Followed by this efficient data outsourcing is performed in a secure manner between the CC and CSP. Thus, a game between a cloud customer and a cloud service provider makes the proposed model achieve Nash equilibrium with measures on the basis of the threshold value in cloud environment. Figure 3 shows the algorithm for Nash Equilibrium-based Trust Evaluation.

| |
|---|
| Input: Cloud Customers '$CC_i = CC_1, CC_2, \ldots, CC_n$', Cloud Service Provider '$CSP_i = CSP_1, CSP_2, \ldots, CSP_n$', Cloud Service Lab '$CSL$', Cloud Customer strategy '$S_{CC}$', Cloud Service Provider strategy '$S_{CSP}$', Utility function '$f()$', Threshold Value '$V = v_1, v_2, \ldots, v_n$', set '$B(CSP_i), DB(CSP_i), UC(CSP_i)$ to be 0' |
| Output: minimized computation overhead |
| 1: Begin<br>2: For each Cloud Customers '$CC_i$'<br>3:Obtain strategy (by $CSL$) for cloud customer and cloud service provider using (1)<br>4:Obtain utility function (by $CSL$) for cloud customer and cloud service provider using (2)<br>5: If $S_{CC}(CSP_1, CSP_2, \ldots, CSP_n) = v_i$then<br>6: Belief over entity '$CSP_i$'<br>7: $B(CSP_i) \rightarrow B(CSP_i) + 1$<br>8: End if<br>9: If $S_{CC}(CSP_1, CSP_2, \ldots, CSP_n) \leq v_i$ then<br>10:Disbelief over entity '$CSP_i$'<br>11: $DB(CSP_i) \rightarrow DB(CSP_i) + 1$<br>12:End if<br>13:If $S_{CC}(CSP_1, CSP_2, \ldots, CSP_n) = 1$ then<br>14:Uncertainty over entity '$CSP_i$'<br>15: $UC(CSP_i) \rightarrow UC(CSP_i) + 1$<br>16: End if<br>17: End for<br>18: End |

*Figure 3 Nash Equilibrium-based Trust Evaluation algorithm*

As shown in the figure, for each cloud customer, the Nash Equilibrium-based Trust Evaluation algorithm evaluates the trustworthiness of the cloud service providers using strategy and utility function. Based on these obtained values, belief, disbelief and uncertainty of cloud service provider are measured to evaluate trustworthiness. Once the trustworthiness is measured, risk analysis during data outsourcing is performed which is discussed in the following section.

Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

### 3.3 Risk Evaluation using Bi-Matrix Decision Model

Based on the trust values obtained using Nash Equilibrium-based Trust Evaluation algorithm, the next step is to design Bi-Matrix Decision model to measure risk analysis. Bi-Matrix Decision model helps us to achieve a secured risk minimized agreement between the cloud customer and the cloud service provider through Nash equilibrium.

In the proposed method using Bi-Matrix Decision model while a cloud customer's perception forms one dimension, cloud service provider forms another dimension and the two significantly inspire integrity towards estimation of trust. Since, the Bi-Matrix Decision model is formed with mixed strategies, equal chance of both cloud customer and the cloud service provider is entitled through proper trust management activity.

Let '$A = CC_1, CC_2, \ldots, CC_n$' be the set of all '$n$' feasible alternatives or cloud consumers, let '$B = CSP_1, CSP_2, \ldots, CSP_n$' be the set of all '$n$' feasible attributes or cloud service providers and let '$CSL$' be the decision makers. Assume that '$w = w_1, w_2, \ldots, w_n$' represents the attribute weight vector used by the cloud service lab in making the decision or ensures information security during data outsourcing in cloud environment. Let the individual decision matrix given by the cloud service lab be represented in the form of normalized decision matrix. Then, the normalized decision matrix is obtained as follows.

$$Norm_{ij}(CSL) = \begin{cases} \frac{\max(DM_{ij}) - (DM_{ij})}{\max(DM_{ij}) - \min(DM_{ij})}, where\ i = 1,2,\ldots,m\ and\ j = 1,2,\ldots,n \\ \frac{DM_{ij} - \min(DM_{ij})}{\max(DM_{ij}) - \min(DM_{ij})}, where\ i = 1,2,\ldots,m\ and\ j = 1,2,\ldots,n \end{cases} \quad (6)$$

From (6), '$DM_{ij}$' represents the decision matrix and '$Norm_{ij}$' is the normalized matrix used by the cloud user in evaluating the cloud service provider before performing data outsourcing aiming at reducing the cost '$I$' involved during risk analysis. With this the risk of data to be outsourced by the cloud customer with the cloud service provider is reduced significantly. Therefore, the risk based on Bi-Matrix Decision model is measured and is as given below.

$$Risk\ (R) = Likelihood\ (L) * Impact\ (I) \quad (7)$$

Let us assign the values of likelihood for measuring risk as '$Very\ High\ (VH) \rightarrow 0.75 - 1$', '$High\ (H) \rightarrow 0.5 - 0.74$', '$Medium\ (M)$ › 0.25 0.49' and '$Low\ (L) \rightarrow 0 - 0.24$' respectively. The Impact '$I$' is evaluated as shown below.

$$Impact\ (I) = B\ (CSP_i) + DB\ (CSP_i) + U(CSP_i) \quad (8)$$

From (8) the impact is obtained by the summation of belief, disbelief and uncertainty over cloud service provider. Greater the impact, lower the rate of risk and vice versa. Hence, related conclusions can provide a clear picture to support the risk analysis based on the values of likelihood and impact.

## 4. EXPERIMENTAL SETTINGS

We conduct extensive simulation experiments to evaluate Risk Evaluation using Nash Equilibrium-based Bi-Matrix Decision (RE-NEBMD) model and compare its performance with Selection of Cloud Service Providers (SCSP) [1] and Time Series Pattern for Privacy Protection (TSP-PP) [2] in cloud using Cloudsim. Our testbed is a server with two quad core 2.33-2.66 GHz Xeon processors (8 cores total), 7 GB RAM, and 1690 GB local disk storage with Java JRE 7.0 and J2EE 7.0 SDK being installed.

The proposed model uses Amazon, a well-known and widely recognized cloud service provider and simulates the dynamic benchmarking approach on Amazon using on-demand cloud services [21]. For experiments to be conducted using CloudSim and implemented in JAVA, the model uses Standard Small EC2 instance (m1.small) and High CPU EC2 instances (cl.medium and cl. xlarge) to construct cloud computing environment. To measure the efficacy of the proposed model, we evaluated Risk Evaluation using Nash Equilibrium-based Bi-Matrix Decision with the impact of three metrics namely, cost during risk analysis, computation overhead, true positive rate or detected threats, cloud service providers.

The cloud computing environment for RE-NEBMD model identifies the cloud service providers, cloud customers for data sharing. As a result, the data sharing is significantly carried out in cloud computing environment using Nash Equilibrium-based Trust Evaluation algorithm. The performance of RE-NEBMD model is measured with respect to number of cloud users, number of

Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cloud service providers, cost involved during risk analysis, computation overhead and true positive rate.

In the experiment cloud environment, the RE-NEBMD model is evaluated in the process as follows. In Section 4.1, the efficiency of the model is evaluated using the parameters cost, computational overhead and true positive rate. In order to conduct experiments, the algorithm is implemented and run on the m1.small EC2 instance as it is the basic type of EC2 CPU instances and measure the efficiency of computation overhead. In Section 4.2, the benchmarking approach is evaluated on c1.medium EC2 instances to show the practicability of our model in cloud environment. In Section 4.3, the utilization of the benchmarking approach is validated by evaluating the efficiency of workload on cl. xlarge.

### 4.1 Scenario 1: Cost involved during Risk Analysis

In this section we focus on analyzing the cost involved during risk analysis with the state-of-the-art works. The cost involved during risk analysis is the product of time taken to obtain the likelihood levels and the time taken to evaluate the impact for measuring risk. It is formulated as given below.

$$CRA = \sum_{i=1}^{n} [Time\ (L) * CSP_i] + [Time\ (I) * CSP_i] \quad (9)$$

From (9), the cost during risk analysis '$CRA$' is measured using likelihood value for obtaining cloud service provider '$Time\ (L) * CSP_i$' and time to measure the impact of cloud service provider '$Time\ (I) * CSP_i$' respectively. To better understand the effectiveness of the proposed RE-NEBMD model, extensive experimental results are reported in table 1. The RE-NEBMD model is compared against the existing SCSP [1] method and TSP-PP [2]. Cloudsim simulator is used to measure and experiment the factors by analyzing the percentage of result with the help of table and graph values.

*Table 1: Tabulation For Cost During Risk Analysis*

| No. of cloud service providers | Cost involved during risk analysis (ms) | | |
|---|---|---|---|
| | RE-NEBMD | SCSP | TSP-PP |
| 3 | 0.220 | 0.236 | 0.252 |
| 6 | 0.314 | 0.429 | 0.449 |
| 9 | 0.428 | 0.534 | 0.554 |
| 12 | 0.517 | 0.622 | 0.642 |
| 15 | 0.634 | 0.741 | 0.761 |
| 18 | 0.789 | 0.893 | 0.903 |
| 21 | 0.821 | 0.932 | 0.952 |

Results are presented for different number of cloud service providers considering the cost involved during risk analysis in cloud environment. The results reported here confirm that with the increase in the number of cloud service providers, the cost involved during risk analysis also gets increased. Finally, it attains saturation when the number of cloud service providers ranges from 18 – 21.

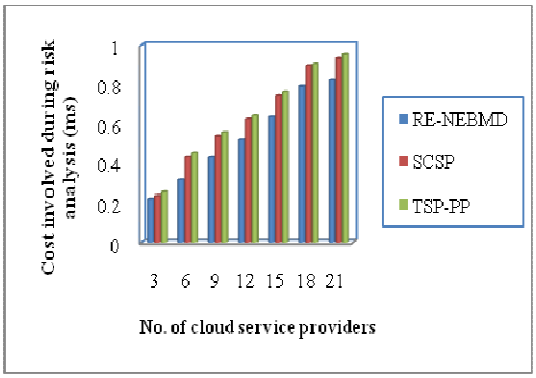


*Figure 4 Measure Of Cost Involved During Risk Analysis*

Figure 4 illustrate the cost involved during risk analysis based on the number of cloud service providers considered for experimental purpose. Our proposed Risk Evaluation using Nash Equilibrium-based Bi-Matrix Decision (RE-NEBMD) model performs relatively well when compared to two other methods SCSP [1] and TSP-PP [2]. This is because using RE-NEBMD model, a Bi-Matrix Decision model is applied using between the cloud customer and the cloud service provider through Nash equilibrium that perform efficient data outsourcing on the cloud environment. This in turn identifies the cloud service providers efficiently for data outsourcing reducing the cost involved by 18 % compared to SCSP. Furthermore, the formulation of assessment value for risk using normalized decision matrix for each cloud customer reduces the cost during risk analysis significantly by 23 % compared to TSP-PP.

### 4.2 Scenario 2: Computation Overhead

The computation overhead or the time taken for deciding the CSP to be trustworthy or untrustworthy is decided based on the parameters, belief '$B(CSP_i$', disbelief '$DB(CSP_i$' and uncertainty '$U(CSP_i)$' involved in measuring the cloud service provider.

$$CO = Time\ B(CSP_i) + Time\ DB(CSP_i) + Time\ U(CSP_i) \quad (10)$$

From (10), the computation overhead is measured in terms of milliseconds (ms). Higher the computation overhead higher is the time taken for

Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

deciding the trustworthiness of a cloud service provider. Therefore, if the time taken is high, obviously, the cloud customer moves to the next provider and soon. As listed in table 2, RE-NEBMD model measures the computation overhead in deciding the CSP to be trustworthy or not on cloud environment which is measured in terms of millisecond (ms). The computational overhead using our model RE-NEBMD model offer comparable consumption values than the state-of-the-art methods.

*Table 2 Tabulation for computation overhead*

| No. of cloud service providers | Computation overhead (ms) | | |
|---|---|---|---|
| | RE-NEBMD | SCSP | TSP-PP |
| 3 | 0.98 | 1.40 | 2.18 |
| 6 | 1.45 | 2.66 | 3.46 |
| 9 | 3.05 | 4.26 | 5.06 |
| 12 | 4.82 | 5.93 | 6.73 |
| 15 | 5.98 | 6.99 | 7.79 |
| 18 | 7.05 | 8.23 | 9.03 |
| 21 | 9.23 | 10.38 | 11.18 |

The targeting results of computation overhead using RE-NEBMD model with two state-of-the-art methods [1], [2] in figure 5 given below is presented for visual comparison based on the number of cloud service providers in cloud environment.

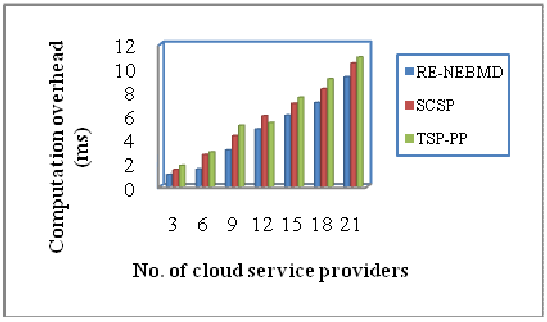


*Figure 5 Measure of computation overhead*

As shown in the figure 5, our method differs from the SCSP [1] and TSP-PP [2] in that we have incorporated Nash Equilibrium Trust Evaluation model by evaluating strategy and utility function. With the application of Nash Equilibrium Trust Evaluation model, a service level between the cloud customer and clouds service provided is arrived at based on the threshold value. With this the computation overhead for measuring the trustworthiness of CSP using the proposed RE-NEBMD model is reduced by 33 % compared to SCSP. In addition, using the mathematical function by the cloud security lab for each cloud customer, based on the threshold value, the computation overhead using the proposed RE-NEBMD model is reduced by 46 % compared to TSP-PP.

### 4.3 Scenario 3: Improving true positive rate or detected threats

True positive rate or threats to be detected is the proportion of positive cases that were correctly identified as calculated using the equation given below.

$$TPR = \frac{Threat_{CI}}{Threat_{CI} + Threat_{ICNT}} \quad (11)$$

From (11), the true positive rate '$TPR$' is the ratio of threat correctly identified as threat '$Threat_{CI}$' to the summation of the threat correctly identified as threat and threat incorrectly identified as not threat '$Threat_{ICNT}$'. In table 3 we show the analysis of true positive rate with respect to number of cloud customers who provided their data to the cloud service provider through cloud service lab ranging.

*Table 3 Tabulation for true positive rate*

| No. of cloud customer | TPR (%) | | |
|---|---|---|---|
| | RE-NEBMD | SCSP | TSP-PP |
| 10 | 85.73 | 76.32 | 65.14 |
| 20 | 89.21 | 80.11 | 69.18 |
| 30 | 91.35 | 84.15 | 75.21 |
| 40 | 87.26 | 81.12 | 72.16 |
| 50 | 90.48 | 84.32 | 75.42 |
| 60 | 88.21 | 82.14 | 73.23 |
| 70 | 93.35 | 87.23 | 78.31 |

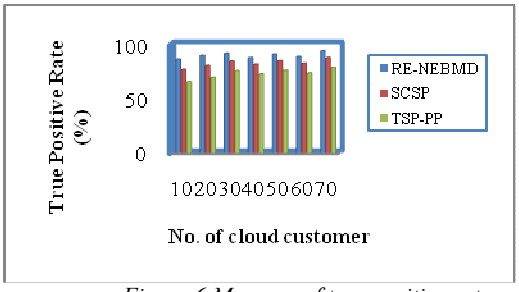


*Figure 6 Measure of true positive rate*

Figure 6 presents the variation of true positive rate of threats being detected using RE-NEBMD model, SCSP and TSP-PP over different number of cloud customers in the cloud environment. All the results provided in figure 6 confirm that the proposed RE-NEBMD model significantly outperforms the other two methods, SCSP [1] and TSP-PP [2]. For example, when 10 cloud customers sent their data, from an actual threat of 8, 8 threats were detected by applying RE-NEBMD model, 7 threats using SCSP and 6 threats using TSP-PP respectively. The better performance of RE-NEBMD model is achieved due to the fact that with the application of Nash Equilibrium-based Trust Evaluation algorithm in RE-NEBMD model, it

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

converges to evaluate trustworthiness in an efficient manner by applying belief, disbelief and uncertainty of cloud service provider separately. This in turn improves the true positive rate by 8 % compared to SCSP and 18 % compared to TSP-PP.

## 5. CONCLUSION

In this paper, we study an instance of the secure risk analysis model in cloud computing environment, where the cloud customer and cloud service providers are mutually distrusting. We employ cloud service lab with trust and risk evaluation model to provide verifiable and risk minimized data outsourcing. We prove the trust evaluation and risk analysis of data being outsourced by constructing Nash Equilibrium-based Trust Evaluation and Bi-Matrix Decision model on the evaluated trust and the risk is analyzed accordingly. We compared the performance with many different system parameters, and evaluated the performance in terms of different metrics. The results show that RE-NEBMD model offers better performance with an improvement of true positive rate of possibly threats being detected by 13 % and reduces the computational overhead by 40 % compared to SCSP and TSP-PP respectively.

## REFRENCES:

[1] Nirnay Ghosh, Soumya K. Ghosh, and Sajal K. Das, "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers", IEEE Transactions on Cloud Computing, Volume 3, Issue 1, January-March 2015, Pages 66-79.

[2] Gaofeng Zhang, Xiao Liu, and Yun Yang, "Time-Series Pattern Based Effective Noise Generation for Privacy Protection on Cloud", IEEE Transactions on Computers, Volume 64, Issue 5, May 2015, Pages 1456-1469.

[3] 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, Volume 22, Issue 5, May 2011, Pages 847-859.

[4] Bogdan Carbunar and Mahesh V. Tripunitara, "Payments for Outsourced Computations", IEEE Transactions on Parallel And Distributed Systems, Volume 23, Issue 2, February 2012, Pages 313-320.

[5] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Volume 62, Issue 2, February 2013, Pages 362-375.

[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, Volume 24, Issue 1, January 2013, Pages 131-143.

[7] Xuyun Zhang, Chang Liu, Surya Nepal, Suraj Pandey, Jinjun Chen, "A Privacy Leakage Upper-bound Constraint based Approach for Cost-effective Privacy Preserving of Intermediate Datasets in Cloud", IEEE Transactions on Parallel and Distributed Systems, Volume 24, Issue 6, January 2013, Pages 1192-1202.

[8] Aishwarya Srinivasana, Abdul Quadir Mdb, Vijayakumar.V, "Era of Cloud Computing: A New Insight To Hybrid Cloud", Elsevier, Procedia Computer Science, Volume 50, 2015, Pages 42–51.

[9] Lucian-Ionel CIOCA, Larisa IVASCU, "IT technology implications analysis on the occupational risk: cloud computing architecture", Elsevier, Procedia Technology, Volume 16, 2014, Pages 1548–1559.

[10] Bao Rong Chang, Hsiu-Fen Tsai, Chia-Yen Chen, and Cin-Long Guo, "Empirical Analysis of High Efficient Remote Cloud Data Center Backup Using HBase and Cassandra", Hindawi Publishing Corporation, Scientific Programming, Volume 2015, December 2014, Pages 1-11.

[11] Xiao-Bing Hu, Adrian V. Gheorghe, Mark S. Leeson, Supeng Leng,Julien Bourgeois, and XiaoboQu, "Risk and Safety of Complex Network Systems", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2016, December 2015, Pages 1-4.

[12] Chang Jin Koo and JeongYeon Kim, "Decision Making for the Adoption of Cloud Computing for Sensor Data: From the Viewpoint of Industrial Security", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2015, December 2014, Pages 1-6.

[13] Knut Haufe, Srdan Dzombeta, and Knud Brandis, "Proposal for a Security Management in Cloud Computing for Health Care", Hindawi Publishing Corporation, The Scientific World Journal, Volume 2014, February 2014, Pages 1-8.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14] Iñaki Bildosola, Rosa Río-Belver, Ernesto Cilleruelo, Gaizka Garechana, "Design and Implementation of a Cloud Computing Adoption Decision Tool: Generating a Cloud Road", PLoS ONE, Volume 10, Issue 7, July 2015, Pages 1-20.

[15] Sameer Hasan Albakri, Bharanidharan Shanmugam, Ganthan Narayana Samy, Norbik Bashah Idris, Azuan Ahmed, "Traditional Security Risk Assessment Methods in Cloud Computing Environment: Usability Analysis", Volume 73, Issue 2, 2014, Pages 483-495.

[16] Kai Hwang, Deyi Li," Trusted Cloud Computing With Secured Sources and Data Coloring", IEEE Computer Society on Internet Computing, Mar 2010

[17] Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Transactions on Services Computing, Volume 6, Issue 2, April-June 2013, Pages 227-238.

[18] Shuai Ding, Chen-Yi Xia, Kai-Le Zhou, Shan-Lin Yang, Jennifer S. Shang, "Decision Support for Personalized Cloud Service Selection through Multi-Attribute Trustworthiness Evaluation", PLoS ONE, Volume 9, Issue 6, June 2014, Pages 1-11.

[19] Niroshinie Fernando , Seng W. Loke , Wenny Rahayu, "Mobile cloud computing: A survey", Elsevier, Future Generation Computer Systems, Volume 29, Issue 1, January 2013, Pages 84–106.