Federation of Selfish Cloud Providers by Innovative Economic and Secure Sharing Model

R. Vijin
Department of Computer Science, University College of Engineering, Nagercoil.

J. Banumathi
Assistant Professor, Department of Computer Science, University College of Engineering, Nagercoil.

Abstract-Cloud computing has a solution for solving enterprise resource allocation and configuration. A cost effective way becomes very challenging and essential among the cloud providers. The plan of a project is to maximizing their profit by selling their unused capacity in the spot market. The proposed work models the interactions among the Cloud Providers as a repeated game among selfish player. Due to uncertain of future workload fluctuations, revenue can act as a participation incentive to sharing in the repeated game. In this proposed system, also investigated the problem of allocation of service security in cloud is a major challenge. One of the key issues is to avoid any unauthorized data modification and virtual machine corruption, possibly due to server compromise. An efficient key pairing homomorphic token based encryption is introduced for verification of virtual machine allocation. The token computation function we are considering belongs to a family of universal hash function.

Index Terms - Security Model, Optimal spot market allocations, Repeated Game-Theoretic Framework.

1. INTRODUCTION

Cloud computing is an emerging paradigm that Substantiates the vision of modifying computational power, storage, and software services [11]. In such a vision, software applications of different clients are executed over the shared cloud. All applications run in complete isolation through virtual machine (VM) instance. It launched and terminated on the cloud data centers to host applications of cloud clients on a per-needed basis. Clients of an IaaS cloud are mostly service providers from small-scale to world-wide enterprises and web service providers. One of the major problems that face the cloud providers (CPs) is the uncertainty in their workloads. So I proposed a new model for capacity sharing in a federation of IaaS CPs.

- The capacity sharing strategies that maximize the long-run revenue of the federation, dubbed as socially optimal spot market allocations, and demonstrate their enforcement limitation.
- Using a formulation based on multistage games, a set of self-enforceable CPs capacity sharing strategies that maximize the federation's long-term revenue yet can achieve more revenue than what the individual CP can achieve outside the federation.

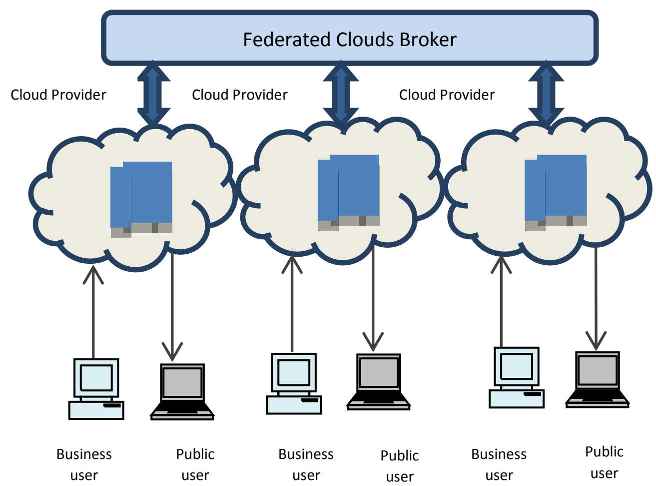


Fig.1.1: The adopted model of federated clouds.

A mechanism to dynamically allocate resources of distributed data centers among different spot markets with the objective of maximizing the total revenue. A market clearing pricing mechanism is developed where a centralized broker dynamically adjusts a single VM price for the federation. The proposed model does not assume any specific pricing scheme for the spot markets, and can employ the following resource allocation.

The problem for allocating the appropriate cloud provider considering tasks with deadline constraints is presented. In general, existing approaches in the literature are concerned only with the instantaneous CP gains. However, most of the attention of these approaches has been focused on finding efficient pricing strategies or techniques for solving the centralized optimization problem of utility maximization in a decentralized manner. The presented work is the first to address the problem of the federated CPs long-term revenue maximization given future workloads uncertainty.

2. RELATED WORKS

2.1. Federated Model

Federation can help providers to absorb overloads due to spikes in demand. At the center of this model, the Cloud Exchange service plays the role of information service directory. With the aim of finding available resources from the members of federation, providers send an inquiry to the Cloud Exchange Service in case of shortage of local resources. The Cloud Exchange is responsible for generating a list of providers with corresponding service prices that can handle the current request. Therefore, the resource availability and price list is used by providers to find suitable providers where requests can be redirected to.

Decision on allocating additional resources from a federated Cloud provider is performed by a component called Cloud Coordinator. The amount of idling capacity each provider shares with other members and the way providers price their resources is also decided by the Cloud Coordinator. These decisions significantly affect the profit of providers, and thus they are of paramount importance for the successful adoption of the federation paradigm by Cloud providers. Moreover, agreements between federation members are necessary in order to make the federation profitable to all its members. We call these agreements Federation Level Agreement (FLA).Therefore, the instant federation price of a resource per hour can be computed as

$$F = \frac{M_p - M_{idle}}{M_p} \cdot (F_{max} - F_{min}) + F._{min}, \rightarrow (1)$$

Where F is the resource's federation price; M_p and M_{idle}aretotal capacity and idling capacity of the provider data center respectively, F_{max} is the on-demand VM price to customers and F_{min} is the minimum profitable price for the provider. The provider does not sell resources for prices smaller thanF_{mim}.

2.2. Economic Sharing Model

The profit obtained from the repeated game can derive higher revenue using a simple grim trigger punishment strategy. Derive a simple update rule to find the sub game perfect Nash Equilibrium values for the spot market allocations. Reduce workload fluctuation.

This pricing mechanism facilitates load balancing between federated providers, since it results in cheaper price for providers with larger amount of resources. Nevertheless, Equation 1 does not reveal such sensitive information, since providers are free to advertise a subset of their resources, and thus members cannot determine the overall utilization of other member's resources.

2.3. Resource Provisioning Policies

Resource provisioning in Cloud providers is a challenge because of the high variability of load over time. Federation of Cloud providers requires having a clear understanding of the consequences of each decision. SP have different choices for incoming requests: rejecting, outsourcing, or terminating spot leases to free for more profitable requests. Outsourcing is more profitable.

Shutting down, unused hosts of the data centers to save electric power consumption. Dynamic pricing of resources to offers idle capacity. It is focused on specific policies to be applied by Cloud IaaS resource providers to decide when to buy computational resources and how resources should be made available in the market for other IaaS providers.

2.4. Optimization of Resource Provisioning

An optimal cloud resource provisioning (OCRP) algorithm is proposed by formulating a stochastic programming model. The OCRP algorithm can compute resources for being used in multiple provisioning stages as well as a long-term plan. OCRP algorithm is proposed to minimize the total cost for provisioning resources in a certain time period. To make an optimal decision, the demand uncertainty from cloud consumer side and price uncertainty from cloud.

This OVMP algorithm can yield the optimal solution for both resource provisioning and VM placement in two provisioning stages. It can reduce the cost of using computing resource significantly. Effectively save the total cost. Effectively achieves an estimated optimal solution. The optimal cloud resource provisioning algorithm is proposed for the virtual machine management. The optimization formulation of stochastic integer programming is proposed to obtain the decision of the OCRP algorithm as such the total cost of resource provisioning in cloud computing environments is minimized. The objective is to address uncertainty of resources availability. In a binary integer program to maximize revenues and utilization of resource providers was formulated. In an optimization framework for resource provisioning was developed. This framework considered multiple client QoS classes under uncertainty of workloads.

2.5. Dynamic Resource Pricing

Strategic-proofing dynamic pricing scheme is suitable for allocating resources on federated clouds. Here, pricing is used to manage rational users. A rational user are an individual user, a group, or an organization, depend on application. In federated clouds, users request more than one type of resources from different providers. Auctions are usually carried out by a third party, called the market-maker, which collects the bids, selects the winners and computes the payments. Buyers and sellers are globally distributed, it is practical to adopt a peer-to-peer approach, where, after pricing and allocation, buyers connect to sellers to use the resources paid for.

It provides better economic efficiency. Also it provides higher number of successful buyer requests and allocated seller resources. Buyer welfare is increased. Dynamic resource pricing use sampling techniques that should be reduce the sampling errors.

3. PROPOSED SYSTEM

3.1. Security Model

The three issues of cloud computing security are: confidentiality, integrity and availability.

Availability:

Availability is the attestation that data will be available to the user in a perpetual manner irrespective of location of the user. It is ensured by: fault tolerance, network security and authentication.

Integrity:

Integrity is the assurance that the data sent is same as the message received and it is not altered in between. Integrity is infringed if the transmitted message is not same as received one. It is ensured by: Firewalls and intrusion detection.

Confidentiality:

Confidentiality is avoidance of unauthorized exposé of user data. It is ensured by: security protocols, authentication services and data encryption services.

Since cloud computing is utility available on internet, so various issues like user privacy, data theft and leakage and unauthenticated accesses are raised.

Cryptography is the science of securely transmitting and retrieving information using an insecure channel. It involves two processes: encryption and decryption. Encryption is a process in which sender converts data in form of an unintelligible string or cipher text for transmission, so that an eavesdropper could not know about the sent data. Decryption is just the reverse of encryption. The receiver transforms sender's cipher text into a meaningful text known as plaintext.

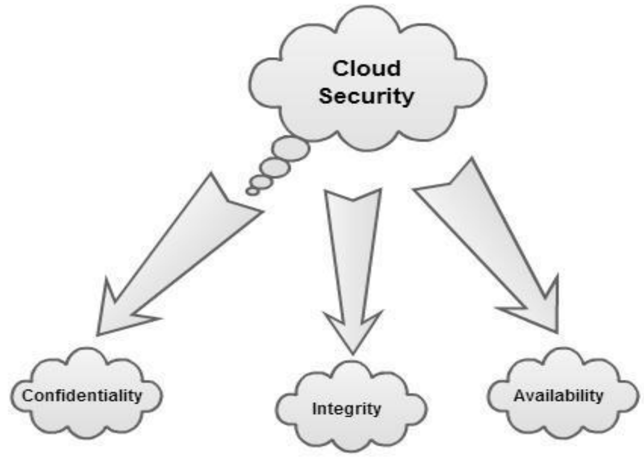


Fig.3.1. Cloud Security

3.2. Protocol Initialization

Using this scheme allows efficient aggregation of encrypted data at the cloud provider's federation, which also guarantees data confidentiality [6]. In the protocol initialization, the cloud trusty performs the following operations of key pre-distribution to all the sensor nodes:

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages, where$k \in [m-1]$, m is a large integer.
- Generate the pairing parameters$\left(p, q, E/F_p, G_1, G_2, e\right)$. Select a generator P of G_1stochastically.
- Choose two cryptographic hash functions: H, for the point mapping hash function which maps strings to elements in G_1, and h, for mapping arbitrary inputs to fixed-length outputs.
- Pick a random integer $\tau \epsilon z_P^*$as the master key msk, set $P_{pub} = \tau p$ as network public key.
- Preload each sensor node with the system parameters $param = (k, m, p, q, E/, G_1, G_2, e, H, h, P, \tau)$.

3.3. Key Management for Security

Assume that a leaf sensor node j transmits a message M to it's CH_i , and encrypts the data using the encryption key k from the additively homomorphic encryption scheme. We denote the cipher text of the encrypted message as C. We adapt the algorithms of the IBS scheme from CWSNs practically and provide the full algorithm in the signature verification, where security is based on the DHP in the multiplicative group [3]. The IBS scheme in the proposed

SET-IBS consists of following three operations: extraction, signing, and verification.

Extraction:

Node j first obtains its private key as $sek_j = \tau H(ID_j \| t_j)$ from *msk* and ID_j, where ID_j is its ID, and t_j is the time stamp of node j's time interval in the current round that is generated by its CH_i from the TDMA control.

Signature signing:

The sensor node j picks a random number $\propto_j \in z_q^*$ and computes $\theta_j = e(P,P)^{\alpha_j}$ the sensor node further computes

$$c_j = h(C_j \| t_j \| \theta_j) \quad \rightarrow (2)$$

Let

$$\sigma_j = c_j sek_j + \propto_j P \quad \rightarrow (3)$$

Where $\langle \sigma_j, c_j \rangle$ is the digital signature of node j on the encrypted message c_j. The broadcast message is now concatenated in the form of $\langle ID_j, C_j, t_j, \sigma_j, c_j \rangle$.

Verification:

Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the time stamp of current time interval t_j and determines whether the received message is fresh [3]. Then, if the time stamp is correct, the sensor node further computes

$$\theta_j' = e(\sigma_j, P) e(H(ID_j \| t_j), -P_{pub})^{c_j} \quad \rightarrow (4)$$

We will have the formula below if the received message is authentic:

$$\begin{aligned}\theta_j' &= e(\sigma_j, P) e(H(ID_j \| t_j), -P_{pub})^{c_j} \\ &= e(\sigma_j, P) e(H(ID_j \| t_j), -\tau P)^{c_j} \\ &= e(c_j sek_j \propto_j P, P) e(H(ID_j \| t_j), \tau P)^{-c_j} \\ &= e(P,P)^{\alpha_j} = \theta_j \quad \rightarrow (5)\end{aligned}$$

If $h(C_j \| t_j \| \theta_j') = h(C_j \| t_j \| \theta_j) = c_j$, which is equal to that in the received message, the sensor node considers the received message authentic, and propagates the message to the next hop or user [6]. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, and ignores it.

3.5. A Game-Theoretic Framework

The proposed approach is motivated by the observation that the behavior of the CPs in the above two models represents two extreme forms of a strategy adopted by players in a game of sharing unused VMs. Recognizing this fact enables us to reformulate the problem in a more general setting that alleviates the limitations of the above two models [5].

In game theory, a stage game is typically defined by a triplet consisting of a set of players, strategies, and payoffs, where the players are assumed to be rational agents representing at maximizing their payoffs. In our setting, the set of N CPs represents the players and the strategies are represented by the allocations of VMs to the spot markets, $(\omega_i(s_t))_{i=1}^N$, while the revenue functions $(r_i(\omega_i(s_t)))_{i=1}^N$ represent their payoffs. Hence, at each time period, t, and after observing the current state, $s_t = (e_1(s_t), \dots, e_N(s_t))$ the CPs engages in the game $\langle \mathcal{N}, (\omega_i(s_t))_{i=1}^N, (r_i(\omega_i(s_t)))_{i=1}^N \rangle$ by deciding the best strategies to maximize their revenues. The game solution represented by the player's strategies where no player has an incentive to deviate from its chosen strategy after considering all other players' strategies is called a *Nash Equilibrium* [5][1].

3.5. Subgame Perfect Spot Allocations

In the subgame perfect spot allocation is used repeated game setting, the CPs is interested in finding a subgame perfect Nash Equilibrium (SPNE). A subgame-perfect Nash Equilibrium is a strategy [4].

That is a NE for the CPs in every sub game (i.e., up to any history h_t) of the original game.

We search for an SPNE strategy that should determine the amount of VMs to offer in the spot market $\omega_i(h_t)$ at time t, and to share in the federation $e_i(s_t) - \omega_i(h_t)$ after observing a history of states ht. The goal of this strategy is to maximize the federation's expected revenue while guaranteeing the participation of the CPs, or, in other words, while ensuring the self-enforcement of the sestrategies [10].

$$P3: \max_{\omega_i(h_t)} \sum_{i=1}^{N} \lambda_i \sum_{t=1}^{\infty} \sum_{h_t} \delta^t \pi(h_t) r_i(\omega_i(h_t)) \quad \rightarrow (6)$$

Subject to

$$r_i(\omega_i(h_t)) + \sum_{\tau=t+1}^{\infty} \sum_{h_r} \delta^{\tau-t} \pi(h_r \mid h_t) r_i(\omega_i(h_\tau)) \geq \underline{R}_i(s_t) \quad \rightarrow (7)$$

$\forall i$; $\forall st$; $\forall ht$ and the capacity constraints.

We refer to the constraints defined as the federation commitment constraints. We also say that a commitment constraint for CP_i at state s_t binds if it is satisfied with strict equality.

A VM sharing strategy, $(\omega_i(h_t))_{i=1}^N$ in the infinitely repeated game $\langle \mathcal{N}, (\omega_i(s_t))_{i=1}^N, (r_i(\omega_i(s_t)))_{i=1}^N \rangle$ that solves P3 is an SPNE.

Solving P3 can be carried out by first considering its Lagrangian which is given by

$$\sum_{t=1}^{\infty}\sum_{h_t}\Big[\delta^t\pi(h_t)\sum_{i=1}^{N}\lambda_i\, r_i\big(\omega_i(h_t)\big) + \zeta(h_t)\omega_i\sum_{i=1}^{N}\big(e^i(h_t)-\omega_i(s_t)\big) + \eta_i(h_t)\Big(\sum_{r=\tau}^{\infty}\sum_{h_\tau}\delta^{\tau-t}\pi(h_\tau\,|s_t)r_i\big(\omega_i(h_\tau)\big) - \underline{R}_i(s_t)\Big)\Big] \quad \rightarrow(8)$$

The obtained $\lambda_i(h_t)$represents the new normalized relative weight of CP_i in the federation after a historyh_t. If $\lambda_i(h_t)$is known for $i = 1, \dots\dots, N$ then a solution to P3 along with the capacity constraint is be obtained. According to Proposition this solution represents the SPNE strategies for the CPs.

3.6. Recursive Formulation

To obtain a solution for P3, the ratios of the marginal revenues in$\frac{\lambda_j(h_t)}{\lambda_i(h_t)}$ must be computed and employed to generate a system of N −1 equations for the unknowns$\omega_i(h_t)$. Combining those equations with the capacity constraint at equality provides a system whose unique solution would serve as the strategy adopted by the CPs.

Using the Markov properties of the workload [7], this problem can be cast as a recursive one, which yields a simple update rule to compute ratios of the CPs' marginal revenues at t, $\frac{\lambda_j(h_t)}{\lambda_i(h_t)}$. We first begin with the derivation of the update rule.

By the definition of the normalized dynamic weights, we have

$$\lambda_i(h_1) = \frac{\lambda_i + \frac{\eta_i(h_1)}{\delta\pi(s_1)}}{\sum_{j=1}^{N}\Big(\lambda_j + \frac{\eta_j(h_1)}{\delta\pi(s_1)}\Big)} = \frac{\lambda_i + \frac{\eta_i(h_1)}{\delta\pi(s_1)}}{1+\sum_{j=1}^{N}\frac{\eta_j(h_1)}{\delta\pi(s_1)}} \quad \rightarrow(9)$$

Then, $\lambda_i(h_t)$can also be defined recursively by

$$\lambda_i(h_t) = \frac{\lambda_i(h_{t-1}) + \frac{\eta_i(h_t)}{\delta\pi(s_t)}}{1+\sum_{j=1}^{N}\frac{\eta_j(h_t)}{\delta\pi(s_t)}}, t > 1 \quad \rightarrow(10)$$

In the infinitely repeated game$\langle\mathcal{N}, (\omega_i(s_t))_{i=1}^{N}, \big(r_i(\omega_i(s_t))\big)_{i=1}^{N}\rangle$, at any state$s_t = s$, the normalized relative weight of the marginal revenue of any CP,CP_i, in the SPNE strategies is always bounded such that$\lambda_i{}^s \le \lambda_i(h_t) \le \lambda'_i{}^s$, where the bounds $\lambda_i{}^s$ and are $\lambda'_i{}^s$only state-dependent constants [2].

In the infinitely repeated game$\langle\mathcal{N}, (\omega_i(s_t))_{i=1}^{N}, \big(r_i(\omega_i(s_t))\big)_{i=1}^{N}\rangle$, at any state$s_t = s$, the normalized relative weight of the marginal revenues for any CP,CP_i, in the SPNE is$\lambda_i(h_t) = \lambda_i{}^s$ if, and only if, the commitment constraint for CP_i binds. In the infinitely repeated game$\langle\mathcal{N}, (\omega_i(s_t))_{i=1}^{N}, \big(r_i(\omega_i(s_t))\big)_{i=1}^{N}\rangle$, the normalized weight of the marginal revenue of any CP,CP_i, in the SPNE strategies, follows the following update rule [5].

$$\lambda_i(h_t)\begin{cases} = \lambda_i{}^s, & \lambda_i(h_{t-1}) \le \lambda_i{}^s, \\ = \lambda_i(h_{t-1}), & \lambda_j{}^s \le \lambda_j(h_{t-1}) \le \lambda'_j{}^s \forall j, \\ \in [\lambda_i{}^s, \lambda_i(h_{t-1})], \lambda_i{}^s \le \lambda_i(h_{t-1}) \le \lambda'_i{}^s, & \\ \quad \wedge\exists j\ s.t\ \lambda_j(h_{t-1}) \le \lambda_j{}^s, & \\ = \lambda'_i{}^s, & \lambda_i(h_{t-1}) \le \lambda'_i{}^s, \end{cases} \quad \rightarrow(11)$$

Given an initial federation weight $\lambda_i(h_0) = \lambda_i$.

4. RESULTS AND DISCUSSIONS

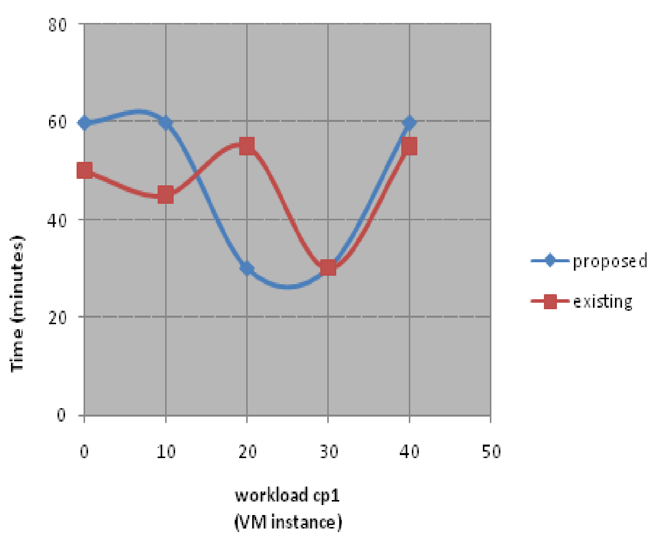
The employed simulation environment models a federation of three CPs, all offering a single type of VMs with the following configurations: 1 CPU core, 1.7-GB RAM, 1 EC2 Compute Unit, and 160 GB of local storage, which is similar to that of Amazon EC2 small instances.

	NFC	FC	SFC
Work load	Reduced up to 35%	Reduced more than 50%	Reduced more than 50%
Revenue	Increased 65%	Increased 80%	Increased 90%
Security	poor	average	Fully

Table 1: Comparison of federated clouds

Where, NFC – Non Federated Cloud,
FC – Federated Cloud,
SFC – Secure Federated Cloud

All CPs follow a dynamic pricing mechanism for the spot market according to the market demand.



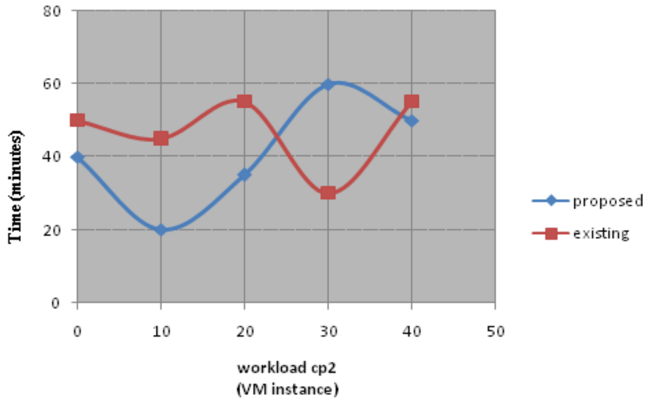


Fig.3.The hourly spot markets workloads.

Two major performance issues for CPs' spot markets are the unpredictability of VM availability and the high variance in the VM hourly prices. These two problems are easily detected from the performance of the non-federated mechanism which provides a 60-hour snapshot of the operation of the CPs' spot markets. The effects of price fluctuation in the non-federated strategy are also reflected by similar fluctuations in the hourly revenue. For example, consider the spot market of CP3, where we can easily see that a sudden decrease of workloads due to a decrease in the VM availability from 950 VMs at $t = 18$ to 150 spot VMs at $t = 19$ results in a VM price spike from less than 0.02 to almost 0.06 dollars. Here, the CPs almost equally divides their VM shares at each step. As $\delta = 0.9$is large enough, both CPs have a value, high enough, for future revenue to self-enforce the best outcome of the game which is that imposed originally by the fully federated model. The obtained values demonstrate how the proposed scheme effectively reduced the variance in the prices and workloads by more than 50 percent. Furthermore, as indicated by much higher revenue can always be achieved if the CPs maintains a higher value (δ) for future revenues.

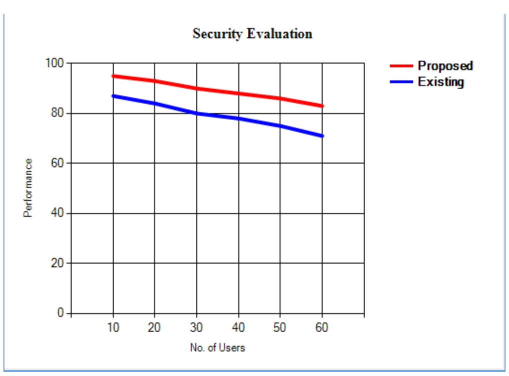


Fig.4.The security evaluation

To evaluate the energy consumption of the computational overhead for security in communication, for the performance evaluation we compare the number of users, performance of security evaluation in cloud environment. The number of cloud users will increase the performance of a security system is very poor. So, I decide to improve their performance of a federation.

5. CONCLUSION

An innovative economic sharing model is used to sharing capacity in a federation of IaaS cloud providers, this can be done by using interaction among cloud providers as a repeated game of virtual machine that can identify the all unused capacity in the spot market. Performance evaluation results computed the profit that increased by the federation as well as by individual cloud providers and also it demonstrated significant amount of smoothing effects on the spot market prices. It also to be achieves fully decentralized and secure virtual machine sharing between cloud providers.

REFERENCES

[1] D. Kusic and N. Kandasamy, "Risk-Aware Limited Lookahead Control for Dynamic Resource Provisioning in Enterprise Computing Systems," Proc. IEEE Int'l Conf. Autonomic Computing, 2006.

[2] S. Chaisiri, B. Lee, and D. Niyato, "Optimization of Resource Provisioning Cost in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 164-177, Apr.-June 2012

[3] K. Le, R. Bianchini, J. Zhang, Y. Jaluria, J. Meng, and T. Nguyen, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks," Proc. Int'l Conf. High Performance Computing, Networking, Storage and Analysis (SC '11), pp. 1-12, 2011.

[4] A. Toosi, R. Calheiros, R. Thulasiram, and R. Buyya, "Resource Provisioning Policies to Increase IaaS Provider's Profit in a Federated Cloud Environment," Proc. IEEE 13th Int'l Conf. High Performance Computing and Communications, pp. 279-287, 2011.

[5] M. Mattess, C. Vecchiola, and R. Buyya, "Managing Peak Loads by Leasing Cloud Infrastructure Services from a Spot Market," Proc. IEEE 12th Int'l Conf. High Performance Computing and Communications (HPCC), pp. 180-188, 2010.

[6] Nancy Samaan, R. Buyya , "A Novel Economic Sharing Model of a Federated Cloud Providers," IEEE Trans. Parallel And Distr. Systems, vol. 25, no. 1, Jan. 2014.

[7] Andrew Chi-Chih Yao and Yunlei Zhao, "Privacy-Preserving Authenticated Key-Exchange Over Internet," IEEE Trans. Info. And Security, VOL. 9, no. 1, Jan 2013.

[8] E. Gomes, Q. Vo, and R. Kowalczyk, "Pure Exchange Markets for Resource Sharing in Federated Clouds," Concurrency and Computation: Practice and Experience, vol. 24, no. 9, pp. 977-991, 2012.

[9] M. Mazzucco and M. Dumas, "Reserved or On-Demand Instances A Revenue Maximization Model for Cloud Providers," Proc. IEEE Int'l Conf. Cloud Computing, pp. 428-435, 2011.

[10] M. Mihailescu and Y. Teo, "Dynamic Resource Pricing on Federated Clouds," Proc. 10th IEEE/ACM Int'l Conf. Cluster, Cloud and Grid Computing (CCGrid), pp. 513-517, 2010.

[11] Aarti Singh, Manisha Malhotra "Security Concerns at Various Levels of Cloud Computing Paradigm", International Journal of Computer Networks and Applications, Volume 2, Issue 2, Page No: 41-45, April – May (2015).