International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 5, October 2017, pp. 2645~2650
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i5.pp2645-2650

Privacy Preserving Auction Based Virtual Machine Instances Allocation Scheme for Cloud Computing Environment

Suneeta Mohanty, Prasant Kumar Pattnaik, G. B. Mund
School of Computer Engineering, KIIT University, Bhubaneswar, India

Article Info

Article history:

Received Jul 23, 2016
Revised Jun 7, 2017
Accepted Sep 11, 2017

Keywords:

Auction
Cloud service provider (CSP)
Cloud computing environment (CCE)
Privacy
Virtual machine (VM)

ABSTRACT

Cloud Computing Environment provides computing resources in the form of Virtual Machines (VMs), to the cloud users through Internet. Auction-based VM instances allocation allows different cloud users to participate in an auction for a bundle of Virtual Machine instances where the user with the highest bid value will be selected as the winner by the auctioneer (Cloud Service Provider) to gain more. In this auction mechanism, individual bid values are revealed to the auctioneer in order to select the winner as a result of which privacy of bid values are lost. In this paper, we proposed an auction scheme to select the winner without revealing the individual bid values to the auctioneer to maintain privacy of bid values. The winner will get the access to the bundle of VM instances. This scheme relies on a set of cryptographic protocols including Oblivious Transfer (OT) protocol and Yao's protocol to maintain privacy of bid values.

Corresponding Author:

Suneeta Mohanty,
School of Computer Engineering,
KIIT University,
Bhubaneswar, India.
Email: suneetamohanty@gmail.com

1. INTRODUCTION (10 PT)

Cloud Computing Environment(CCE) enables the cloud users to deploy their applications in cloud via Internet on demand[1]. Cloud is a type of distributed and parallel system comprising of a collection of interconnected and virtualized computers which are dynamically provisioned and presented as one or more unified computing resources based on Service Level Agreement(SLA) [2][3] using pay per use model. At the same time, Cloud Service Provider get benefit due to commercialization of huge computing resources through cloud platform. SLA is a legal contract between CSP and cloud user to achieve Quality of Service(QoS) [3]. A virtualization environment enables the service provision by creating Virtual Machine instances which has become the essential technology of Cloud Computing Environments[4]. Virtual Machines are the software implementation of the computing environment where an OS or a program may be installed and run. Currently fixed-price allocation mechanism is used by most of the CSPs to allocate Virtual Machine instances to their user. Cloud Computing Environment offers IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) on the basis of subscription that helps different organizations in decreasing operational expenses. In fixed price mechanism, cloud user who values the VM instances more may or may not get access to it. Hence it is not economically efficient[5]. Also fixed price allocation mechanisms may lead to generate revenue which is less than optimal revenue for CSP[5]. This problem can be addressed by using auction based VM instances allocation mechanism. Security is the major concern in cloud[6] and privacy preservation is required to achieve the integrity of data[15]. In this paper, we proposed a privacy preserving auction based VM instances allocation scheme run by CSP which will help in selecting the winner of the auction without seeing the individual bid values of participants of the auction i.e, cloud users.

This paper is organized as follows: Section 2 discusses the existing pricing schemes in CCE. Section 3 proposes a privacy preserving auction scheme for VM instances allocation. Section 4 discusses the experimental result analysis. Lastly section 5 concludes the work along with its future scope.

2. RELATED WORK

Through Cloud Computing Environment(CCE), individual and small to large organizations can fulfil their computational requirements with minimum cost. It is becoming critical for the several Cloud Service Providers(CSP) to determine appropriate price for users. There exist many pricing schemes for Cloud Service Providers which are broadly classified into fixed and dynamic pricing scheme.

CCE provides the required computational needs of the cloud user in terms of Virtual Machines(VM) in pay per use basis. In current scenario, the majority of Cloud Service Provider fix their price based on the size of VM instances. Fixed pricing scheme is one of the widely used technique in CCE. In fixed price mechanism, VM instances are allocated on a first-come, first-serve basis to the users till the resources are exhausted[7].Use of fixed price scheme may tend to lower the revenue generation for the CSP as the cloud user pay less for using the same resources for a long period. So to address the problem of high revenue generation for CSP, auction based pricing scheme is used.

In dynamic pricing scheme, final service price is decided dynamically through auctions. Auction based pricing scheme follows dynamic pricing policy where a target service price is achieved resulting from dynamic supply and demand through auction.

Combinatorial auction in CCE allows the user to buy a bundle of VM instances through auction which is profitable to both the buyer and seller. For the entire bundle, bid is submitted as a single unit.

Zaman and Grosu [7] proposed a combinatorial auction mechanism which allows the cloud users to bid for a subset of a VM instances (bundle). Cloud Service Provider being the auctioneer selects the winner having the highest bid value for that particular bundle of VM instances. In their work, they have proposed CA-GREEDY and CA-LP mechanism to perform combinatorial auction. They analysed the pros and cons of the proposed mechanisms and provided the guidelines for its implementation.

Prasad et al. [8] presented a procurement auction as a solution of resource allocation problem in cloud. In their proposed auction scheme they have introduced the concept of auction broker which will run the auction mechanism instead of Cloud Service Provider. As a result of which cloud users will contact auction broker for their resource requirements and different Cloud Service Providers will participate in the auction run by the broker for the resource allocation. Their proposed auction scheme was based on Combinatorial Auction Branch on Bids(CABOB) model and supports multiple resource selection by cloud user.

Garg et al. [9] proposed a double auction mechanism that involves both buyer and seller to submit their bids to the auctioneer. The auctioneer takes the help of meta scheduler to sort the bids in ascending and descending order and look for a match. If match found, the average of the values is set as the auction price for the resource. The same process continued for the unmatched request. Both seller and buyer are benefitted in this auction mechanism.

Zaman and Grosu [10] proposed CA-PROVISION mechanism to address the dynamic provisioning of VM instances to generate more profit for cloud which is not considered in their previous work[7].Through extensive experiments they have proved that in case of low demand, CA-PROVISION generates higher revenue than CA-GREEDY.

Amazon EC2 uses an auction called as Amazon spot instances [11] where the users bid for the unused virtual machines. User having higher price than spot price which is set based on data centre utilization by the Amazon will get the access to that VM instances.

Choi and Lim [12] discussed the importance of SLA violation cost to increase Cloud Service Provider's profit. They proposed a scheme to reduce the penalty cost for SLA violation during combinatorial Auction considering urgency of jobs. They calculated probability of each job's deadline violation to find expected profit value for the service provider to select the user with largest expected value as the bid winner. Thus decreasing SLA violation leads to decrease penalty cost which in turn increases service provider's profit.

3. PROBLEM STATEMENT

Cloud user can choose a wide range of VM instances based on the performance he/she wants. Deployment of more VM instances or replacing the existing VM instances with powerful VM instances can increase the performance of the application. Hence to get better performance, cloud user can opt to get appropriate VM instances. In existing auction mechanisms, auctioneer knows the bid values. It may lead to loss of privacy and integrity of bid values to win the auction or to gain more profit. Hence to prevent such kind of activities, we have proposed an auction scheme that allows the user to participate in a privacy preserving auction to get the best VM instances without revealing their bid values to the auctioneer (CSP. The VM instances are assigned to the cloud user with highest bid value. Hence, generating higher revenue for the Cloud Service Provider (CSP). The auction-based VM instances allocation scheme is run by the CSP. Like other secure computation, the proposed auction scheme can determine the winner of the auction using secure multiparty computation which relies on a set of cryptographic protocols including Oblivious Transfer (OT) protocol and Yao's protocol using RSA algorithm.

3.1. Yao's Protocol

Secure multi-party computation allows multiple parties each having a secret input to compute a function while ensuring no party will reveal the inputs to each other or to a trusted third party. The computation result will be communicated to all parties. However, a given party will only be able to compute what can be inferred from the final results and its own input. In [13] Yao introduce the problem of computing the maximum with the following problem: Two millionaires want to compare their riches, but do not want to reveal to each other which is the exact amount of their wealth.

3.2. Oblivious Transfer (OT) protocol

Oblivious Transfer protocol [14] is central to implement Yao's protocol. OT_1^2, 1-out-of-2 oblivious transfer ensures that one party can obtain one of the two messages from a second party and both the parties could not know which values are selected by each other. OT_1^k,1-out-of-k oblivious transfer, is the functionality: $OT_1^k((\sigma_{1,}\ \sigma_{2,\dots,}\ \sigma_k\ ),i) = (\lambda, \sigma_i)$ where $\sigma_{1,}\ \sigma_{2,\dots,}\ \sigma_k \in \{\ 0,1\}$ and $i \in \{\ 1,\dots,k\ \}$.Here, the first party (Alice) has k secret bits $\sigma_{1,}\ \sigma_{2,\dots,}\ \sigma_{k.}$ Bob has a secret index i. At the end of the protocol, Bob learns only σ_i and Alice learns nothing (λ). In particular, Alice does not know which of her bits was learned by Bob, and Bob does not learn σ_j for any $j \neq i$. Oblivious transfer is central to many of the constructions for secure multiparty computation.

4. THE PROPOSED PRIVACY PRESERVING AUCTION SCHEME

The system model of the proposed scheme, which includes 'n' organizations (Cloud $User_1$, Cloud $User_2$..., Cloud $User_n$) and a Cloud Service Provider is illustrated in Figure1. The public key (data encryption) and private key (data decryption) are managed by the Cloud Service Provider to perform privacy-preserving auction among a number of organizations.

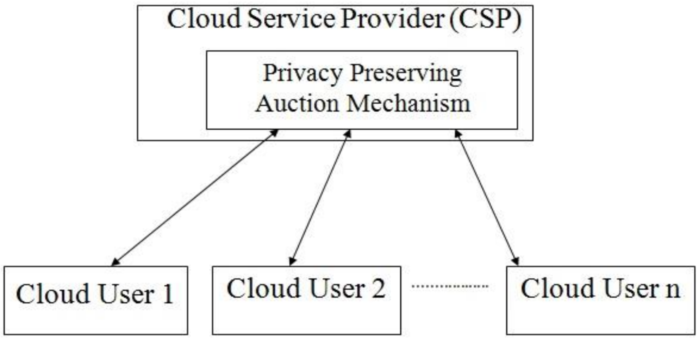
Cloud Service Provider (CSP)
Privacy Preserving Auction Mechanism
Cloud User 1
Cloud User 2
Cloud User n

Figure 1. System model of the proposed privacy preserving auction scheme

All participants of this scheme work in a semi-honest environment, where they may try to deduce additional information during the protocol execution. The workflow of the proposed scheme is summarized in Table 1 as given below:

Table 1. Workflow of the proposed system

```
Step 1-Key Generation Algorithm used by CSP
1.1   Choose p and q: two distinct prime numbers
1.2   Compute $N = p×q$, Where N is used as the modulus for public and private keys
1.3   Compute $\Phi (N) = (p-1)×(q-1)$, Where $\Phi$ is the Eulier function
1.4   Choose encryption key which is an integer 'e' such that, $1 < e < \Phi (N)$ and greatest common
      divisor of $(e, \Phi (N)) = 1$
1.5   Determine the decryption key $d =( 1/e) \bmod \Phi (N)$
1.6   All the above values of public key(e,N=p×q) and private key(d) must be kept secret by CSP
Step 2- Collection of request from participants and preparation of list by CSP
2.1   for j = 1, . . . , n do
2.2       Receive $(r^j_1, . . . , r^j_m )$ from user $u_j$
2.3   end for
2.4   Sort users according to their time of placing the request, from earliest to latest
      (Here we assume u1, u2, . . . , un as the order.)
Step 3- Winner selection by the Cloud Service Provider
3.1   Let us assume first and second participant in this protocol are denoted by Alice and Bob
      respectively
3.2   CSP will send e,N to Bob and N to Alice
3.3   Bob picks random integer 'X' of N bit and calculate $C = X^e \bmod N$
3.4   Bob calculates $C- I_t + 1$, where $I_t$ is the sensitive data of Bob and send it to CSP
3.5   CSP will generate $Y_1,Y_2,Y_3......,Y_{10}$ such that $Y_1$ is the decipherment of $C- I_t +1$, $Y_2$ is the
      decipherment of $C- I_t +2$ and so on. using the formula :
      $Y_1= (C- I_t +1)^d \bmod N$ ,$Y_2= (C- I_t +2)^d \bmod N...Y_{10}= (C- I_t +10)^d \bmod N$
3.6   CSP sends $Y_1,...Y_{10}$ to Alice
3.7   Alice generates a prime number P which is N/2 bit and $|Z_i-Z_j| \geq 2$ for $i\neq j$ and calculates
      $Z_i=Y_i \bmod P$ where $i,j \in [1..10]$
3.8   Alice adds 1 to $Z_i$ values for all $i >I_k$ where $I_k$ is the secret value of Alice
3.9   Alice sends P, Z values to CSP
3.10  CSP sends P, Z values to Bob
3.11  Bob calculates $G= X \bmod P$ and checks
      If ($Z_n \equiv G \bmod P$)
      Set W= 0
      Else
      Set W= 1
3.12  Bob sends W to CSP
3.13  CSP checks
       if( W==0)
        Alice is the winner
       else
        Bob is the winner
3.14  The same process will be repeated for the winner and next participant till n number of user
      to determine the winner of the Auction
Step 4- VM instance allocation
4.1   Winner pays the CSP
4.2   CSP will assign VM instances to the winner
```

5. RESULT ANALYSIS

In this section, we focus on evaluating the performance of one of the existing auction scheme and the proposed auction scheme in terms of execution time. The technical specification of CPU, OS and RAM considered for our experimental setup are as follows: CPU: Intel Core i5 2.7GHz, OS: Ubuntu, RAM: 8GB. In our experiment,we have increased the number of participants(Cloud Users) from 2,4,8 to 16 and recorded corresponding execution times in milli seconds(ms) to select the winner using CA-GREEDY algorithm[7] and our proposed privacy preserving auction scheme which are shown in Figure 2 and Figure 3 respectively. As shown in Figure 2, CA-GREEDYalgorithm takes 58ms for two users, 62ms for four users, 65ms for eight users, 66ms for 16 users to select the winner of the auction. As shown in Figure 3, the proposed auction scheme takes 995ms for two users, 1582ms for four users, 2946ms for eight users, 5638ms for 16 users to select the winner of the auction.

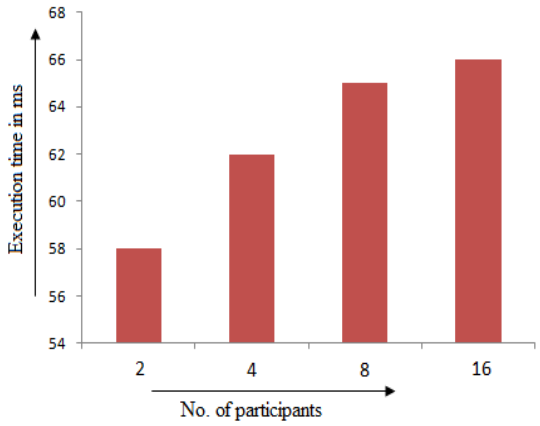

Figure 2. Execution Time vs. No. of participants for CA-GREEDY[7] Algorithm

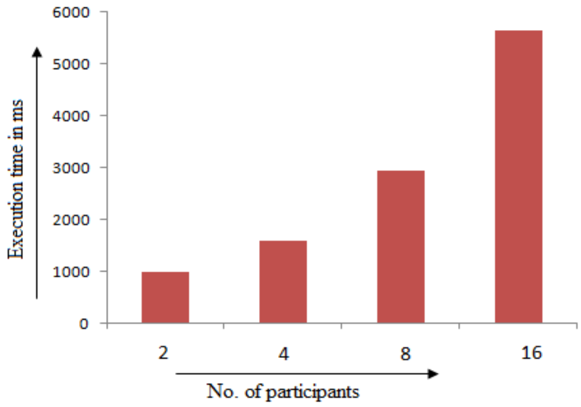

Figure 3. Execution Time vs. No. of participants for the proposed auction scheme

The result obtained shows that the execution time of our proposed auction scheme increases by 1.17% than the existing CA-GREEDY algorithm [7] by considering the privacy issues of bid values which is missing in CA-GREEDYalgorithm. However, the computing ability of CSP is much more than our simulation PC to carry out these auction mechanisms. Hence the computation time will be comparatively less than ours in real CCE. Hence, this algorithm can be used as a privacy preserving auction scheme to achieve privacy of bid values for a fair auction in Cloud Computing Environment.

6. CONCLUSION

In this paper, we presented one scheme to facilitate privacy preserving auction for VM instances allocation where all participants follow the protocol and nothing can be inferred from one's input and output. This proposed scheme can be used to generate higher revenue for CSP without disclosing the bid values of different users participated in the auction to the auctioneer (CSP). Our proposed auction scheme work in the semi-honest model along with the assumption that all participants are following the protocols that need further investigation.

REFERENCES

[1] Sarathy V, Narayan P, Mikkilineni R. *Next generation cloud computing architecture -enabling real-time dynamism for shared distributed physical infrastructure*. 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE'10), Larissa, Greece. 2010; 48-53.

[2] Buyyaa R, Yeoa CS, Venugopala S, Broberga J, and Brandicc I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*. 2009; Volume 25(6): 599-616.

[3] T Sutikno, D Stiawan, IMI Subroto, "Fortifying big data infrastructures to face security and privacy issues," *TELKOMNIKA Telecommunication Computing Electronics and Control.*, vol. 12, no. 4, pp. 751-752, 2014.

[4] Mohanty S, Pattnaik PK, Mund GB. *Framework for Auditing in Cloud Computing Environment.* Proceedings Journal of Theoritical and Applied Information Technology. 2014; Volume 65(1): 261-267.

[5] Wang R. Auctions versus posted-price selling. *The American Economic Review*, 1993; vol. 83(4): 838–851.

[6] Sastry KN, Rao BT, Gunasekhar T. Novel approach for control Data Theft Attack in Cloud Computing. *International Journal of Electrical and Computer Engineering (IJECE)*. 2015; Vol. 5(6): 1545-1552.

[7] Zaman S, Grosu D. Combinatorial auction-based allocation of virtual machine instances in clouds. *Journal of parallel and distributed computing.* 2013; 1-14.

[8] Prasad V, Rao S, Prasad A. *A Combinatorial Auction mechanism for Multiple Resource Procurement in Cloud Computing*. Procedings of 12th International Conference on Intelligent System Design and Application. 2012; 337-344.

[9] Garg SK, Venugopal S, Broberg J, Buyya R. Double auction-inspired metascheduling of parallel applications on global grids. *Journal of Parallel and Distributed Computing*. 2013; 450-464.

[10] Zaman S, Grosu D. A Combinatorial Auction-Based Mechanism for Dynamic VM Provisioning and Allocation in Clouds. *IEEE Transactions On Cloud Computing*. 2013; Vol.1(2): 129-141.

[11] I Irmeilyana, I Indrawati, FM Puspita, J Juniwati, "Model and optimal solution of single link pricing scheme multiservice network," *TELKOMNIKA Telecommunication Computing Electronics and Control.,* vol. 12, no. 1, pp. 173-178, 2014.

[12] Choi Y, Lim Y. Optimization Approach for Resource Allocation on Cloud Computing for IoT. *International Journal of Distributed Sensor Networks*, 2016; 1-6.

[13] Yao A. Protocols for Secure Computations. *Proceedings of the IEEE Symposium on foundations of computer science*. 1982.

[14] Rabin MO. How to Exchange Secrets with Oblivious Transfer. *Technical Report Tech.Memo TR-81,Aiken Computation Laborotory.* 1981.

[15] Mohanty S, De R. Survey on Privacy Preservation Methodology in Knowledge Discoverable Cloud Environment. *International Journal of Innovative and Emerging Research in Engineering.* 2017; Volume 4(3): 120-123.