UDC: 004.72
DOI: http://dx.doi.org/10.7708/ijtte2021.11(2).03

A SECURITY-DRIVEN APPROACH TO THE AUCTION-BASED CLOUD SERVICE PRICING

Branka Mikavica[1], Aleksandra Kostić-Ljubisavljević[2], Dražen Popović[3]
[1,2,3] *University of Belgrade, Faculty of Transport and Traffic Engineering, Vojvode Stepe 305, 11000 Belgrade, Serbia*

Received 30 November 2020; accepted 20 January 2021

Abstract: Cloud computing is a widely used paradigm due to its substantial resource integration and computing capabilities. Cloud resources are organized into virtual machines (VMs) with corresponding computational and storage capacities. Security and pricing are considered as important issues from both cloud provider and cloud customers' perspective, directly affecting the cloud provider's revenues and cloud customers' experience. VMs are one of the most vulnerable segments in the cloud environment. In this paper, the VMs security modelling is introduced to assess the security level of VMs. This approach is gathered with cloud service pricing. Auction-based pricing mechanisms are often suggested as a promising solution for revenue maximization. Appropriately set auction mechanisms provide incentives for cloud customers to bid truthfully, i.e., create bids that depict their real willingness to pay cloud service. This paper addresses various bidding strategies and various security levels provided under two auction-based pricing mechanisms, Uniform price auction and Generalized Second-price auction. Comparison of these security-driven auction-based pricing mechanisms is provided based on the winning bids, cloud provider's revenues and possible losses due to VMs unavailability.

Keywords: cloud virtual machines, auction, bidding, pricing, security.

1. Introduction

Cloud computing dynamically organizes cloud resources into virtual machines (VMs) with the required CPU, memory and I/O resources to provide cloud services. The dynamic organization, virtualization, and elasticity, as key characteristics of cloud computing, enable flexible management of cloud resources which can be provided on demand, upon cloud customers' requests. It is a multitenant system that reduces costs and maximizes utilization. Cloud resources can be easily initiated and terminated to adjust to demand.

Security is considered as a major architectural component of the cloud computing environment that affects cloud providers, cloud customers, and other relevant participants. Cloud systems comprise various service management operations. Therefore, there are numerous attacking possibilities for adversaries. Depending on the cloud component under attack, various security issues arise including network-based attacks, storage-based attacks, application-based attacks and VM based attacks (Mikavica and Kostić-Ljubisavljević, 2020a). The cloud resources are connected through a network, concurrently providing

[1] Corresponding author: b.mikavica@sf.bg.ac.rs

connections outside the cloud. Therefore, an intruder may deteriorate data privacy and confidentiality by network-based attacks, such as port scanning, botnets and spoofing attack. The port scanning can monitor the status of a service provisioning on a certain VM and may result in a denial of service. A botnet may be used to take over the data from a host machine. A control system can be set by a bot-master, while several machines may assist to steal private data. The spoofing attacks result in entity impersonation for malicious purposes. These attacks replace the IP address of a packet with the counterfeit one. Thus, a DNS spoofing attack can redirect traffic to an attacker's system. Private data stored on a cloud device can be stolen by malicious insider via two storage-based attacks, data scavenging and data deduplication. The data scavenging recovers removed data from a storage device, while the data deduplication occurs during minimization of storage and bandwidth requirements, when files and their contents may be identified. The applications running on a cloud may be attacked by injecting code to trace execution paths and use the information for malicious purposes. Furthermore, protocols and shared architectural components may also be used as a source for malicious activities. Three application-based attacks may be distinguished: malware injection and steganography attacks, shared architecture and web services and protocol-based attacks. Malicious code may be injected if a cloud platform supports an insecure interface for application development. If the malicious code is embedded within files and transmitted through the network, the steganography attack occurs. The execution path of the application can be traced and used to detect activities in shared architecture. The application-based attack may occur if the message headers of the implemented protocols are manipulated. VM based attacks often violate data protection (Mikavica and Kostić-Ljubisavljević, 2020a). In general, VM based attacks can be classified into cross VM side-channel, VM creation attacks, VM migration and rollback attacks and VM scheduler-based attacks (Khan, 2016). The VM side-channel attacks can extract cryptographic keys and other sensitive data from a VM under attack. Usually, the attacker's VM is placed at the same physical machine as the target VM. Malicious code can be inserted into a VM image during the VM creation. Thus, a virtual image management system is needed for detection and VM recovering. During VM migration from one physical machine to another, VM contents may become vulnerable. Hence, the log execution state being maintained for implementing a rollback may become accessible. Resource stealing or theft-of-service may occur due to VM scheduler based-attacks. VM security significantly affects the security of the cloud system. Therefore, security assessment and evaluation of its impacts on the cloud service performances are important issues to be solved. Cloud providers seek to improve cloud service performances while cloud customers expect high standards in cloud service provisioning at reasonable prices.

Pricing is another key issue in a cloud environment. In general, pricing mechanisms can be classified into static and dynamic. The static pricing mechanisms are widely adopted and involve fixed prices per billing cycle per VM. Despite their simplicity, these mechanisms do not support revenue maximization. The dynamic pricing mechanisms adjust prices according to the actual or forecasted dependences between the demand and supply. As a dynamic form

of pricing, auction mechanisms provide price variation by creating competition among cloud customers and allocate resources to the customers that value them the most. Cloud customers participate in an auction mechanism by submitting their bids that represent the maximum price they are willing to pay for requested resources. The major drawback of these mechanisms is the lack of any guarantees on minimum sustained availability. Cloud provider defines the prices for cloud resources. When the price exceeds the value of the bid, the cloud instance is terminated. Adequately set auctions can support cloud customers to bid truthfully. Selection of an appropriate bidding strategy is essential for customers and affects the performance metrics including costs, wait time and interruption rate. Lower bids can provide lower costs, but also deteriorate task completion time and interruptions. Therefore, bidding high is often recommended. The process of bidding in an auction is complex and often lacks transparency. Hence, dynamic pricing mechanisms are less accepted, despite lower prices compared to static pricing mechanisms. However, auctions are considered as an effective and promising solution to optimize the cloud provider's revenues. Various auction-based pricing mechanisms in the cloud environment are proposed including Uniform price auctions, Second-price auctions, Combinatorial auctions, Double auctions etc (Mikavica and Kostić-Ljubisavljević, 2018; Mikavica and Kostić-Ljubisavljević, 2020b).

Majority of the proposed pricing models are focused only on the resource pricing and allocation without a security assessment. The main contribution of this paper is the introduction of VM security modelling in the process of auction-based pricing and resource allocation. Depending on the guaranteed security level, cloud customers choose one of the three proposed bidding strategies. Two auction-based pricing mechanisms are analysed, Uniform price auction and Generalized-Second price auction. The paper aims to provide a comprehensive analysis and comparison of these pricing mechanisms depending on traffic load and customers' incentives to bid truthfully. Cloud provider's revenues are also observed. The remainder of the paper is organized as follows. A brief literature review on the security, pricing and bidding strategies in the cloud environment is provided in Section 2. Modelling of VMs' security level, bidding strategies and auction setting for the two observed auction mechanisms are introduced in Section 3. Experimental evaluations and results are given in Section 4. Finally, concluding remarks are presented in Section 5.

2. Literature Review

Security in a cloud environment is an essential aspect that requires comprehensive coordination across roles and it has to be implemented consistently. It comprises physical and application security and includes authentication, authorization, availability, confidentiality, integrity, incident response, security monitoring and security policy management (ITU-T Recommendation Y.3500, 2014). Since cloud resources are connected using an internal network, various attacks may increase delays in communication and disable network access (Mikavica and Kostić-Ljubisavljević, 2020a). Attacks on VMs and cloud services may violate the data protection or disable service provisioning for all cloud customers. Despite the increasing number of threats,

the corresponding countermeasures are also being developed. Some proposed solutions address attacks such as botnet and stepping-stone attacks (Kourai *et al.,* 2012). Furthermore, various cryptographic techniques can mitigate vulnerabilities in VM migration (Godfrey and Zulkernine, 2013) Cloud system performances are highly affected by security issues. Xu *et al.* (2018) point at two critical security factors: malicious attacks and the security protection mechanism. A hierarchical approach is used to model relations between security and cloud service performance. The results emphasize the importance of security in the modelling and evaluation of the Quality of Service (QoS). A comprehensive classification of attacks and corresponding countermeasures are provided by Hashizume *et al.* (2013).

Along with security, pricing and allocation of cloud resources have to be properly addressed. Dynamic pricing mechanisms are used to offer idle cloud resources at lower prices to improve resource utilization, and raise the prices if the demand increases (Wan *et al.,* 2016). Auction mechanisms are considered as a promising solution for dynamic cloud pricing (Toosi *et al.,* 2016). Appropriately set auctions provide incentives for cloud customers to bid the true values they are willing to pay for given resources and allocate those resources to the customers that value them the most (Zaman and Grosu, 2013). Furthermore, auctions create competition among cloud customers and modify the prices depending on the demand and supply on the cloud market. Thus, the market value of cloud resources can be efficiently determined, especially if relatively limited resources are allocated to a potentially large number of cloud customers (Chichin *et al.,* 2014). Auction-based pricing mechanisms set, on average, lower prices compared to static pricing mechanisms (Jung *et al.,* 2011; Kaminski and Szufel, 2015). Amazon EC2 Spot pricing, as a prominent example of auction-based pricing, provides savings over static pricing mechanisms up to 36% (Leslie *et al.,* 2013). Furthermore, customers' satisfaction is also significantly improved (Mikavica and Kostić-Ljubisavljević, 2020b). According to Shi *et al.* (2016), it is possible to establish fair interactions between cloud providers and customers under auction-based pricing mechanisms with appropriate market structure.

Closely related to cloud resource pricing is resource allocation. Various auction-based mechanisms for cloud resource allocation and pricing are proposed so far (Kumar *et al.,* 2017; Kumar *et al.,* 2018; Lu *et al.,* 2018). Sheikholeslami and Navimipour (2018) provided a comprehensive literature review of auction mechanisms for cloud resource allocation.

Baranwal *et al.* (2018) classified numerous auction-based pricing mechanisms for cloud resources. Most often used are one-sided, double-sided and combinatorial auctions. One-sided auctions provide a setup where bidders submit their bids without any insight into other bids. A bidder with the highest bid value wins in an auction. A well-known one-sided auction is Vickrey auction, also referred to as Second-price auction, where the resources are allocated to the bidder with the second-highest bid. Another prominent example of the one-sided auction in a cloud environment is the Uniform price auction (Zhang *et al.,* 2011). In this case, the provider allocates resources by the decreasing order

to the bids and determines the price that is equal to the lowest winning bid. The concept of the marginal bid (the highest unsuccessful bid) for cloud resource pricing and allocation under Second-price auction can also be established (Lin *et al.,* 2010). Double-sided auctions enable bidding for both cloud providers and cloud customers. When cloud providers can set their offers and cloud customers can place their bids at any time, the auction process is referred to as Continuous Double Auction. Kumar *et al.* (2017) provided a detailed study of double-sided auctions in cloud environment along with a framework for the future cloud market. It is also shown that double-sided auctions can be an effective pricing and allocation mechanism for two-sided markets. Combinatorial auctions can be applied if a cloud provider offers a group of resources as bundles, while cloud customers submit their bids. These auctions are considered as a convenient and efficient mechanism for all relevant participants in the cloud market. Two combinatorial auction-based mechanisms for the allocation of several VM instance types to several customers are proposed by (Zaman and Grosu, 2013). The first mechanism observes the situation with a few types of items and many instances of each type, while the second allocates resources depending on the customers' bids and the total number of items demanded. Afterwards, these mechanisms are compared to static pricing mechanisms. It is shown that the proposed mechanisms improve resource utilization and allocation efficiency, and provide high revenues for cloud providers as well. However, the customers' perspective is not considered.

An essential part of the auction process in the pricing and allocation of cloud resources is bidding. It is important to emphasize that the chosen bidding strategy affects costs, wait time and interruption rate (Karunakaran and Sundarraj, 2014). Lower bids potentially can decrease costs, but concurrently, metrics such as task completion time and interruption rate deteriorate. Cloud providers often suggest bidding high to decrease the possibility of cloud instance termination. Price-sensitive customers usually submit low bid values, thus indicating their willingness to pay only a low price for cloud resources. However, those VMs have low availability and high possibility of revocation if the market price increases more than the bid price. Frequent revocations decrease performances and lengthen deadlines. Therefore, an appropriate bidding strategy should minimize costs and deadlines, for a wide range of applications. Due to the high complexity of bidding, auction-based pricing mechanisms are not dominantly used in a cloud environment (Sharma *et al.,* 2017). Various bidding strategies are proposed to optimize cost-availability trade-offs (Sharma *et al.,* 2017; Mikavica and Kostić-Ljubisavljević, 2018). If a customer increases bid, the availability also increases at the expense of more pay per billing cycle. Furthermore, the availability of idle resources and costs are not sensitive to bidding for a wide range of bid values, since there are no penalties for bidding high. Revocations are inevitable when using cloud idle resources. Therefore, the frequency of revocations needs to be carefully considered in bidding. Sharma *et al.* (2017) suggest that cloud customers should not employ complex bidding strategies. Customers should rather choose adequate VM type to reduce the risk of revocation and apply the migration to other VMs when needed. This strategy could also reduce costs. Therefore, the appropriate

selection of VMs' type and fault tolerance policies are crucial in trade-offs between performances and costs.

As stated above, the majority of the proposed pricing models address the pricing and allocation of cloud resources without a security assessment. This paper aims to introduce security modelling into the auction-based process of pricing and allocation of cloud resources. Along with, various bidding strategies are proposed to analyse the cloud provider's revenues and losses in different scenarios.

3. Problem Statement

Suppose the physical and logical structure of the cloud system owned by a cloud provider as shown in Fig. 1.

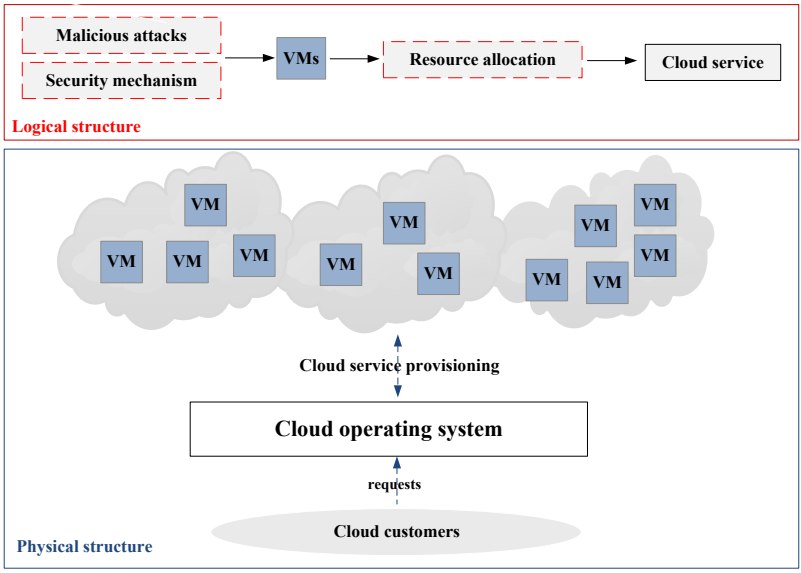

Fig. 1.
The Physical and Logical Structure of the Cloud System

The most important component of the observed system is the cloud operating system. This operating system is placed in the infrastructure level and manages cloud infrastructure, including virtual machines and equipment, back-end hardware and software resources. Moreover, the cloud operating system processes cloud customers' requests. In the service provisioning process, the customers' requests are sent to the suitable VMs for execution, while the results are sent back from VMs to the cloud operating system. The request for cloud service provisioning is satisfied if the task is processed and the correct result is sent back to the cloud operating system. Therefore, the availability of VMs is crucial for cloud service provisioning. The resource layer of the cloud system comprises all the hardware and software (storage, server infrastructure and virtual infrastructure). This layer is in charge of the organization of cloud resources

in the form of VMs. In general, VMs are individually accessible over the Internet and thus, highly vulnerable to malicious attacks. Allocation of customers' requests and the collection of results are performed at the application layer of the cloud operating system.

In the cloud system observed in this paper, access to the cloud VMs is provided in an auction-like process. Considering that a sufficient number of the participants in the market is needed for revenue maximization in long term (Mikavica and Kostić-Ljubisavljević, 2018), it is assumed that the number of cloud customers, denoted as M, is greater than the number of the available VMs. Without loss of generality, the analysis is executed into *N* consecutive time intervals. The number of cloud customers initiating the request for task execution can be modelled using a Poisson distribution with the two parameters, λ_h and λ_l for the periods of high and low traffic load, respectively (Mikavica and Kostić-Ljubisavljević, 2018). If the malicious attack occurs, a VMs' availability depends on the applied security mechanism. To initiate a certain VM for task completion, the cloud customer creates a bid. Submitting a bid, cloud customer defines the value of the bid, i.e. the maximum price per time slot that cloud customer is willing to pay for a given VM with the corresponding intensity level of the applied security mechanism. Once the auction process is finished, the VMs are allocated to the cloud customers with winning bids. The value that cloud customer pay for VM's initiation is not the value of the bid, but the value of the VM's price. The VM's price and the cloud provider's revenue depend on the applied auction mechanism. The procedure of bidding and VMs' allocation is depicted in Fig. 2 and explained in detail in the following subsections.

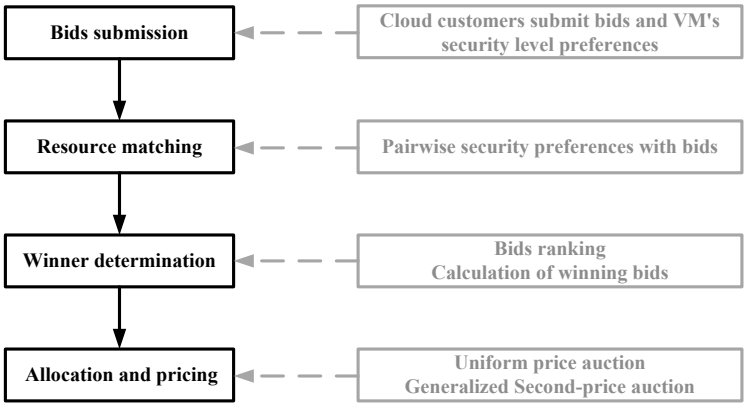

Fig. 2.
The Algorithm of Security-driven Auction-based pricing

3.1. The VMs' Security Modelling

VM security is an inevitable vulnerability for the cloud system. Evaluation of VM security and the analysis of previous malicious attacks along with the security mechanisms can improve the security of cloud systems. In general, malicious attacks are random. The theoretical modelling approach can just describe the randomness depending

on its characteristic of abstraction and the view of the comprehensive statistic (Xu *et al.,* 2018). When the availability of VMs is threatened by malicious attacks, it may fail the cloud customers' requests provisioning. Furthermore, the malicious attacks may reduce the number of available VMs and results in the overflow failure, if there are only a few available VMs. The majority of attacks are unorganized and spontaneous, with random arrival rate. The probability of a malicious attack is denoted as $p_m \in (0,1)$.

Implementation of different security mechanisms may protect the cloud system from malicious attacks. However, their application occupies a part of computing resources and reduces the resources that are used to process tasks. Also, the processing time of the tasks may be extended and overtime failure may occur. Therefore, the applied security mechanism affects the service performance and the availability of VMs. The occupation of computing resources by a security mechanism depends on the algorithm complexity or security level. Intensity can be used to describe the complexity of the algorithm or the security level (Xu *et al.,* 2018). It is assumed there are three intensities defined for security mechanism including high, middle and low. The higher the intensity is, the more complex the applied algorithm and the higher the security level are.

The total number of VMs is denoted as n. It is assumed that cloud resources are divided into trust zones (TZ), and all VMs in the same TZ apply the unitive security mechanism with the same intensity. We assume there are four TZs, TZ0, TZ1, TZ2, and TZ3. TZ0 has no security mechanism implemented. TZ1, TZ2 and TZ3 apply security mechanism of low, medium and high intensity, respectively. In each VM, only one task is provisioned at one time, and each task can be completed during a single time interval.

The probability that a VM is available is denoted as p_a^h, p_a^m and p_a^l for the VMs in the TZ with high, medium and low-intensity security mechanism, respectively. If no security mechanism is implemented, the probability of VM's availability is denoted as p_a^0. According to the provided security level of VMs within the TZs, it applies $p_a^0 < p_a^l < p_a^m < p_a^h$, where $p_a^0, p_a^l, p_a^m, p_a^h \in (0,1)$. The number of the available VMs in time interval $i \in [1, N]$ within TZ $k \in [0,3]$ is denoted by $n_{i,k}$. If the applied security mechanism failed to protect VMs' availability, it applies $\sum_{k=0}^{3} n_{i,k} \neq n$.

3.2. Bidding Strategies and VMs' Prices

To initiate a certain VM for task completion, the cloud customer creates a bid. Submitting a bid, cloud customer selects an appropriate security level for the task (cloud customer determines TZ with an adequate intensity of the security mechanism) and defines the value of the bid (the maximum price per time slot that cloud customer is willing to pay for the selected VM). Set of all bidders in time interval $i \in [1, N]$ is denoted as B_i. The bid of the cloud customer $j \in B_i$ in time interval $i \in [1, N]$ for the TZ $k \in [0,3]$ can be denoted as:

$$b_{i,j,k} = (v_{i,j}, k) \tag{1}$$

In (1), $v_{i,j}$ represents the value of the bid, i.e., the price that customer is willing to pay for VM in chosen TZ k with an appropriate security level. Also, cloud customers have no information on other customers' bids.

Cloud provider allocates the available VMs to cloud customers that value them the most.

Customers with the winning bids can initiate VMs and pay the value of the VM's price per time interval.

Depending on the applied auction mechanism and the chosen TZ, VMs' prices differ. Therefore, VMs' prices in TZ0, TZ1, TZ2, and TZ3 in time interval i, $i \in [1,\ N]$, are denoted as $P_{i,0}$, $P_{i,1}$, $P_{i,2}$, and $P_{i,3}$, respectively. These prices are unknown to cloud customers. However, it is assumed that VMs' prices in the previous time interval, $P_{i-1,0}$, $P_{i-1,1}$, $P_{i-1,2}$, and $P_{i-1,3}$, are publicly available. The greatest VM's price is set for the TZ with the highest security level (TZ3), while the lowest VM's price is set for the TZ with no security mechanism implemented. Therefore, it applies $P_{i,0} < P_{i,1} < P_{i,2} < P_{i,3}$.

Based on these prices, cloud customers select bidding strategy and place a bid. In this paper, three possible bidding strategies are introduced, namely, task-related bidding strategy, greedy bidding strategy, and random bidding strategy.

3.2.1. Task-related Bidding Strategy

Under this bidding strategy, cloud customers submit bids for VMs in selected TZ whose values are close to the corresponding VMs' prices in the previous time interval. Therefore, submitted bids in time interval i for a given TZ take values:

$$b^{I}_{i,j,k} \in \left[P_{i-1,k} - \delta, P_{i-1,k} + \delta\right], \quad i \in [1,\ N],\ j \in [1, |B_i|],\ k \in [0,3] \tag{2}$$

δ denotes a small variation of the VM's price in corresponding TZ in the previous time interval. The probability of choosing this bidding strategy is denoted as q^{I}.

3.2.2. Greedy Bidding Strategy

Considering that cloud customers pay the value of the VM's price defined in the auction process, and not the value of their bid, customers can choose greedy bidding strategy to ensure winning in the auction process and get the access to the targeted VM with the selected security level. Thus, customers place bids with greater values than the VM's price for chosen TZ in the previous time interval. Those bids can be expressed as follows:

$$b^{II}_{i,j,k} \in \left[P_{i-1,k+1} - \delta, P_{i-1,3} + \delta\right], \quad i \in [1,\ N],\ j \in [1, |B_i|],\ k \in [0,3] \tag{3}$$

Again, δ denotes a small variation of the VM's price in corresponding TZ in the previous time interval. It is noteworthy that this bidding strategy matches the task-related bidding strategy for the tasks requiring the security mechanism with the highest intensity. The probability of choosing the greedy bidding strategy is denoted as q^{II}.

3.2.3. Random Bidding Strategy

Random bidding strategy assumes that cloud customers place bids with values that are randomly selected in the range of VMs' prices in the previous time interval. Since cloud customers are unaware of the bid values placed by other bidders, this bidding strategy might be considered as truthful. Bid values under this bidding strategy can be expressed as follows:

$$b^{III}_{i,j,k} \in \left[P_{i-1,0} - \delta, P_{i-1,3} + \delta\right], \quad i \in [1,\ N],\ j \in [1, |B_i|],\ k \in [0,3] \tag{4}$$

Likewise previous bidding strategies, δ denotes a small variation of the VM's price

in corresponding TZ in the previous time interval. The probability of choosing the random bidding strategy is denoted as q^{III}. It applies $q^{I} + q^{II} + q^{III} = 1$.

3.3. Auction Mechanisms

Once bids are submitted for each TZ, the VMs' allocation is performed based on the set of winning bids, i.e. each cloud customer with winning bid can initiate VM with a required security level. Cloud customers payoffs differ depending on the applied auction mechanism. In this paper, Uniform price auction and Generalized Second-price auction are analyzed to obtain cloud provider's revenues in VMs' provisioning with several security levels. The set of winning bids for each TZ can be represented as follows:

$$W_{i,k} \in \left\{w_{i,1,k}, w_{i,2,k}, \dots, w_{i,n_{i,k},k}\right\}, \quad i \in [1,\ N],\ k \in [0,3] \tag{5}$$

In (5), $w_{i,1,k}$ represents the highest bid value for the VM in TZ $k \in [0,3]$ in time interval $i \in [1,\ N]$, $w_{i,2,k}$ represents the second-highest bid value, etc.

3.3.1. Uniform Price Auction

If Uniform price auction is applied, each winning bidder pays the same price equal to the lowest winning bid. Set of the winning customers' payoffs for TZ $k \in [0,3]$ in the time interval $i \in [1,\ N]$ under Uniform price auction can be represented as follows:

$$W_{i,k}^{U} \in \left\{w_{i,1,k}^{U} w_{i,1,k}, w_{i,2,k}^{U}, \dots, w_{i,n_{i,k},k}^{U}\right\}, \quad i \in [1,\ N],\ k \in [0,3] \tag{6}$$

Since all winning bidders pay the same price, it applies $w_{i,1,k}^{U} = w_{i,2,k}^{U} = \cdots = w_{i,n_{i,k},k}^{U} = w_{i,n_{i,k},k}$. Cloud provider's revenue under Uniform price auction in time interval $i \in [1,\ N]$ can be expressed as:

$$R_i^{U} = \sum_{k=0}^{3} \sum_{t=1}^{|W_{i,k}^{U}|} w_{i,t,k}^{U},\ i \in [1,\ N] \tag{7}$$

3.3.2. Generalized Second-price Auction

When Generalized Second-price auction is applied, the winning bidder pays the value of the next highest bid. Thus, set of winning customers' payoffs for TZ $k \in [0,3]$ in the time interval $i \in [1,\ N]$ under Generalized Second-price auction can be represented as follows:

$$W_{i,k}^{G} \in \left\{w_{i,1,k}^{G}, w_{i,2,k}^{G}, \dots, w_{i,n_{i,k},k}^{G}\right\}, \quad i \in [1,\ N],\ k \in [0,3] \tag{8}$$

Considering the rules of Generalized Second-price auction, it applies $w_{i,1,k}^{G} = w_{i,2,k}$, $w_{i,2,k}^{G} = w_{i,3,k}$, …, $w_{i,n_{i,k},k}^{G} = w_{i,n_{i,k}+1,k}$. Cloud provider's revenue under this auction mechanism in time interval $i \in [1,\ N]$ can be expressed as:

$$R_i^{G} = \sum_{k=0}^{3} \sum_{t=1}^{|W_{i,k}^{G}|} w_{i,t,k}^{G},\ i \in [1,\ N] \tag{9}$$

4. Performance Evaluation

To analyze the implementation of the two auction mechanisms in a cloud system with the possibility of malicious attacks, simulations in open source programming language Python 2.7 are performed in 50 iterations. Period of 30 days is simulated. Each day is divided into $N = 24$ time intervals. Time intervals 7-20 belong to the period

of high traffic load (Mikavica and Kostić-Ljubisavljević, 2018). The number of cloud customers that initiate requests for tasks' execution is modelled by Poisson distribution parameter $\lambda_h = 1.25$, and $\lambda_l = 0.75$, for the periods of high and low traffic load, respectively. There are 40 VMs, segmented into TZs, where each TZ comprises 10 VMs. The average number of cloud customers is 80. If a malicious attack occurs, the assumed probabilities that the applied security mechanism will protect the VM's availability are $p_a^l = 0.66$, $p_a^m = 0.75$, $p_a^h = 0.84$, for security mechanism with low, medium, and high intensity, respectively. Additionally, we assume that if a malicious attack occurs in the TZ0 (without any security mechanism implemented), the probability that the VM remains available is $p_a^0 = 0.5$. We observed situations when the probability of malicious attack at a VM takes the following values $\{0.05, 0.1, 0.2\}$. The initial VM's price for the TZ0 is chosen from publicly available data for Amazon EC2 spot instance m5n.xlarge in EU (Frankfurt) region and Windows operating system (Amazon EC2 Spot Pricing, 2020) and equals 2.256 $/h. Assumed initial VM's prices for low, medium, and high-security level are 2.820 $/h, 3.525 $/h, and 4.406 $/h, respectively.

We observe four scenarios depending on the dominant bidding strategy. Scenarios 1, 2 and 3 analyze setting where cloud customers predominantly choose the task-related bidding strategy ($q^I = 0.50, q^{II} = 0.30, q^{III} = 0.20$), the greedy bidding strategy $q^I = 0.30, q^{II} = 0.50, q^{III} = 0.20$, and the random bidding strategy $q^I = 0.20, q^{II} = 0.30, q^{III} = 0.50$. The fourth scenario analyzes the setting where all bidding strategies are equally possible $q^I = q^{II} = q^{III} = 0.33$. The parameter depicting the variation of the VMs' prices in the previous time interval is set as $\delta = 0.2$.

Table 1 shows average winning bids (expressed in $) for all observed bidding strategies in the periods of low and high traffic load if the Uniform price auction and Generalized Second-price auction mechanisms are applied for pricing and resource allocation. The results indicate that Generalized Second-price auction increases the values of winning bids on average for all observed scenarios. Therefore, Uniform price auction is more convenient from the cloud customers' perspective. Furthermore, the scenario with the dominant task-related bidding strategy provides the lowest winning bids in most cases. Notably, the dominant greedy bidding strategy (Scenario 2) is not recommended since it generates greater bids and customers' payoffs are increased. Moreover, the scenario where the majority of customers randomly chooses strategy (Scenario 3), is less convenient for customers compared to Scenario 2. When the possibility of malicious attack increases, the average winning bids slightly differ due to lower VMs' availability.

Table 1

Average Winning Bids [$]

Auction	p_m	Scenario	Low Traffic Load				High Traffic Load			
			TZ0	TZ1	TZ2	TZ3	TZ0	TZ1	TZ2	TZ3
Uniform Price Auction	0.05	1	1.693	2.450	2.913	3.468	2.483	2.907	3.558	4.109
	0.05	2	2.146	2.588	3.123	3.478	3.167	3.247	3.789	4.111
	0.05	3	2.203	2.511	2.850	3.098	3.222	3.283	3.669	3.932
	0.05	4	1.977	2.485	2.909	3.304	2.964	3.125	3.642	4.037
	0.1	1	1.704	2.448	2.903	3.479	2.484	2.907	3.555	4.110
	0.1	2	2.151	2.589	3.122	3.474	3.163	3.251	3.790	4.109
	0.1	3	2.213	2.510	2.855	3.099	3.223	3.288	3.669	3.929
	0.1	4	1.980	2.489	2.913	3.304	2.963	3.125	3.645	4.033
	0.2	1	1.703	2.446	2.909	3.474	2.482	2.908	3.556	4.107
	0.2	2	2.138	2.594	3.121	3.472	3.167	3.252	3.792	4.107
	0.2	3	2.204	2.512	2.852	3.095	3.229	3.283	3.673	3.932
	0.2	4	1.968	2.490	2.906	3.306	2.963	3.128	3.644	4.032
General. Second-price Auction	0.05	1	2.613	3.039	3.522	4.038	3.316	3.502	3.957	4.422
	0.05	2	3.106	3.301	3.746	4.038	3.802	3.840	4.184	4.422
	0.05	3	3.157	3.297	3.592	3.813	3.844	3.870	4.110	4.306
	0.05	4	2.951	3.187	3.588	3.936	3.674	3.735	4.067	4.372
	0.1	1	2.609	3.034	3.521	4.033	3.316	3.504	3.960	4.424
	0.1	2	3.101	3.300	3.741	4.034	3.798	3.834	4.184	4.421
	0.1	3	3.158	3.284	3.600	3.814	3.847	3.868	4.107	4.307
	0.1	4	2.952	3.204	3.584	3.939	3.672	3.734	4.066	4.374
	0.2	1	2.613	3.039	3.521	4.039	3.327	3.504	3.960	4.422
	0.2	2	3.105	3.298	3.740	4.039	3.806	3.840	4.184	4.423
	0.2	3	3.161	3.297	3.601	3.812	3.844	3.867	4.109	4.306
	0.2	4	2.954	3.194	3.592	3.936	3.671	3.736	4.067	4.374

Fig. 3 shows the average revenue per interval of an hour duration in both low and high traffic load that the cloud provider achieves per VM in each TZ with the appropriate security level. A1 stands for the Uniform price auction, while A2 stands for the Generalized Second-price auction. L and H indicate low and high traffic load, respectively. The revenues slightly decrease with the greater attack probability, in all observed scenarios. Scenario 3 (each cloud customer defines the value of the bid randomly) assures the greatest revenues in both Uniform price auction and Generalized Second-price auction, regardless of network traffic load. Moreover, Generalized Second-price auction provides greater revenues in all observed scenarios, under all circumstances.

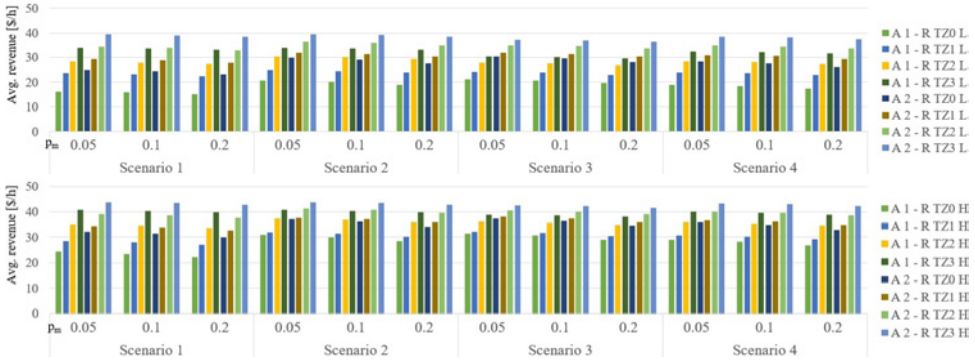

Fig. 3.
Average Cloud Provider's Revenues per Time Interval [$/h]

Table 2 shows average cloud provider's loss due to VMs' unavailability (expressed in $) for all observed bidding strategies in the periods of low and high traffic load and all observed scenarios under the two auction mechanisms. It appears that regardless of the chosen dominant bidding strategy, the cloud provider's loss is doubled as the probability of malicious attack increases. Higher intensity of the security mechanism assures lower losses; the lowest loss is attained for the TZ3 with the highest level of security protection. Furthermore, Generalized Second-price auction provides greater losses compared to Uniform price auction. It should be also noted that loss is doubled in the trust zone without security mechanism implemented for all observed cases and both auction mechanisms

Table 2
Average Cloud Provider's Loss due to VMs' Unavailability [$]

Auction	p_m	Scenario	Low Traffic Load				High Traffic Load			
			TZ0	TZ1	TZ2	TZ3	TZ0	TZ1	TZ2	TZ3
Uniform Price Auction	0.05	1	0.421	0.412	0.357	0.280	0.632	0.508	0.444	16.824
	0.05	2	0.503	0.436	0.376	0.270	0.787	0.547	0.466	16.630
	0.05	3	0.536	0.421	0.348	0.246	0.809	0.555	0.473	15.837
	0.05	4	0.478	0.419	0.362	0.271	0.745	0.527	0.452	16.381
	0.1	1	0.846	0.841	0.711	0.540	1.240	1.008	0.886	33.284
	0.1	2	1.051	0.890	0.753	0.559	1.578	1.104	0.961	32.797
	0.1	3	1.100	0.833	0.704	0.489	1.594	1.127	0.947	31.320
	0.1	4	0.976	0.855	0.725	0.533	1.459	1.055	0.908	32.106
	0.2	1	1.672	1.664	1.440	1.085	2.495	1.955	1.764	64.775
	0.2	2	2.115	1.699	1.533	1.096	3.143	2.228	1.902	65.241
	0.2	3	2.158	1.683	1.413	0.969	3.188	2.235	1.834	63.065
	0.2	4	1.928	1.684	1.450	1.038	2.949	2.166	1.807	66.457

Auction	p_m	Scenario	Low Traffic Load				High Traffic Load			
			TZ0	TZ1	TZ2	TZ3	TZ0	TZ1	TZ2	TZ3
General. Second-price Auction	0.05	1	0.652	0.512	0.433	0.303	0.832	0.595	0.494	17.992
	0.05	2	0.757	0.550	0.465	0.313	0.962	0.665	0.528	17.149
	0.05	3	0.775	0.574	0.432	0.291	0.941	0.641	0.506	17.370
	0.05	4	0.723	0.545	0.457	0.298	0.935	0.621	0.520	17.834
	0.1	1	1.295	1.023	0.868	0.637	1.640	1.206	0.969	34.978
	0.1	2	1.525	1.114	0.913	0.629	1.884	1.299	1.031	34.752
	0.1	3	1.574	1.076	0.893	0.578	1.935	1.305	1.001	34.641
	0.1	4	1.454	1.077	0.876	0.635	1.814	1.254	0.978	34.932
	0.2	1	2.567	2.041	1.721	1.290	3.332	2.369	2.036	70.554
	0.2	2	3.053	2.245	1.868	1.288	3.763	2.580	2.079	70.883
	0.2	3	3.099	2.202	1.780	1.211	3.798	2.645	2.058	69.371
	0.2	4	2.897	2.135	1.734	1.257	3.634	2.538	2.026	70.722

5. Conclusion

In this paper, the application of the two auction-based mechanisms, Uniform price auction and Generalized Second-price auction, for pricing and allocation of cloud resources, is addressed. The intensity of the applied security mechanism is introduced as a relevant parameter depicting the VM security level. Initiating a request for access to the VM, customers choose one of the three bidding strategies. Depending on the dominant bidding strategy, we observe several scenarios. Average winning bids, average revenues and average losses per VM are analyzed. The results show that Generalized Second-price auction achieves greater revenues, regardless of the chosen bidding strategy and regardless of the traffic load period, while Uniform price auction is more convenient from cloud customers' perspective. Furthermore, task-related bidding strategy is shown as the most convenient since it provides the lowest winning bids in the majority of cases. Higher intensity of the applied security mechanism generates higher cloud provider's revenues due to greater initial prices, and it lowers the cloud provider's losses. However, higher VM's security level requires more CPU occupied and increases costs for the cloud provider. This also affects service performances and needs comprehensive analysis, which is the subject of future research.

Acknowledgements

This work was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia [grant number TR 32025].

References

Amazon EC2 Spot Pricing. 2020. Available from Internet: <https://aws.amazon.com/ec2/spot/pricing/>.

Baranwal, G.; Kumar, D.; Raza, Z.; Vidyarthi, D.P. 2018. *Auction Based Resource Provisioning in Cloud Computing*. Spinger. 125p.

Chichin, S.; Vo, Q.B.; Kowalczyk, R. 2014. Truthful Market-based Trading of Cloud Services with Reservation Price. In *Proceedings of the IEEE International Conference on Services Computing (SCC 2014)*, 27-34.

Godfrey, M.; Zulkernine, M. 2013. A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud. In *Proceedings of the International Conference on Cloud Computing (CLOUD),* 163-170.

Hashizume, K.; Rosado, D.G.; Fernandez-Medina, E.; Fernandez, E.B. 2013. An Analysis of Security Issues for Cloud Computing, *Journal of Internet Services and Applications* 4(1): 1-13.

ITU-T Recommendation Y.3500. 2014. *Information technology – Cloud computing – Overview and vocabulary*.

Jung, D.; Chin, S.; Chung, K.; Yu, H.; Gil, J. 2011. *An Efficient Checkpointing Scheme Using Price History of Spot Instances in Cloud Computing Environment*. In: Altman E., Shi W. (eds) Network and Parallel Computing. Lecture Notes in Computer Science, 6985. Springer.

Kaminski, B.; Szufel, P. 2015. On Optimization of Simulation Execution on Amazon EC2 Spot Market, *Simulation Modelling Practice and Theory* 58(2): 172-187.

Karunakaran, S.; Sundarraj, R. 2014. Bidding Strategies for Spot Instances in Cloud Computing Markets, *IEEE Internet Computing* 19(3): 32-40.

Khan, M.A. 2016. A Survey of Security Issues for Cloud Computing, *Journal of Network and Computer Applications* 71: 11-29.

Kourai, K.; Azumi, T.; Chiba, S. 2012. A self-protection mechanism against stepping-stone attacks for IaaS clouds. In *Proceedings of the International Conference on Ubiquitous Intelligence Computing and International Conference on Autonomic Trusted Computing*, 539-546.

Kumar, D.; Baranwal, G.; Raza, Z.; Vidyarthi, D. P. 2017. A Systematic Study of Double Auction Mechanisms in Cloud Computing, *Journal of Systems and Software* 125: 234-255.

Kumar, D.; Baranwal, G.; Raza, Z.; Vidyarthi, D. P. 2018. A Survey on Spot Pricing in Cloud Computing, *Journal of Network and Systems Management* 26(4): 809-856.

Leslie, L.M.; Lee, Y.C.; Lu, P.; Zomaya, A.Y. 2013. Exploiting Performance and Cost Diversity in the Cloud. In *Proceedings of the IEEE Sixth International Conference on Cloud Computing,* 107-114.

Lin, W.Y.; Lin, G.Y.; Wei, H.Y. 2010. Dynamic Auction Mechanism for Cloud Resource Allocation. In *Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid)*, 591-592.

Lu, L.; Yu, J.; Zhu, Y.; Li, M. 2018. A Double Auction Mechanism to Bridge Users' Task Requirements and Providers' Resources in Two-Sided Cloud Markets, *IEEE Transaction on Parallel and Distributed Systems* 29(4): 720-733.

Mikavica, B.; Kostić-Ljubisavljević, A. 2018. Pricing and Bidding Strategies for Cloud Spot Block Instances. In *Proceedings of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 419-424.

Mikavica, B.; Kostić-Ljubisavljević, A. 2020a. *Security Issues of Cloud Migration and Optical Networking in Future Internet*. In M. Stojanović & S. Bostjančič Rakas (eds.), Cyber Security of Industrial Control Systems in the Future Internet Environment, 91-106. IGI Global.

Mikavica, B.; Kostić-Ljubisavljević, A. 2020b. *Auction-based Pricing in Cloud Environment*. In M. Khosrow-Pour (ed.), Encyclopedia of Organizational Knowledge, Administration, and Technologies, 86-97. IGI Global.

Sharma, P.; Irwin, D.; Shenov, P. 2017. Keep It Simple: Bidding for Servers in Today's Cloud Platforms, *IEEE Internet Computing* 21(3): 88-92.

Sheikholeslami, F.; Navimipour, N. J. 2018. Auction-Based Resource Allocation mechanisms in the Cloud Environments: A Review of the Literature and Reflection on Future Challenges, *Concurrency and Computation Practice and Experience* 30(16): 1-15.

Shi, W.; Zhang, L.; Wu, C.; Li, Z.; Lau, F. C. M. 2016. An Online Auction Framework for Dynamic Resource Provisioning in Cloud Computing, *IEEE/ACM Transactions on Networking* 24(4): 2060-2073.

Toosi, A. N.; Vanmechelen, K.; Khodadadi, F.; Buyya, R. 2016. An Auction Mechanism for Cloud Spot Markets, *ACM Transactions on Autonomous and Adaptive Systems* 11(1): 25-57.

Wan, J.; Zhang, R.; Gui, X.; Xu, B. 2016. Reactive Pricing: An Adaptive Pricing Policy for Cloud Providers to Maximize Profit, *IEEE Transactions on Network and Service Management* 13(4): 941-953.

Xu, H.; Qiu, X.; Sheng, Y.; Luo, L; Xiang, Y. 2018. A QoS-Driven Approach to the Cloud Service Addressing Attributes of Security, *IEEE Access* 6: 34477-34487.

Zaman, S.; Grosu, D. 2013. Combinatorial Auction-Based Allocation of Virtual Machine Instances in Clouds, *Journal of Parallel and Distributed Computing* 73(4): 495-508.

Zhang, Q.; Gurses, E.; Boutaba, R. 2011. Dynamic Resource Allocation for Spot Markets in Clouds. In *Proceedings of the 4th IEEE International Conference on Utility and Cloud Computing (UCC)*, 178-185.