A Security-Driven Approach for Energy-Aware Cloud Resource Pricing and Allocation

Branka MIKAVICA, Aleksandra KOSTIC-LJUBISAVLJEVIC
University of Belgrade-Faculty of Transport and Traffic Engineering, Vojvode Stepe 305, Belgrade, Serbia
b.mikavica@sf.bg.ac.rs

***Abstract*—Auctions are often recommended as effective cloud resource pricing and allocation mechanism. If adequately set, auctions provide incentives for cloud users' truthful bidding and support cloud provider's revenue maximization. In such a cloud system, resources are offered via an auction mechanism as Virtual Machines (VMs). Due to the virtualization of the cloud system, VMs' security becomes a critical factor. However, security requirements are often in contrast with performance requirements since the operation of security mechanism inevitably consumes a certain amount of Central Processing Time (CPU) and memory. Thus, delays and energy consumption increase. In this paper, we propose a novel simulation model based on a truthful auction mechanism to address revenues, security, and energy consumption in a cloud system. The VMs security modeling is introduced to assess the security level of VMs. A Vickrey-Clarke-Groves (VCG) driven algorithm is established for winner determination. The proposed simulation model is used to observe cloud provider's revenues, lost revenues, cloud users' task rejection rate and energy consumption depending on the offered security level. This model supports decision making in terms of investments in security and selection of security scenario that maximizes revenues and minimizes task rejection rate and energy consumption.**

***Index Terms*—decision making, energy consumption, security, simulation, virtual machining.**

I. INTRODUCTION

The cloud computing paradigm provided a global revolution in the IT industry due to its powerful resource integration and computing capabilities. The Infrastructure-as-a-Service (IaaS) cloud deployment model shows the ever-increasing adoption across several industry verticals to meet the cloud users' demands through virtualization. Major advantages of virtualization comprise availability, hardware independence, and security. Computing resources, storage, networking-related services, or processing power are provided by cloud providers, such as Amazon EC2, Microsoft Azure, Google cloud, VMware, Salesforce, etc. Recently, hypervisor-based virtualization technologies, such as VMware ESXi, XenServer, KVM, and Microsoft's Hyper-V become very popular in IaaS [1]. In general, cloud resources are provided in the form of virtual machines (VMs). Multiple VM instances can be deployed on a single physical server (host), thus improving the utilization of resources and increasing the return on investment [2].

Due to virtualization, VM security is a new factor that has to be addressed. Most cloud-specific attacks occur through compromised VM. There are numerous types of VM attacks including VM side channel attack, VM attack through hypervisor (HV), live VM attack, disk injection to live VM, VM migration attack, etc. VM side channel attack is possible when two or more VMs share the same hardware [3]. Thus, the attacker can extract information from the target VM by observing the hardware's behavior. In the case of a VM attack through the HV, the attacker uses malware or performs spearfishing and surveillance to obtain valid user credentials from a compromised VM. Live VM attack occurs if the attacker illicitly obtains the credentials from outside the cloud to gain regular access to a VM. Disk injection to live VM attack occurs when the attacker obtain access to target data by placing malicious code in the storage of the targeted VM [4]. Since VMs are frequently migrated to prevent the overloading of physical servers and to optimally allocate workloads to available resources, the attacker may abuse the exposure of a VM during VM migration operations in the cloud. Thus, useful information is extracted from the captured VM and is used to compromise additional VMs. When VMs are threatened by malicious attacks, VMs may fail to process cloud users' tasks. Depending on the attacks' severity, the number of the available VMs may be reduced, resulting in overflow failure. Implementation of security mechanisms may protect VMs from failures. However, those mechanisms consume a part of Central Processing Unit (CPU) resources, and potentially, extend the processing time of the tasks. Appropriate security evaluation can support efficient resource allocation and improves cloud users' experience.

Resource allocation and pricing are fundamental issues in a cloud environment. IaaS providers offer pre-configured VMs via multiple pricing strategies. For example, Amazon EC2 has adopted on-demand, saving plans, reserved instances, and spot pricing. The majority of cloud providers use a fixed pricing strategy, charging a fixed price for each VM, while the total payment depends on the time of usage. Despite the simplicity, fixed pricing mechanisms do not support dynamic change in demand and supply. Auctions are considered as a promising solution to improve efficiency and enable the fair distribution of resources to the cloud users that value them the most [5].

To maximize revenue, the cloud provider often prefers to allocate as many VMs as possible, thus significantly increasing energy consumption due to a large number of active hosts [6]. Concurrently, energy consumption is the major impediment in cloud data centers, and it is measured at the host level. A large amount of energy is consumed in periods of low traffic load [2]. Furthermore, idle hosts consume up to 70% of their peak energy consumption. Significant energy savings can be achieved by using resource allocation, scheduling, and VM consolidation

This work was supported by the Ministry of Education, Science and Technological Development of Serbia.

Digital Object Identifier 10.4316/AECE.2021.04011

techniques [2], [7-10]. Since the energy consumption is a linear relation of the CPU utilization [11], implementation of a security mechanism can further increase the energy consumption. To overcome these challenges, we propose a novel simulation model for balancing the multi-objective trade-offs between the cloud provider's revenue, security level assessment, and energy consumption estimation.

The main contributions of this paper are the following: (i) we introduce a VM security modeling where the complexity of the security mechanism and the malicious VM attack are the two critical factors affecting the VM's availability; (ii) implementation of a truthful auction-based mechanism that satisfies individual rationality and budget-balancing to observe the cloud provider's revenues; (iii) depending on the chosen security scenario, we estimate energy consumption, where the upper CPU utilization threshold is used to prevent hosts' overloading.

The remainder of the paper is organized as follows. Section 2 presents the related works on security, auction-based cloud resource pricing and allocation, and energy consumption in a cloud system. The system model and problem formulation comprising security modelling, VCG-based auction mechanism for pricing and allocation and calculation of revenues, lost revenues, rejection rate and energy consumption are presented in Section 3. The evaluation of the proposed model is provided in Section 4. In Section 5, we discuss the simulation results under various evaluation parameters. Finally, Section 6 provides concluding remarks and some future research directions.

II. Related Work

The security-related challenges in a cloud environment play an important role in the wider acceptance of cloud services. Main cloud computing security factors, threats, and challenges are summarized by [12]. Several studies on cloud system security are related to the effects of security mechanism implementation, or malicious attacks [4], [13-14]. Thus, a Quality of Service (QoS)-driven approach addressing effects of the overhead imposed by the security mechanisms on the service performance in the cloud environment is proposed in [13]. In [4], relations between security and the service performance are analyzed depending on the number of VMs and the service rate, where relevant factors are the security mechanism and the malicious attack. A pricing mechanism for the security risk and QoS assessment under persistent threats in the cloud-enabled Internet of Controlled Things (IoCT) is performed through a contract-based FlipCloud game in [14].

Auction-based cloud allocation and pricing strategies are widely studied in the literature. A comprehensive survey of auction-based mechanisms for cloud resource allocation is provided by [15]. Various approaches are proposed, including one-sided, double-sided, combinatorial auctions, and their variations [16]. Vickrey-Clarke-Groves (VCG) auction mechanism is one of the most commonly used mechanisms and provides a socially optimal solution [17]. Relations between security and cloud resource pricing and allocation are studied in [18-19]. A Dominant-Strategy Incentive-Compatible (DSIC) auction mechanism that gives incentives to cloud users to reveal their actual resource provisioning requests and security valuations is proposed by [18]. This mechanism follows a greedy allocation rule, where cloud users are prioritized according to their valuation of the security. The results show acceptable performance compared to the offline VCG mechanism. Various cloud users' bidding strategies for various VM's security levels under the two auction-based pricing mechanisms, Uniform-price auction and Generalized Second-price auction are analyzed in [19].

An effective VM allocation and pricing mechanism should not only aim at revenue maximization but also reduce the energy consumption of the hosts used for running cloud users' tasks. To reduce energy consumption, bin packing-based static resource allocation [20-21] and threshold-based dynamic resource consolidation can be used [22-25]. Some solutions are proposed to tackle both revenue maximization and energy consumption [26-27]. An efficient decentralized multiagent-based approach for VM allocation and minimization of the energy consumption is proposed in [28]. An online truthful double auction mechanism addressing multi-objective optimization between energy, revenue, and performance in IaaS is proposed in [1]. The authors apply weighted bipartite matching for winner determination and a VCG-driven algorithm for pricing.

In this paper, the proposed simulation model gathers security, pricing, and energy consumption. To the best of our knowledge, this is the first paper addressing the following aspects jointly: (i) security modeling, where the complexity of the security mechanism and malicious attacks are used to observe various security scenarios; (ii) truthful auctioning while considering obtained revenues, and (iii) energy consumption estimation for proposed security scenarios.

III. System Model and Problem Statement

In this section, we discuss the system model and formulate the problem. Fig. 1 shows an overview of the observed cloud system architecture. An essential segment of the observed cloud model is the Cloud Operating System (COS). This segment manages the virtual infrastructure of cloud resources including VMs, virtual switches, etc., back-end hardware and software, and processes cloud users' tasks.

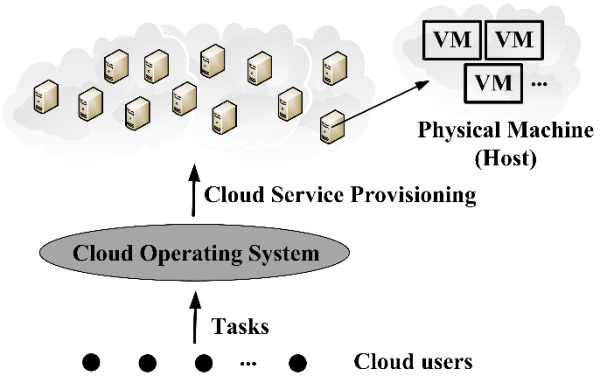

Figure 1. Cloud system physical architecture

Cloud resources are offered to cloud users in the form of pre-configured VM instances. In the cloud system, more than one heterogeneous VMs can be installed on a host. Each VM and each host are characterized by corresponding parameters including CPU defined in Million Instructions

per Second (MIPS), memory, and network bandwidth.

In general, VMs are individually accessible over the network and thus, VMs are vulnerable to malicious attacks. When the availability of VMs is threatened by malicious attacks, VMs may fail to process cloud users' tasks. Attacks may also reduce the number of available VMs. Implementation of security mechanisms in VMs may alleviate the effects of malicious attacks. However, such a mechanism consumes a part of CPU resources, memory, storage, and decreases the capacity used to process cloud users' tasks. This may extend the processing time and result in overtime failure. Since energy consumption mainly depends on CPU utilization, in this paper we take only this parameter for further consideration. It should be noted that the CPU occupation by a security mechanism depends on its algorithm complexity or security level. Similar to [4], we use the term intensity to describe the algorithm complexity or security level of the implemented security mechanism.

A. Security Modeling

In this paper, we divide all hosts and their VMs into several Trust Zones (TZs). The term TZ is firstly introduced by [3] and represents a combination of network segmentation and identity access management controls that define physical, logical, or virtual boundaries around network resources. TZs aim to facilitate the management and processing of different tasks in a cloud environment [3-4]. A TZ can be deployed using physical devices, virtually by firewall and switching applications, or using both physical and virtual tools [3]. Cloud network segmentation within a TZ is depicted in Fig. 2. Network segments are isolated by physical or virtual Network Interface Cards (NICs). This approach is based on the virtual networking capabilities offered by VMware and provides a hybrid strategy that comprises physical and virtual firewall barriers to protect data in TZ [3]. Similar security interpretation can be found at Amazon Web Virtual Private Clouds (Amazon VPC).

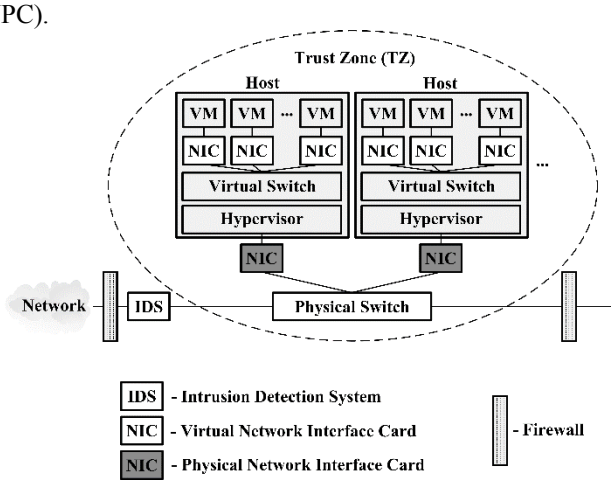

Figure 2. Cloud system segmentation within a TZ

There are numerous options for configuring, segmenting, and implementing security controls to a cloud system. An effective cloud security system comprises Intrusion Detection Systems (IDSs), keystroke logging, reverse web proxy servers, Security Incident Event Managers (SIEMs), and other protection systems. The security of a TZ relies on a correct configuration of domain controllers, firewalls, switches, and routers that enable segmentation and protect access to the cloud network.

For simplicity, we assume that all VMs have the same computation and storage characteristics. The analysis is performed in N consecutive time slots. Similar to [4], we assume that all VMs within one TZ apply the unitive security mechanism with the same intensity. There are three intensities defined for security mechanism: high, middle, and low. Higher intensity of the security mechanism means higher security level and higher complexity of the implemented algorithm. Depending on the provided security level, we distinguish four TZs: TZ0, TZ1, TZ2, and TZ3. The highest security protection is provided in TZ0, where all VMs apply the security mechanism with high intensity. Following that, VMs in TZ1 and TZ2 apply the security mechanism with medium and low intensity, respectively. VMs in TZ3 do not apply security mechanism and there are no guarantees of security protection. Most attacks are spontaneous, unorganized, with a random arrival rate, according to [4]. The probability that a VM will be threatened by a malicious attack is denoted by $p_a \in (0,1)$. $\beta_j \in (0,1)$ denotes the probability that a VM remains available under a malicious attack, where $j \in \{0, 1, 2, 3\}$ denotes the TZ to which the given VM belongs to. Each TZ j comprises m_j VMs at the beginning of each time slot. A lower security level induces a higher probability of a successful attack on a VM in the corresponding TZ. Thus, $\beta_0 > \beta_1 > \beta_2 > \beta_3$.

B. Auction Mechanism

The dynamic cloud resource allocation and pricing is performed through a VCG-based auction mechanism. To initiate a VM in a certain TZ for task execution, the cloud user creates a bid. Submitting a bid, the cloud user chooses a VM with a preferred security level (i.e., cloud user defines a TZ), and the value of the bid (i.e., cloud user defines its willingness to pay for selected VM in a given time slot). In this paper, the terms cloud user and bidder will be used interchangeably.

The probability that a cloud user chooses a VM in the TZ j in an auction process is denoted by $\phi_j \in (0,1)$. Set of all bidders in the time slot $i \in [1, N]$ for the TZ j is denoted by B^i_j. All bids are placed at the beginning of each time slot, and bidders have no information on other users' bids. The arrival rate of bidders initiating the request for task execution can be modelled using a Poisson distribution with the parameters λ_h and λ_l for the period of high and low traffic load, respectively [29].

We assume that each cloud user's task can be completed within a single time slot, and each cloud user bids for a single VM. Additionally, each cloud user's task is characterized by the amount of the VM's CPU it occupies. This parameter can be defined in the task classification process based on the configurations of the task and historical logs. A similar process can be found in [30]. Thus, each cloud user $b^i_j \in B^i_j$ can be described as follows:

$$b^i_j = \left(\upsilon_{b^i_j}, \ \rho_{b^i_j} \right), \ \upsilon_{b^i_j} \in (0, p_{o,j}] \tag{1}$$

where $\upsilon_{b_j^i}$ is the bidder's willingness to pay for a VM in the TZ j, while $\rho_{b_j^i}$ is the CPU occupation rate of the cloud user's task for the VM in the TZ j. We assume that $\upsilon_{b_j^i}$ depicts the bidder's true valuation for the task execution. The assumed maximum bid value is the on-demand price for the given VM initiation denoted as $p_{o,j}$. Once the bids are placed, the set of winning bids can be determined. At first, the bids are sorted in the nonincreasing order by the values of the bids, as indicated in (2). Set of the winning bids in time slot i for the TZ j is denoted by W_j^i, and it applies:

$$\omega_{l_j}^i \geq \omega_{l_j+1}^i,\ l_j \leq m_j,\quad \omega_{l_j}^i, \omega_{l_j+1}^i \in W_j^i \tag{2}$$

where l_j denotes the position of the bidder in the W_j^i,. Based on the bids placed, the cloud provider matches available resources and demand. The pseudo-code describing this procedure of winners' determination is shown in Algorithm 1. Afterwards, the cloud provider performs resource allocation and pricing.

Algorithm 1 Winner determination

Input: m_j, B_j^i
Output: W_j^i
1: **for each** $i \in [1, N]$ **do**
2: **for each** $j \in [0, 3]$ **do**
3: sort B_j^i in nonincreasing order of bid value
4: **if** length of $B_j^i \leq m_j$ **then**
5: $W_j^i \leftarrow B_j^i$
6: **else**
7: **for each** $l_j \in [1, m_j]$ **do**
8: Add $W_j^i \leftarrow B_j^i$
9: Return W_j^i

The price that each winning cloud user pays is determined using the VCG-based auction, where each winning bidder pays the value of the next highest bid. If the number of bidders in current time slot for a given TZ is less or equal to the number of the available VMs, the last bidder pays the value of its bid. Thus, if all VMs are available, i.e., there are no malicious attacks, or the security mechanism prevented failure due to the attack, the cloud provider's revenue per each VM can be expressed as follows:

$$p_{j,k_j}^i = \begin{cases} \omega_{k_j+1}, k_j < \left|B_j^i\right| \\ \omega_{k_j}, k_j = \left|B_j^i\right| \\ 0, k_j > \left|B_j^i\right| \end{cases}, \forall k_j \in [1, m_j]\ \omega_{k_j}^i, \omega_{k_j+1}^i \in W_j^i \tag{3}$$

The cloud provider's revenue, denoted by Θ, depends on the VMs' availability and the placed bids in the given time slot, and it can be expressed as follows:

$$\Theta = \sum_i \sum_j \sum_{kj} \gamma_{j,k_j}^i \cdot p_{j,k_j}^i \tag{4}$$

where, γ_{j,k_j}^i is a binary parameter that takes the value of 0 if the VM k_j is unavailable due to the malicious attack in the current time slot, and 1 otherwise. We assume that each VM is available at the beginning of each time slot. Therefore, the total number of rejected cloud user's requests can be expressed as follows:

$$\Psi = \sum_i \sum_j \sum_{k_j} \gamma_{j,k_j}^i \tag{5}$$

Another important indicator for the cloud provider in an insecure environment is the lost revenue, i.e., revenue that would be gathered if there were no failures due to malicious attacks. The lost revenue can be expressed as follows:

$$\Delta = \sum_i \sum_j \sum_{kj} \left(1 - \gamma_{j,k_j}^i\right) \cdot p_{j,k_j}^i \tag{6}$$

The pseudo-code showing the security-driven VCG-based calculation of revenue, lost revenue and number of rejected requests for each TZ is shown in Algorithm 2.

Algorithm 2 Security-driven VCG-based calculation

Input: B_j^i, W_j^i
Output: Θ, Ψ, Δ
1: **for each** $i \in [1, N]$ **do**
2: **for each** $j \in [0, 3]$ **do**
3: **for each** $k_j \in [1, m_j]$ **do**
4: $\gamma_{j,k_j}^i \leftarrow 1$
5: **if** $k_j <$ length of B_j^i **then**
6: $p_{j,k_j}^i \leftarrow \omega_{k_j+1}$
7: **elif** $k_j =$ length of B_j^i **then** // $\omega_{kj}^i \geq \omega_{kj+1}^i \in W_j^i$
8: $p_{j,k_j}^i \leftarrow \omega_{k_j}$
9: **else**
10: $p_{j,k_j}^i \leftarrow 0$
11: **if** k_j is unavailable due to malicious attack **then**
12: $\gamma_{j,k_j}^i \leftarrow 0$; $p_{j,k_j}^i \leftarrow 0$
13: Calculate revenue using (4)
14: Calculate number of rejected requests using (5)
15: Calculate lost revenue using (6)
16: Return Θ, Ψ, Δ

C. *Energy Consumption*

Each TZ j comprises τ_j hosts. A binary parameter $\delta_{q_j}^{k_j}$ is used to indicate whether a VM k_j is placed to the host $q_j \in (1, \tau_j)$, when it takes value of 1, and 0 otherwise. Each VM can be placed on at most one host. Therefore, $\sum_{q_j} \delta_{q_j}^{k_j} = 1$. The CPU capacity in MIPS of each host is denoted by σ_{q_j}. Hosts can be in an active or idle state. Power consumption of the host q_j is denoted by $\pi_{q_j,idle}$ and $\pi_{q_j,active}$ for the idle and active state, respectively. An idle host is being activated only if the capacity of an active host is exceeded. Thus, the number of active hosts is reduced. We assume there are no violations of the Service Level Agreement (SLA), and no penalties. Another important assumption is that VMs are not overloaded. Therefore, we introduce the parameter $\chi \in (0,1)$ representing a threshold of VMs' CPU utilization. The CPU is found to consume the maximum energy of a host compared to other

system resources [11]. Hence, the total energy consumption can be expressed as follows:

$$\Pi = \sum_i \sum_j \sum_{q_j} \left[\pi_{q_j,active} \cdot U^i_{q_j} + \pi_{q_j,idle} \cdot \left(1 - U^i_{q_j}\right) \right] \quad (7)$$

In (7), $U^i_{q_j}$ denotes the CPU utilization of a host q_j in the time slot i, and it can be expressed as follows:

$$U^i_{q_j} = \frac{\sum_j \delta^{k_j}_{q_j} \cdot (1-\gamma^i_{j,k_j}) \cdot \chi \cdot \eta_{k_j} \cdot \left(1-\rho^s_j-\rho_{b^i_j}\right)}{\sigma_{q_j}} \quad (8)$$

where, η_{k_j} denotes the VM's k_j CPU capacity (in MIPS), ρ^s_j denotes the CPU occupation rate of the running security mechanism in each VM in the TZ j, and $\rho_{b^i_j}$ is defined in (1). The pseudo-code describing the security-driven calculation of energy consumption is shown in Algorithm 3.

Algorithm 3 Security-driven calculation of energy consumption

Input: τ_j, m_j, B^i_j, W^i_j, σ_{q_j}, η_{k_j}, $\pi_{q_j,idle}$, $\pi_{q_j,active}$, χ, ρ^s_j
Output: Π
1: **for each** $i \in [1, N]$ **do**
2: **for each** $j \in [0, 3]$ **do**
3: **for each** $q_j \in [1, \tau_j]$ **do**
4: **for each** $k_j \in [1, m_j]$ **do**
5: $\gamma^i_{j,k_j} \leftarrow 1$; $\delta^{k_j}_{q_j} \leftarrow 0$
6: **if** k_j is unavailable due to malicious attack **then**
7: $\gamma^i_{j,k_j} \leftarrow 0$
8: **if** k_j is placed to the host q_j **then**
9: $\delta^{k_j}_{q_j} \leftarrow 1$
10: Calculate hosts' utilization using (8)
11: Calculate energy consumption using (7)
12: Return Π

IV. Performance Evaluation

To analyze the proposed scenarios, we conducted a set of simulation experiments in the open-source programming language Python 3.7 in 1000 iterations.

A. Simulation Setup

To investigate the overall performance of the proposed auction-based mechanism and the effects of security modeling on pricing and energy consumption, we set several scenarios. The analysis comprises $N=24$ time slots of one-hour duration. Time slots from $i=7$ up to $i=20$ belong to the period of high traffic load [29].

The average number of cloud users takes values from the set (1000, 1500, 3000). The number of cloud users initiating requests in the period of high traffic load is modeled by the Poisson distribution parameter $\lambda_h=1.25$, while the period of low traffic load is modeled by the Poisson distribution parameter $\lambda_l=0.75$ [19].

Cloud users choose TZ j with the probability Φ_j=0.25. There are 1200 VMs available at the beginning of each time slot. These VMs can be placed into 600 hosts. Depending on the VM allocation per TZ, we set 6 scenarios, as described in Table 1.

TABLE I. ALLOCATION OF VMS PER EACH TZ

Scenario	The number of VMs per TZ			
	TZ0	TZ1	TZ2	TZ3
1. Equal VM allocation	300	300	300	300
2. The highest security	540	320	220	120
3. High security	420	250	170	360
4. Medium security	300	200	100	600
5. Low security	180	110	70	840
6. The lowest security	60	36	24	1080

For simplicity, we assume that all hosts belong to a single type, namely HP ProLiant ML110 G5 (dual core CPU with 2660 MIPS per core, 4 GB RAM). The analysis can easily be extended to a more heterogeneous environment. $\pi_{q_j,idle}$ for the observed host is 93.7 Watts, while $\pi_{q_j,active}$ is 135 Watts. More details about power consumption for the host's various CPU utilization can be found in [11]. Each VM has 2500 MIPS single core, 0.85 GB RAM. The threshold for preventing a VM's overloading is set at χ=0.9, meaning that up to 90% of VM's CPU capacity can be allocated to cloud user's task execution.

The probability of a VM malicious attack takes values from the set $p_a=\{0.0,0.1,0.2,0.3\}$. Simulation parameters relevant for TZs are listed in Table 2. Values for the CPU occupation rate and the probability of VM's availability are in accordance with [4]. Selected VMs' on-demand prices are in the range of Amazon EC2 prices for on-demand VM instances.

TABLE II. SIMULATION PARAMETERS FOR TZS

Parameter	Trust Zones			
	TZ0	TZ1	TZ2	TZ3
Security mechanism's intensity	High	Medium	Low	-
CPU occupation rate of the security mechanism, ρ^s_j [%]	35	21	2	-
Probability of VM's availability, β_j	0.84	0.75	0.66	0.50
VM's on-demand price per time slot $p_{o,j}$, [$]	0.085	0.0425	0.0212	0.0106

B. The Cloud Provider's Average Revenue

The cloud provider's revenues depend on the number of cloud users, i.e., bidders, and on the VM allocation per TZ. The average revenue per time slot also differs for the periods of low and high traffic load. Furthermore, security conditions in the cloud environment affect provider's revenues significantly. In general, as demand increases average revenues per time slot are higher, as shown in Fig. 3. If the cloud environment is highly secure and the probability of a malicious attack is low, revenues increase. In a sparse situation, when there are fewer bidders than available VMs, the greatest revenue is provided for the low security scenario. Even if the probability of a malicious attack increases, the obtained revenues are the most preferred ones. The lowest revenues are obtained for the scenario with the lowest security level. However, when the demand exceeds the number of the available VMs, the scenarios with equal distribution of VMs per TZ and high

security scenario provide the greatest revenues in the period of low traffic load. In the period of high traffic load, the scenarios with high and the highest security level are preferred.

C. The Cloud Provider's Lost Revenue

The cloud provider's lost revenue is mainly affected by security issues. Fig. 4 shows the cloud provider's average lost revenue per time slot in both low and high traffic loads, for all observed scenarios, and various probabilities of malicious attack occurrence (excluding the situation without attacks, when lost revenue equals 0 $/h). It appears that scenarios with medium, low, and the lowest security level provided are more preferable in terms of lost revenue. This is due to the lower upper bound for bidding, i.e., on-demand prices are lower for VM instances with lower intensity of the security mechanism implemented. Thus, lower lost revenue would be obtained if there were no malicious attacks. Lost revenue increases if the cloud environment is less trusted.

D. Average Rejection Rate

The rejection rate is directly affected by the chosen scenario for VMs' allocation per TZ and the frequency of failures due to malicious attacks. Fig. 5 shows the average rejection rate per time slot in high, and low traffic load, expressed in [%]. The case when there are no malicious attacks is excluded when the rejection rate equals 0%. As the probability of a malicious attack increases, the average rejection rate also increases.

However, the investment in security by allocating more VMs in the TZ with a reliable security mechanism can significantly reduce the rejection rate. Thus, scenarios with the highest and high security level assure acceptable rejection rates, even if the cloud environment is prone to malicious attacks.

E. Average Energy Consumption

Energy consumption per time slot mainly depends on the chosen security scenario. The higher intensity of a security mechanism implies higher VM's CPU occupation. This directly increases the power consumption of the host. Therefore, scenarios with improved security consume greater power on average. Fig. 6 shows energy consumption in kWh per time slot for both high and low traffic load. With the increase of the average number of bidders, the number of idle hosts decreases. Also, a less secure environment with a greater probability of a malicious attack causes more failures and lowers energy consumption. This is an undesired situation, so a compromising solution is necessary.

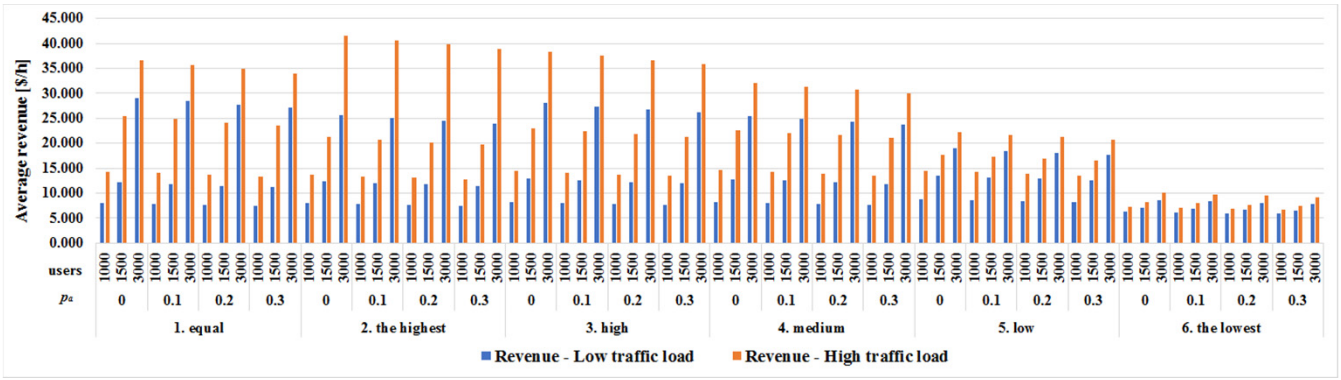

Figure 3. The average cloud provider's revenues per time slot in the periods of low and high traffic load in [$/h]

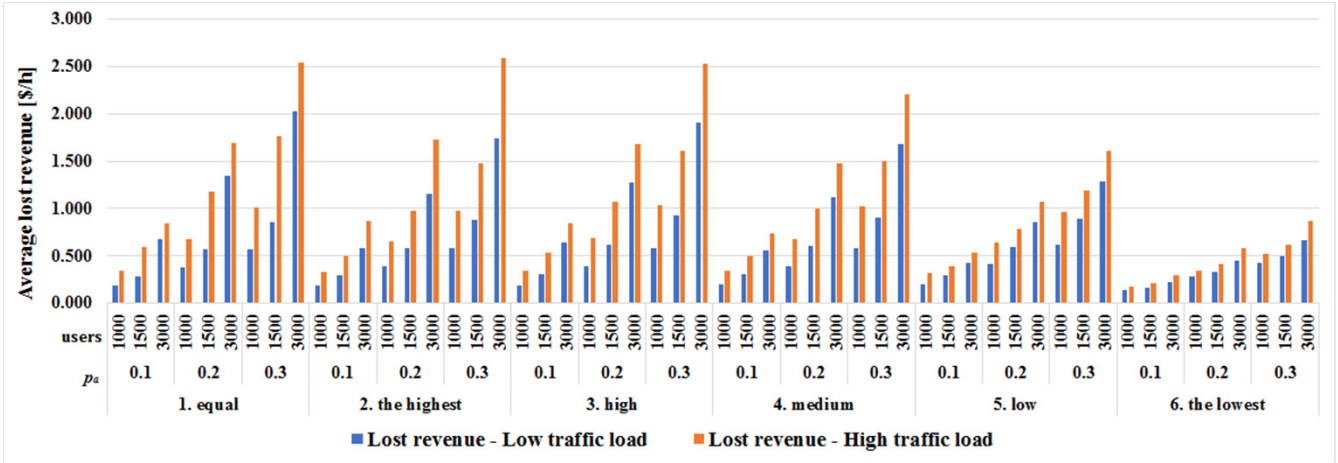

Figure 4. The average cloud provider's lost revenue per time slot in the periods of low and high traffic load in [$/h]

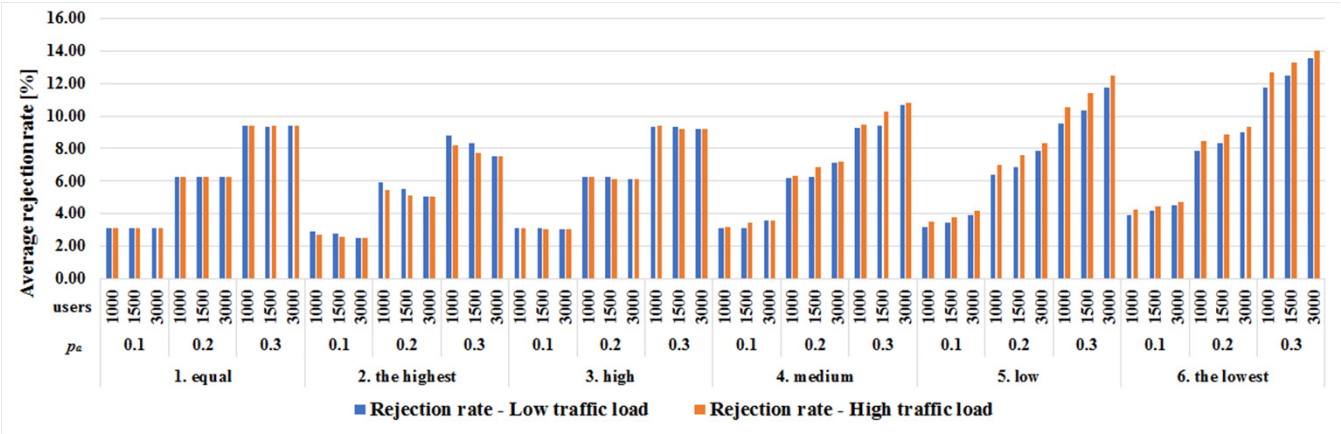

Figure 5. The average rejection rate per time slot in the periods of low and high traffic load in [%]

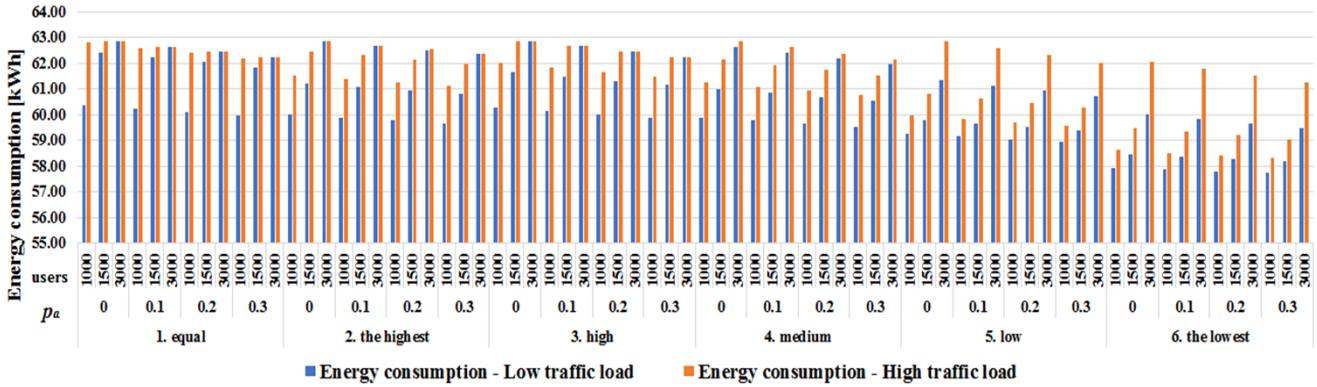

Figure 6. The average energy consumption per time slot in the periods of low and high traffic load in [kWh]

V. Discussion

Revenue maximization, security improvements and optimization of energy consumption are opposite goals from cloud provider's perspective. Investment into security improvement is costly, but the preferable solution. However, the highest security level provided is not always the best choice. Therefore, the decision making in terms of investment into security improvement in a cloud system is a challenging issue. The proposed simulation model observes various security scenarios, and VMs allocation per TZ that directly affects revenue, lost revenue, rejection rate, and energy consumption.

Since appropriately set auction mechanisms support revenue maximization, in this paper we observe a VCG-based approach. The auction is set in a way that cloud users' payoffs are always less than on-demand prices. Furthermore, each cloud user pays the value that is less or equal to the placed bid. Thus, users always have an incentive to participate in an auction process, i.e., the proposed auction has the property of individual rationality. The proposed auction-based mechanism is truthful, implying that each bid value of each cloud user must be equal to the actual true valuation, and the user obtains the largest utility if and only if place bids truthfully. Considering that all bids are non-negative, this auction-based mechanism is budget-balanced.

In a highly secure environment and sparse situation, the scenario with low security provides the greatest revenue, but acceptable solutions are also scenarios with medium and high security. Concurrently, the scenarios with the lowest, low, and medium security level induce the acceptable lost revenue, due to upper bounds in bidding. In terms of rejection rate, the best solution assures the scenario with the highest security, followed by scenarios with medium, equal allocation, and high security. On the other hand, scenarios with equal allocation and high security are the least efficient in terms of energy consumption.

As the number of bidders increases, the best solutions for revenue and energy consumption are provided by the opposite scenarios. The same applies if the probability of malicious attack increases. The cloud provider's lost revenue increases as the number of bidders increases. The average rejection rate can be used as a decision parameter since it affects users' experience and consequently, cloud provider's reputation. If a threshold for rejection rate is set, the field of acceptable solutions can be reduced. For example, if the cloud provider's target for rejection rate is less than 10 % in an insecure environment, scenarios with low and the lowest security are not applicable. In that situation, scenarios with medium and high security could be compromising solutions for the set goals.

VI. Conclusion

The paper addresses auction-based pricing and allocation of cloud resources with the security assessment, and energy consumption estimation. The truthful VCG-based auction mechanism is established for winners' determination. Depending on the security mechanism's intensity, VMs' availability can be improved and the resistance to the VM-based attacks can be increased. We analyze the cloud provider's revenue, lost revenue, rejection rate, and energy consumption in several security-related scenarios.

Extensive simulations show that investment in security

improvement is always the preferred solution. It increases revenues and reduces the rejection rate. However, it also increases energy consumption, and, to some extent, increases the provider's lost revenue. Therefore, a comprehensive analysis is required to obtain a compromising solution.

The proposed simulation model provides a cloud provider with an insight into relations among the revenue, lost revenue, security level provided, and energy consumption, and can be used for the selection of appropriate security level that balances the multi-objective trade-offs between revenues, security, and energy.

There are several future research directions. Implementation of security mechanism affects service performance and potentially may increase delays. Therefore, the proposed model can be extended to address the energy-performance relations. Furthermore, energy consumption can be further reduced by transferring idle hosts into sleep mode. Providing a more efficient VMs allocation algorithm along with the analysis of VMs' migration can be another research course. In terms of auction-based pricing, the proposed model can be improved to support a more heterogeneous environment. Also, checkpointing techniques can be introduced to determine impacts on revenues and cloud users' utility.

REFERENCES

[1] Y. S. Patel, Z. Malwi, A. Nighojkar, "Truthful online double auction based dynamic resource provisioning for multi-objective trade-offs in IaaS clouds," Cluster Comput., 2021. doi:10.1007/s10586-020-03225-9

[2] R. Yadav, W. Zhang, K. Li, C. Liu, A. A. Laghari, "Managing overloaded hosts for energy-efficiency in cloud data centers," Cluster Comput., 2021. doi:10.1007/s10586-020-03182-3

[3] D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman, D. Woods, "Cloud-trust – a security assessment model for infrastructure as a service (IaaS) clouds," IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 523-536, 2017. doi:10.1109/TCC.2015.2415794

[4] H. Xu, X. Qiu, Y. Sheng, L. Luo, Y. Xiang, "A QoS-driven approach to the cloud service addressing attributes of security," IEEE Access., vol. 6, pp. 34477-34487, 2018. doi:10.1109/ACCESS.2018.2849594

[5] B. Mikavica, A. Kostic-Ljubisavljevic, "Auction-based pricing in cloud environment," In M. Khosrow-Pour (eds), Encyclopedia of Organizational Knowledge, Administration, and Technologies. IGI Global, pp. 86-97, 2021. doi:10.4018/978-1-7998-3473-1.ch008

[6] M. Amoon, T. E. El-Tobely, "A green energy-efficient scheduler for cloud data centers," Cluster Comput., vol. 22, pp. 3247-3259, 2019. doi:10.1007/s10586-018-2028-z

[7] R. Yadav, W. Zhang, O. Kaiwartya, P. R. Singh, I. A. Elgendy, Y. Tian, "Adaptive energy-aware algorithms for minimizing energy consumption and SLA violation in cloud computing," IEEE Access, vol. 6, pp. 55923-55936, 2018. doi:10.1109/ACCESS.2018.2872750

[8] Z. Tong, X. Deng, H. Chen, J. Mei, "DDMTS: A novel dynamic load balancing scheduling scheme under SLA constraints in cloud computing," J. Parallel Distrib. Comput, vol. 149, pp. 138-148, 2021. doi:10.1016/j.jpdc.2020.11.007

[9] Y. Saadi, S. El Kafhali, "Energy-efficient strategy for virtual machine consolidation in cloud environment," Soft Comput., vol. 24, pp. 14845-14859, 2020. doi:10.1007/s00500-020-04839-2

[10] S. Azizi, M. Zandsalimi, D. Li, "An energy-efficient algorithm for virtual machine placement optimization in cloud data centers," Cluster Comput., vol. 23, pp. 3421-3434, 2020. doi:10.1007/s10586-020-03096-0

[11] A. Tarafdar, M. Debnath, S. Khatua, R. K. Das, "Energy and quality of service-aware virtual machine consolidation in a cloud data center," J. Supercomput., vol. 76, pp. 9095-9126, 2020. doi:10.1007/s11227-020-03203-3

[12] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," IEEE Access., vol. 9, pp. 57792-57807, 2021. doi:10.1109/ACCESS.2021.3073203

[13] B. G. Batista, C. H. G. Ferreira, D. C. M. Segura, D. M. L. Filho, M. L. M. Peixoto, "A QoS-driven approach for cloud computing addressing attributes of performance and security," Future Gener. Comput. Syst., vol. 68, pp. 260-274, 2017. doi:10.1016/j.future.2016.09.018

[14] J. Chen, Q. Zhu, "Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: a contract design approach," IEEE Trans. Inf. Forensics Security, vol. 12, no. 11, pp. 2736-2750, 2017. doi:10.1109/TIFS.2017.2718489

[15] F. Sheikholeslami, N. J. Navimipour, "Auction-based resource allocation mechanisms in the cloud environments: a review of the literature and reflection on future challenges," Concurr. Comput. Pract. Exp., vol. 30, no. 16, pp. 1-15, 2018. doi:10.1002/cpe.4456

[16] G. Baranwal, D. Kumar, Z. Raza, D. P. Vidyarthi. Auction based resource provisioning in cloud computing, pp. 38-43, Spinger. 2018

[17] X. Wang, X. Chen, W. Wu, "Towards truthful auction mechanisms for task assignment in mobile device clouds," in Proc. IEEE Conf. Computer Communications (INFOCOM), Atlanta, 2017, pp. 1–9. doi:10.1109/INFOCOM.2017.8057198

[18] T. Halabi, M. Bellaiche, A. Abusitta, "Cloud security up for auction: a dsic online mechanism for secure IaaS resource allocation," in Proc. 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1–8. doi:10.1109/CSNET.2018.8602979

[19] B. Mikavica, A. Kostic-Ljubisavljevic, D. Popovic, "A security-driven approach to the auction-based cloud service pricing," Int. J. Transport and Traffic Engineering, vol. 11. no. 2, pp. 213-228, 2020. doi:10.7708/ijtte.2021.11(2).03

[20] W. Song, Z. Xiao, Q. Chen, H. Luo, "Adaptive resource provisioning for the cloud using online bin packing," IEEE Trans. Comput., vol. 63, no. 11, pp. 2647–2660, 2014. doi:10.1109/TC.2013.148

[21] H. Cambazard, D. Mehta, B. O'Sullivan, H. Simonis, "Bin packing with linear usage costs - an application to energy management in data centres," In Schulte C. (eds), Principles and Practice of Constraint Programming. CP 2013. Lecture Notes in Computer Science, vol. 8124. Springer, 2013. doi:10.1007/978-3-642-40627-0_7

[22] C. Mastroianni, M. Meo, G. Papuzzo, "Probabilistic consolidation of virtual machines in self-organizing cloud data centers," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 215–228, 2013. doi:10.1109/TCC.2013.17

[23] Z. Xiao, W. Song, Q. Chen, "Dynamic resource allocation using virtual machines for cloud computing environment," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1107–1117, 2013. doi:10.1109/TPDS.2012.283

[24] A. Beloglazov, J. Abawajy, R. Buyya, "Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing," Future Gener. Comput. Syst., vol. 28, no. 5, pp. 755-768, 2020. doi:10.1016/j.future.2011.04.017

[25] A. Beloglazov, R. Buyya, "Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers," Concurr. Comput. Pract. Exp., vol. 24, no. 13, pp. 1397-1420, 2012. doi:10.1002/cpe.1867

[26] J. Cao, K. Hwang, K. Li, A. Y. Zomaya, "Optimal multiserver configuration for profit maximization in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1087–1096, 2013. doi:10.1109/TPDS.2012.203

[27] T. T. Huu, C.-K. Tham, "An auction-based resource allocation model for green cloud computing," in Proc. IEEE Int. Conf. Cloud Eng. (IC2E), San Francisco, 2013, pp. 269–278. doi:10.1109/IC2E.2013.21

[28] W. Wang, Y. Jiang and W. Wu, "Multiagent-based resource allocation for energy minimization in cloud computing systems," IEEE Trans. Syst. Man, Cybern. Syst., vol. 47, no. 2, pp. 205-220, 2017. doi:10.1109/TSMC.2016.2523910

[29] B. Mikavica, A. Kostic-Ljubisavljevic, "Pricing and bidding strategies for cloud spot block instances," in Proc. 41st Int. Conv. Inf. Comm. Tech. Electr. Microelectr. (MIPRO), Opatija, 2018, pp. 419-424. doi:10.23919/MIPRO.2018.8400073

[30] H. S. Choi, J. B. Lim, H. Yu, E. Y. Lee, "Task classification based energy-aware consolidation in clouds," Scientific Programming, vol. 2016, 6208358, 13p. doi:10.1155/2016/6208358