Cluster Computing
https://doi.org/10.1007/s10586-024-04604-2

Enhancing cloud security: harnessing bayesian game theory for a dynamic defense mechanism

El Mehdi Kandoussi[1] · Adam Houmairi[2] · Iman El Mir[3] · Mostafa Bellafkih[1]

Received: 4 February 2024 / Revised: 25 May 2024 / Accepted: 29 May 2024

Abstract
Security challenges in complex information technologies continue to grow and diversify. To improve network security, many researchers have explored the game theoretic approach as a hopeful modeling tool. Knowing that the attacker can take advantage of vulnerabilities and explore existing weaknesses in the network configuration to gain access to the system for a successful attack, our objective is to benefit from virtual machines' migration as a moving target defense technique and honeypot as a deceiving technique to increase the attack surface's dynamicity. This paper presents a game-theoretic framework for modeling attack-defense interaction. A model based on incomplete information game and attack graph is developed. Our main findings reveal in which case migration of virtual machines should be established in a architecture where a honeypot is deployed and identify the potential attack paths based on system security parameters. This provides network administrators with the ability to find unsecure nodes, avoid negative externality and more precisely inefficient migrations which impact the quality of service.

Keywords Cloud computing · Migration · Honeypot · Attack path · Game theory · Bayesian Nash equilibrium

1 Introduction

Cloud security encompasses a range of technologies, controls, processes, and policies designed to safeguard cloud-based systems, data, and infrastructure [1]. It constitutes a subset of IT security and, more broadly, falls under the umbrella of information security [2]. The advent of cloud computing has revolutionized organizational operations by offering flexible and scalable solutions to address diverse IT needs. Consequently, the burgeoning demand for cloud technology is paralleled by the evolution of cloud computing trends [3].

The global cloud computing market has witnessed substantial growth, with projections from the International Data Corporation (IDC) indicating a significant expansion. The market size is anticipated to surge from $371.4 billion in 2020 to $832.1 billion in 2025, representing a robust compound annual growth rate of 17.5%. This remarkable growth underscores the widespread adoption of cloud-based solutions across various industries [4]. Furthermore, investments in public cloud infrastructure and services have experienced a remarkable upswing. Projections suggest that expenditures in this marking a substantial increase from $229 billion in 2019. This surge is indicative of a compound annual growth rate of 22.3%, highlighting the escalating significance of public cloud resources and services in meeting the evolving technological needs of organizations globally.

✉ El Mehdi Kandoussi
kandoussi@inpt.ac.ma

Adam Houmairi
adam.houmairi@gmail.com

Iman El Mir
iman.elmir@uhp.ac.ma

Mostafa Bellafkih
bellafkih@inpt.ac.ma

[1] Telecommunications Systems, Networks and Services laboratory (STRS), National Institute of Post and Telecommunication (INPT), Rabat, Morocco

[2] Sciences and Technologies of Engineering laboratory (LaSTI), Sultan Moulay Slimane University (USMS), National School of Applied Sciences of Khouribga (ENSAK), Beni Mellal, Morocco

[3] Computer, Networks, Mobility and Modeling laboratory (IR2M), Hassan 1st University of Settat, Institute of Sports Sciences (ISS), Settat, Morocco

Published online: 14 June 2024

As advanced computing technologies such as cloud computing, artificial intelligence, and blockchain have developed rapidly, web applications have become diverse and intelligent. This remarkable evolution brings several challenges, the main ones related to security. The extensive implementation of cloud networks renders data centers more susceptible to various forms of attacks [5]. As well as virtualization-based cloud infrastructure is under threat from malicious processes aimed at damaging its virtual resources. To detect attacks based on predefined behavior patterns, several intrusion detection systems have been developed [6]. These security issues are mostly due to the nature of network configurations, which are deterministic, static because these features enable the cyber attackers to carefully scan the network and identify its points of failure to build up and execute successful attacks [7].

The continuous transmission and collection of data in the cloud exposes cloud data centers to significant security vulnerabilities. Major security threats in cloud computing include data breaches, distributed denial of service (DDoS) attacks, malware injection, account hacking, unsupported application programming interfaces (APIs) and data loss [8]. Several defensive tools such as firewalls, IDSs, Honeypots, etc are available to defend from such attacks. An IDS works like a piece of software that monitors ongoing network traffic, identifying malicious activity. Two techniques are used namely signature-based and anomaly-based [9].

As an advanced proactive technology, cyber deception has evolved as a distinct field within cyber defense, aiming to provide attackers with seemingly credible yet intentionally misleading information, leading them to make strategic errors. Historically, deception techniques were traditionally applied in the physical domain of traditional warfare. They have been applied as intrusion detection in cyberspace. To capture attackers and closely monitor their actions, proactive measures can be used. Honeypots assume a crucial role in this procedure by functioning as simulated entities within the system or network, with the purpose of deceiving potential attackers [10]. Thanks to using of honeypots, we study the strategies and intentions of the attacker so that defenders can better understand and analyze the attack and even propose more relevant deception strategies. Honeypots, deployed on the network and furnished with deceptive data, serve as a means to lure attackers and subsequently block their access. Enhancing the efficiency of defense mechanisms requires the integration of intelligent systems that carry on regular monitoring of network traffic.

To meet the demands of system security and overcome the associated challenges, we focus on honeypots as a MTD technique to maximize the resilience of cloud computing environment. Moving Target Defense has been proposed as a more valuable security technique. Different mechanisms and techniques of the underlying system are diversified and changeable over time to neutralize the attacker and minimize the opportunity of the advanced adversarial attacker. As an additional security layer and active defense technology, the honeypot can serve as MTD and is carefully useful for detection, and gathering attack information. To analyze the impact of this MTD technique, our problem is modeled as a Bayesian game. Basically, a Bayesian game [11], is a game in which the information available to each player about the characteristics of other players is incomplete. In particular, a game is thus represented in which one or more players face uncertainty as to the gain of the other players. Hence, the key contributions of this paper can be summarized as follows:

Firstly, the applicability of MTD deployment based on the combination of honeypot was discussed in the sense that it can improve the resilience for cloud-hosted applications. Then, this latter was modeled as a simultaneous non-cooperative and Bayesian game where different Nash equilibriums were calculated in order to prove the effectiveness of our solution. Finally, our security game model was evaluated by numerical results illustrating the contribution of our solution in terms of improving security in a cloud environment.

The remaining sections of the paper are structured as follows. Section 2 offers an overview of related work. In Sect. 3, we present the security mechanisms in a cloud architecture and the attack graph as an offensive approach and source of threats. Section 4 introduces and analyzes our proposed game model within diverse attack-defense scenarios. Section 5 delves into the numerical findings. Finally, Sect. 6 is dedicated to concluding our work and exploring potential directions for future research.

2 Related work

In the existing literature, numerous studies emphasize vulnerability as the potential gateway through which cloud systems can be influenced and compromised. As a result, a thorough understanding of system design and operation, coupled with information on potential threats, is crucial for effective vulnerability analysis. Assessing network security goes beyond merely considering the presence or absence of isolated vulnerabilities, especially in large networks that rely on various platforms, software packages, and support multiple modes of connectivity. In such complex networks, security vulnerabilities may exist, possibly escaping detection during initial analyses.

To address this complexity, the concept of an attack graph is frequently employed. An attack graph serves as a concise representation of all possible paths within a system

that could lead to a state where an intrusion is successful. It systematically enumerates these potential attack paths based on a comprehensive analysis of network configuration and vulnerability information. This approach aids defenders in intuitively grasping the intricate relationships between vulnerabilities in the target network and the configuration of network security. By providing a visual representation of these relationships, the attack graph becomes a valuable tool for enhancing the understanding of potential security risks and guiding efforts to fortify the network against various attack vectors [12].

To analyze the network security, two offensive parts must be analyzed namely attacker and defender. Because the attacker can exploit the system's vulnerabilities and gain access to the network. He performs recognition phase and understands in depth the network configuration to execute a successful attack, whereas the defender must secure the network even in the presence of its potential vulnerabilities. In addition, the defender is a proactive stance rather than a passive one because in modern network security involves active and strategic efforts to prevent, detect and respond to threats, which can be seen as offensive actions in a defensive context. Hence, researchers in the domain of network security. They are actively exploring resilient security architectures and mathematical modeling tools to assess the equilibrium between reinforced security measures and the corresponding costs incurred by defense solutions. The work [13] introduces a game-theoretic model from the point of view of network survivability using the attack graph. They implement the attack graph for extracting attack-defense actions and define possible attack-defense strategies and their payoffs. They designed an attack-defense model using dynamic game theory. In the multi-stage attack scenario, attack defense exhibits the characteristics of collaborative evolution. Among the solutions proposed to meet these challenges, the defense of moving targets appears to be an effective technique, which stands out from traditional security architectures based on detection mechanisms.

Research on deception in computer networks focuses on advancing techniques, strategies, and technologies to enhance the efficacy of deception as a proactive cybersecurity measure. In [14], the authors employ stochastic dynamics across various layers of computer systems to argue for system security by constantly altering its attack surface. It is essential to consider the reconfiguration cost associated with shifting this surface and the cost incurred by the attacker in learning and modifying their attack vector. Consequently, a dynamic game model is proposed to capture the interaction between attack and defense. In this model, the system dynamically creates a moving target to minimize risk and preserve its utility, while the attacker endeavors to dynamically explore and exploit vulnerabilities to compromise the system. The objective is to establish a proactive defense strategy that adapts to potential threats. Additionally, in [15], the authors delve into preparing and processing network-level information, encompassing network topology, host details, and traffic information. This information is crucial for understanding and addressing potential vulnerabilities, forming a comprehensive approach to bolstering network security.

In several research studies, researchers have introduced the DDoS detection and mitigation technique in software-defined networks. This strategy remains effective in terms of limiting packets by acting on the redirection of illegitimate traffic, the aim of which is to minimize downtime and better analyze the network [16]. The authors in [17] proposed an intrusion detection framework for detecting known and unknown attacks by analyzing system call sequences. They analyzed the system call sequences of virtual machines with a model combining both long-term memory and anomaly detection techniques based on the frequency of system calls.

The application of defensive cyber deception based on software-defined networks (SDN) has been used to ensure the reliability of network systems and improve security [18]. The authors investigate the use of deception on computer networks to better gather relevant information about various possible threats. Software-defined networking has been used as a platform for MTD implementation. The authors of [19] use Sniffer Reflector as an MTD technique against network reconnaissance using software defined networking. Their proposed solution aims to disrupt various network recognition attacks because Sniffer Reflector was designed to send the analysis traffic back to a shadow network where the analysis responses are given and confused. Thus, attackers will concentrate only on the obscured representations of a shadow network rather than the desired views of the network. Jafarian et al. [20] have introduced an MTD architecture involving OpenFlow, designed to modify IP addresses in scenarios marked by significant unpredictability. The basic concept is to preserve configuration integrity while reducing operational costs. Deploying MTD techniques provides a robust countermeasure against attacks, improving the resilience of cloud-hosted applications [21].

The MTD techniques have been applied to prevent from different types of attacks such as DDoS attacks. Venkatesan et al. [22] applied MTD on proxies-based architectures. They frequently move and change proxies and remap clients to proxies after network reconfiguration. In other words, the attack cannot precisely define its object and the reconnaissance phase remains unsuccessful. They implemented their proposed solution and accross some experiments and simulation findings, they reduced the probability of the attacker detecting the proxies for a certain period of

time and minimized the attack surface. In this research work [23], the authors try to select the optimal hopping strategy that acts perfectly. To achieve this, using dynamic game theory, they formulated an MTD model to describe multiple phases of the MTD hopping process. Thus, To outline the process of creating a model for the transitions in network states during the MTD hopping process, they used Markovian Decision Process (MDP) as well as a mathematical framework based on the main property of Markov.

Much research work has been deployed to assess the effectiveness of MTD mechanisms that require quantitative measurement of changes on the attack surface in order to find the best trade-off between cost and efficiency of mutation. Thus, the development of network security analysis and defense techniques using game theory and MTD has emerged as a perfectly suited mitigation solution to alter the static nature of cyber systems.

Honeypots play a crucial role in implementing various cyber-deception techniques by misleading attackers and diverting them from valuable assets. Many studies regard honeypots as essential deception tools. To this end, the authors [24] propose a game theory-based approach that models an attack-defense scenario and develops an optimal honeypot allocation strategy for the defender. Their approach considers changes in network connectivity as well as the specific characteristics and criticality of different nodes. Specifically, they introduce a dynamic two-player game model that explicitly incorporates the evolution of future states resulting from connectivity changes.

The authors of [25] presented a HoneyCloud system equipped with a robust honeypot for identifying attacks. To analyze the detailed actions recorded by this honeypot, we tested three machine learning techniques. We implemented machine learning models such as Naïve Bayes (NB), Support Vector Machine (SVM), and Random Forest (RF) to classify incoming data from these honey clouds as malicious with remarkable precision. The experimental results presented in the paper indicate that the Random Forest technique offers the highest accuracy.

Depending on the game scenario, different types of game were implemented. Jeffrey et al. introduced the taxonomy of game theory to explain the different types of defensive deception [26]. To consider attack detection, Bayesian gaming was used to study the deceptive nature of DDoS attacks and to search for optimal strategies for both sides of the game. Dynamic evolution under attack between ordinary nodes and honeypots were modeled to study strategic decision-making. The proposed solution aims to improve Honeynet design and mitigate Honeynet attacks [27].

In [21], the authors introduced a game theoretical model aimed at defining optimal strategies for allocating honeypots. They proposed a dynamic two-player game model that explicitly considers the future evolution of states resulting from changes in network connectivity. The purpose is to maximize the probability of the attacker encountering a honeypot while minimizing the costs associated with deception and reconfiguration due to alterations in network topology. To find Nash equilibrium strategies, the authors developed an iterative algorithm.

In [28], the authors created and applied an adaptive attacker strategy evolution model to understand how an adaptive attacker learns to overcome a moving target cyber defense. The interaction between the attacker and defender is framed as a game, with a non-adaptive defender deploying a diverse moving target defense. Faced with this defense, various types of attackers develop strategies, often investing in resources for zero-day exploits to compromise the defender. The findings suggest that diversity-maximizing defenses are most effective in situations where engagements between attackers and defenders are of short duration.

Abdallah et al. [29] presented an impact analysis of behavioral decision making on the security of interdependent systems. They considered a system consisting of a set of defenders and several interdependent assets, with each defender responsible for protecting a subset of the assets from an attacker. They then used an attack graph to capture the interdependencies between the assets where each defender misperceives the probabilities of a successful attack. A behavioral anarchy price is proposed to capture the inefficiency of equilibrium investments made by behavioral decision makers relative to a non-behavioral optimal solution. The authors studied the characteristics of optimal investments and the impacts of behavioral biases of advocates. A case study is presented in which equilibrium inefficiency increased as defenders became more behavioral. Hasan et al. [30] proposed a signaling game model to analyze the co-resident attacks and corresponding defense strategies in a cloud environment where the same virtual machine images provide the same services. The proposed solution provides optimal strategies to defend the malicious virtual machines, while limiting the impact on the benign virtual machines. The obtained results from the proposed mechanism shown to be powerful in the two attack cases, using a single virtual machine or a number of collaborative virtual machines.

In much of the existing literature, the Stackelberg games have been widely applied in the fields of security to quantitatively model and analyze the attack-defense interaction. The authors [31] introduced a Stackelberg framework of Markov's play to accurately describe the spatial and temporal decision-making by the defender against malicious attackers. The approach they propose allows the defender to calculate the optimal defense of the moving target and demonstrates its effectiveness for the defender to

concurrently choose the moment and state to which the system is to be migrated. In [32], the authors introduced a game-theoretic approach called GTA-IDS (Game Theoretic Approach for Intrusion Detection System) in a Cloud Environment to enhance the efficiency and decision-making accuracy of the defender while conserving energy. The proposed methodology is well-established in non-zero-sum non-cooperative game theory, employing Bayesian Nash Equilibrium to formulate the defender's strategies and optimize its actions for maximizing payoffs.

The model's efficacy was evaluated using the NSL-KDD dataset, and the obtained results were compared with those derived from existing models. The outcomes demonstrated that, throughout the evaluation, the defender consistently achieved superior gains, ultimately successfully thwarting the attack despite the persistent efforts exerted by the attacker. In the study documented in [33], the authors directed their attention to the denial-of-service (DoS) attack, a scenario in which an attacker intentionally congests a bottleneck router queue that is shared among virtual machines (VMs) hosted on the same physical machine (PM) within a cloud environment. To emulate and assess the behavior of this shared router queue, the authors employed the Click modular router on the DETER testbed.

The research showcased the application of game theoretic approaches in modeling this particular type of attack as a two-player game. By framing the DoS attack scenario within the context of a game. The authors successfully examined the strategic interactions occurring between the attacker and the defender. This modeling approach allowed for a nuanced exploration of the dynamics involved in such attacks and facilitated the identification of strategies for defending against them.

As a result, the study not only highlighted the vulnerability of shared router queues in cloud environments but also proposed strategic countermeasures based on game theory. This strategic perspective can contribute valuable insights into developing effective defense mechanisms against DoS attacks targeting shared resources in cloud computing settings.

In [34], the authors introduced the Security Incident System Vulnerability (SISV) model, leveraging game theory to analyze the interactions among vulnerability components within the security incident system. By delving into the game characteristics inherent in these vulnerabilities, the model seeks to uncover the Bayesian Stackelberg game effect among them. This approach provides insights into the intelligent aspects of security incidents, specifically from the vantage point of vulnerabilities.

The primary objective of the model is to optimize the vulnerability levels within security incident systems. By doing so, it aims to contribute to the advancement of the field of security vulnerabilities, particularly in the context of petrochemical plants. The results derived from this model are expected to shed light on the dynamics of vulnerability interactions, offering a framework to enhance the security posture of incident systems. Ultimately, this research holds the potential to drive improvements in managing and mitigating security risks within the petrochemical industry.

In addition, a novel framework named Cyber Mission Impact Assessment (CMIA) based on the Bayesian Stackelburg game and the Bayesian network is proposed in [35]. This framework provides the most probable cyber threat and the optimal defense securing the resilience of mission-critical systems. The experimental outcomes proved that the suggested framework can efficiently optimize and produce results that meet user expectations.

In [36], the authors have established a propagation dynamics model for a scale-free network to analyze the evolution of the security state in complex networks with significant variations in node degrees. This includes designing network attack and defense strategies, as well as methods for calculating gains, based on the analysis of confrontational behaviors between attackers and defenders, and their impact on the security states of network nodes. Furthermore, the authors have constructed a real-time game model to address network attack and defense dynamics, drawing upon insights gleaned from the evolution analysis of network security states and employing principles from differential game theory. They introduced a method to compute the saddle point equilibrium strategy within the network attack and defense game, thereby facilitating the identification of optimal defense strategies through this equilibrium strategy algorithm. To validate their findings, the authors conducted experiments on a simulated network constructed using real-world connection averages. These experiments aimed to scrutinize the evolution and stability of optimal defense strategies. Additionally, the authors performed comparisons of various network defense decision-making methods to verify the efficacy and performance of the proposed models and methodologies.

In [37], the authors seek to establish a cyber threat propagation model aimed at enabling a detailed analysis of network node security states at a microscopic level. This endeavor involves not only proposing a comprehensive attack and defense control strategy on a broader scale but also conducting calculations to determine the game payoffs for both attackers and defenders. Furthermore, they have crafted an attack-defense potential differential game model that boasts real-time analysis capabilities, drawing upon principles from potential differential game theory. Within this model, they have introduced a methodology to compute the saddle point equilibrium strategy, alongside designing a global optimal decision algorithm that aligns with the overarching objectives of network defense. To

validate their approach, the authors conducted verification experiments on typical complex networks. In these experiments, they created a simulation environment mirroring the characteristics of small-world and scale-free networks. By comparing their proposed model against stochastic defense strategies, they were able to demonstrate its efficacy in significantly bolstering the defense effectiveness of networks.

The table below provides a comparative analysis of various game modeling approaches within the security cloud computing domain. When juxtaposed with the examined works, our model exhibits the capability to integrate two robust security measures: Virtual Machine (VM) migration as a Moving Target Defense (MTD) technique and the honeypot technique. Additionally, it leverages attack graphs to model the attack surface, thereby enhancing its ability to predict potential attack paths. This predictive capability facilitates informed decisions on when a VM should undergo migration and which physical server should host the migrated VM, guided by the parameters of the security system.

The proposed model integrates VM migration as a MTD technique with honeypots to enhance cloud security, improving prediction accuracy and reliability despite initial incomplete information. This approach contrasts with existing methods like those that enhance zero-day attack prediction using hybrid game theory and neural networks [47], and systems that employ honeypots for malicious detection using machine learning techniques [25]. Other models include game-theoretic approaches for strategic honeypot allocation in dynamic networks [24], fog-cloud based intrusion detection systems using recurrent neural networks for IoT networks [48], and comprehensive reviews of game-theoretic models addressing various security requirements in cloud environments [49]. The proposed model's combination of MTD and honeypots leverages attack graphs to visually represent potential vulnerabilities and attack paths, facilitating informed decisions on VM migration and hosting. This integration of dynamic defenses complicates attackers' efforts to gather complete information, enhancing security more effectively compared to traditional models.

Motivated by previous related works, many efforts have been made to investigate different practical MTD strategies. However, in the literature, a few research works introduce a dynamic defense framework that involves MTD strategy and honeypot in a combined manner. For that, this paper provides probabilistic models to quantitatively evaluate the efficiency of the proposed MTD schemes.

3 Security mechanisms and attack graph

In this section, we explore two proactive cybersecurity measures: MTD and honeypots. MTD involves dynamically changing system configurations to increase resilience against attacks. Honeypots, on the other hand, are decoy systems designed to attract and detect malicious activity. Additionally, we provide an illustration of the attack surface using an attack graph, which visually represents the potential vulnerabilities and attack paths within a system.

Figure 1 illustrates a Cloud data center comprising three physical servers, each hosting multiple VMs. The servers are categorized into three security policies: more secure server, current server, and less secure server. The classification is based on the security scores of the servers, specifically the complexity of vulnerabilities present in the hosted VMs. We assume that the VMs are homogeneous and possess the same level of security. In other words, the overall security of a server is determined by the security level of its components. VMs are grouped based on their common vulnerabilities score within the same server. This grouping is important because the security of one VM can impact the security of others within the same server. If the VMs are randomly distributed across the data center's servers, an attacker can exploit the least secure VM in the environment, leveraging its connection to a shared platform, to target more secure VMs. This issue is referred to as negative externality and has been explored in [50]. Furthermore, the security of the hypervisors is critical as a compromise in their security could potentially grant control over all the VMs, as discussed in [51]. For instance, in Fig. 2, assuming the servers are ordered in increasing order of complexity to be compromised from "1" to "n", an attacker aiming to compromise a secured VM located in server "n" would first target an unsecured VM that has already been migrated to server "n". Subsequently, the attacker would attack the hypervisor, which is relatively easier to gain privileges compared to their primary target, and ultimately exploit the targeted VM.

Concerning, the second part in Fig. 3 with grey color, it represents the honeypot. Indeed, the component mimic the real network. Consequently, the attacker is unable to detect the real network from the fictitious one.

From a technical standpoint, the MTD defense mechanism in our cloud computing environment context used the live migration of Virtual Machines (VMs) to mitigate the degradation on Quality of Service (QoS) metrics. Turning to the deployment of honeypots, any node within the network can serve as a decoy to identify malicious activities. Specifically, within a physical server, deploying fictitious VMs with the same vulnerabilities mimics those in production. This strategic use of virtualization increases the

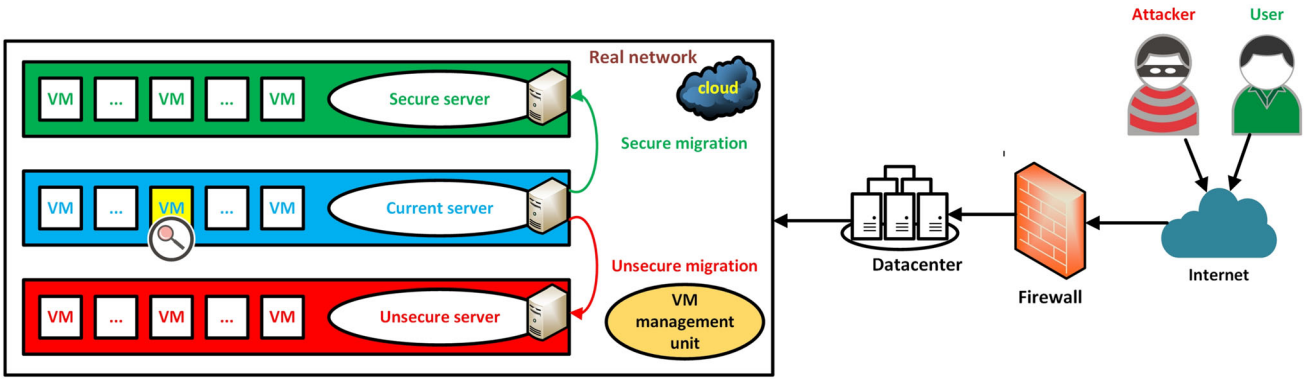

Fig. 1 VM migration without honeypot deployment

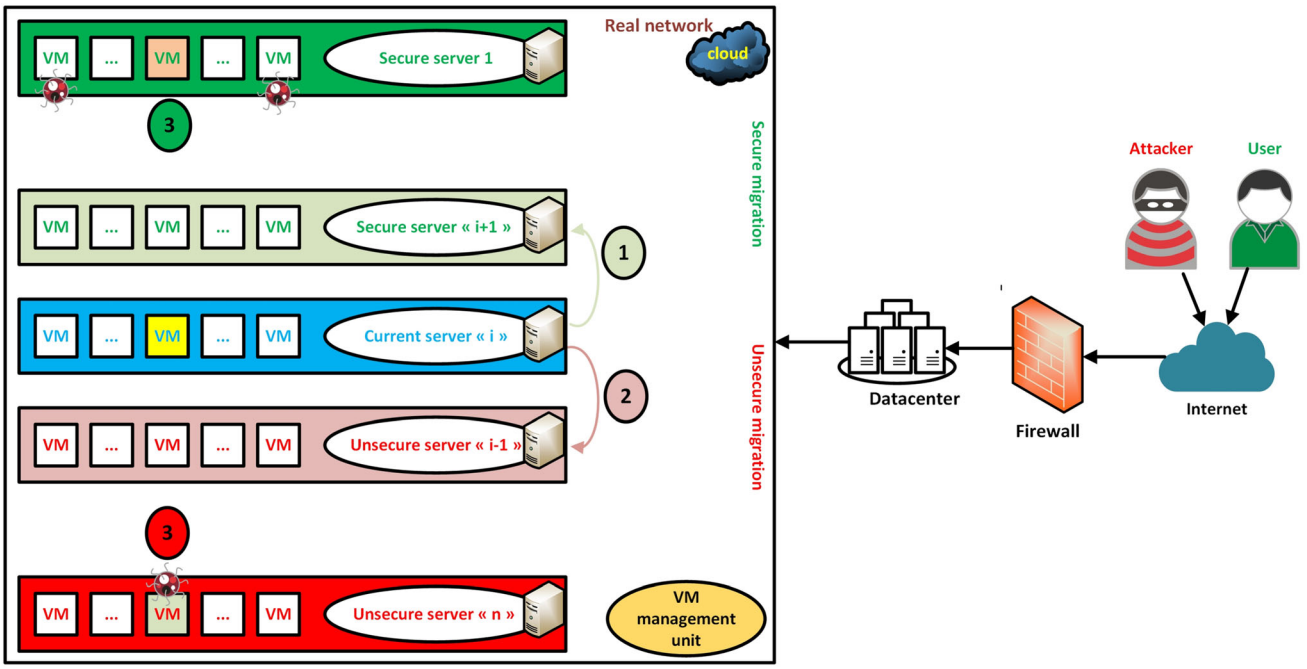

Fig. 2 Negative externality impact

likelihood of a production VM becoming a target. The same explanation applies to other network components such as routers used as a decoy. Consequently, in such a scenario, it becomes imperative to implement an intrusion detection system to mirror the network and study the entry points. In our context, this behavior is theoretically modeled by using Bayesian game model which take into consideration the incompleteness of information. Moreover, in our context, the MTD (Moving Target Defense) is event-driven. Specifically, the migration is triggered by automatic scripts that monitor specific events or anomalies detected by the intrusion detection system. Additionally, our approach leverages attack graphs to optimize the migration process and avoid inefficient migrations. The implementation is carried out using the Python library "psutil".

In our context, Bayesian game theory addresses incomplete information by incorporating probabilities to represent the uncertainty about various aspects of the system. Specifically, the proposed approach employs virtual machine migration and honeypots as dynamic defense mechanisms. By relocating VMs and deploying decoy systems, the model creates a moving target defense, complicating the attacker's efforts to gather complete information. This strategy enhances security by leveraging the uncertainty and making it more difficult for attackers to accurately target the system, thereby mitigating the effects of initial incomplete information.

The main objective of the MTD and honeypot deployment is to have a dynamic attack surface that increase the likelihood to compromise a targeted VM. To succeed his mission, the attacker needs a considerable amount of

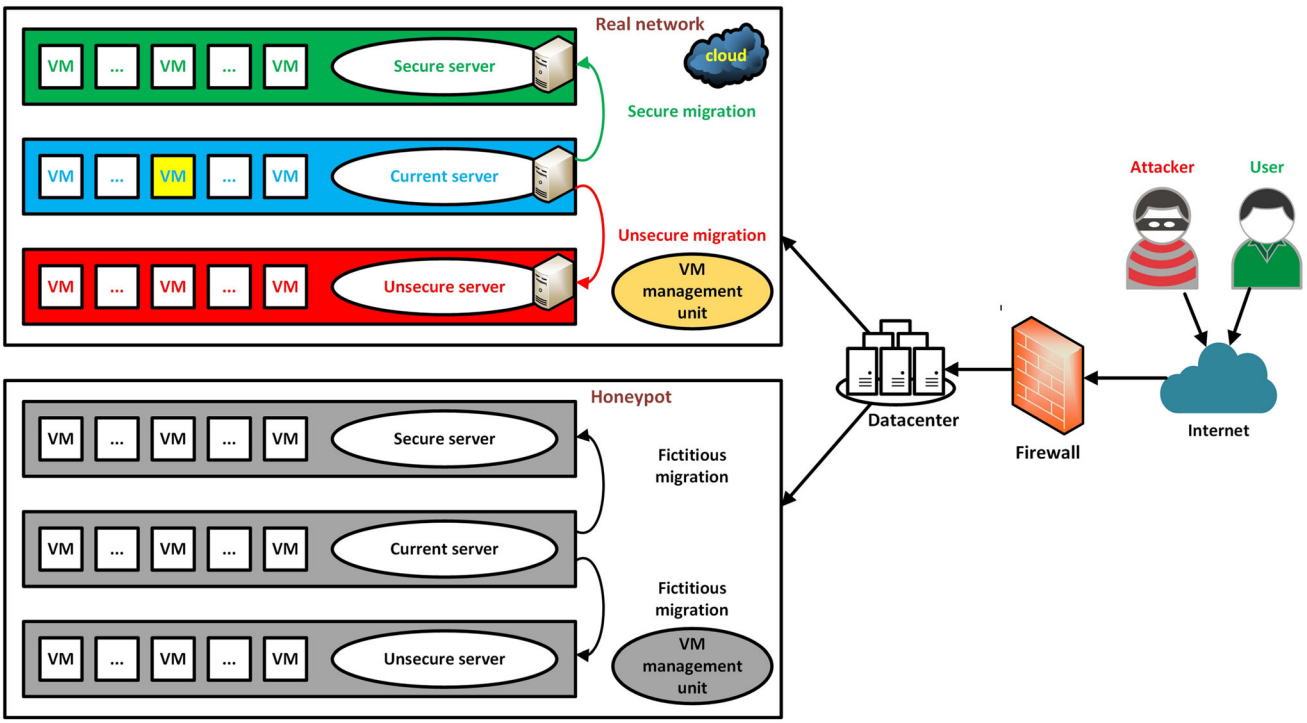

Fig. 3 VM migration with honeypot deployment

computational resources and time to analyze an attack surface changing over time.

In Fig. 4, an oriented graph with three types of nodes (requirement, rule and consequence) is used to illustrate an exhaustive list of attack path. More precisely, it shows all conditions (requirements) needed for actions' successful execution (rules) to attain a certain goal. The repetition of this process leads to reach the global goal which is the execution of code in a VM with root privileges. The generation of the attack graph is based on a database of

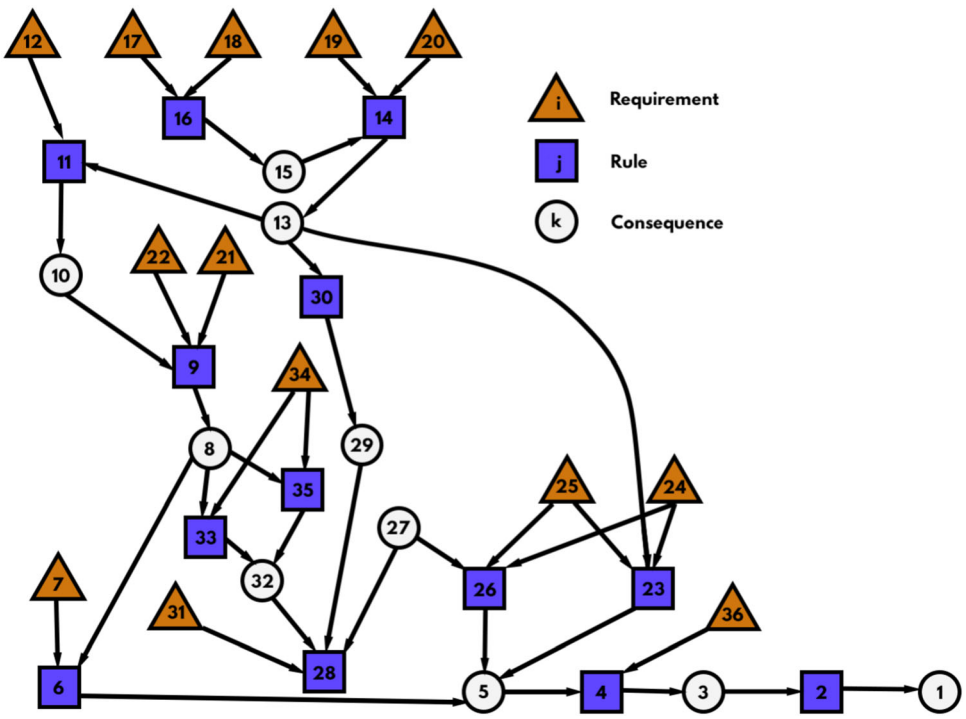

Fig. 4 Attack graph generated by MulVAL

Table 1 Qualitative comparison of mathematical approaches modeling dynamic security in cloud computing environment

Contributions	Year	Context	Game types	Information completeness	Universality
[38]	2020	MTD	Signal game (dynamic bayesian game)	Incomplete information	Good
[39]	2021	Random disturbances	Stochastic differential game		
[40]	2019	MTD based on moving attack surface	Markov robust game		
[41]	2018	MTD	Markov game		
[42]	2020	Cyber deception	Bayesian game		
Proposed model		MTD and honeypot			
[43]	2020	MTD and honeypot	Stochastic game		
[44]	2021	MTD and SDN			
[45]	2013	MTD based on shifting attack surface	Two-person zero-sum game	Complete information	Poor
[46]	2016	IP hopping	Markov game		

Table 2 Requirements

Requirements' id	Requirements
7	**canAccessFile**(fileServer,root,write,'/export')
12	**hacl**(webServer,fileserver,rpc,100005)
17	**hacl**(internet,webServer,tcp,80)
18	**attackerLocated**(internet)
19	**networkServiceInfo**(webServer,httpd,tcp,80,apache)
20	**vulExists**(webServer,'CVE-2008-0074',httpd,remoteExploit, privEscalation)
21	**networkServiceInfo**(fileserver,mountcl,rpc,100005,root)
22	**vulExists**(fileserver,vulID,mountd,remoteExploit,privEscalation)
24	**hacl**(webServer,fileServer,nfsProtocol,nfsPort)
25	**nfsExportInfo**(fileServer,'/export',write,webServer)
31	**hasAccount**(sysAdmin,webServer,root)
34	**hasAccount**(sysAdmin,fileServer,root)
36	**nfsMounted**(VirtualMachine,'/usr/local/share',fileServer,'/export', read)

Table 3 Rules

Rules' id	Rules
2	Trojan horse installation
4	NFS semantics
6	execCode implies file access
9 and 14	Remote exploit of a server program
11	Multi-hop access
16	Direct network access
23 and 26	NFS shell
28	When a principal is compromised any machine he has an account on will also be compromised
30	Access a host through executing code on the machine
33 and 35	Password sniffing

vulnerabilities, network topology and rules. In our context MulVAL is used. More details about our generator is provided in [52]. The case studied in 4 shows that the attacker should start from one of the thirteen entry points of the system (orange triangle). To have the meaning of each nodes, Tables 2, 3 and 4 maps each node in the attack

Table 4 Consequences

Consequences' id	Consequences
1	**execCode**(virtualMachine,root)
3	**accessFile**(virtualMachine,write,'/usr/local/share')
5	**accessFile**(fileServer,write,'/export')
8	**execCode**(fileServer,root)
10	**netAccess**(fileServer,rpc,100005)
13	**execCode**(webServer,apache)
15	**netAccess**(webServer,tcp,80)
27	**execCode**(webServer,root)
29	**canAccessHost**(webServer)
32	**principalCompromised**(sysAdmin)

graph with the corresponding meaning.For example, by targeting remotely the file server through the vulnerability exploitation and if the remote exploit is succeeded, more privileges as admin code execution are obtained by the attacker ($22 \Rightarrow 9 \Rightarrow 8$).

In modern networks, such as cloud environments and Software-Defined Networks (SDNs), dynamic configurations and the deployment of Moving Target Defense (MTD) strategies can significantly alter attack surfaces. Capturing these changes is crucial for maintaining effective security. Practically, this is achieved through dynamic updates using automatic scripts. Attack graphs can be dynamically updated to reflect changes in network configurations and the deployment of MTD strategies. This involves continuously monitoring the network for configuration changes and updating the graph accordingly.

In general, the attacker is typically assumed to be outside the network, but there are no constraints preventing the consideration of an attacker located inside the network. In this scenario, we analyze all vulnerabilities from the entry node to which the attacker is connected and provide this information, along with the network topology, to MulVAL. The generated attack graph in this case shows a significantly higher number of attack paths compared to an external attacker, indicating a greater likelihood of a successful attack. Mathematically, as detailed in the following section, the attacker's location does not impact the model or its resolution and all other considered assumptions are explained in the first paragraph of the following section.

4 Model description

In this section, we begin by constructing a mathematical model based on the framework of a Bayesian game. We will explain the rationale behind employing this specific mathematical framework and its relevance to our study. Subsequently, we proceed to offer a detailed resolution of the game by providing explicit expressions for the Bayesian equilibrium.

Table 5 Acronyms

Notations	Meanings
Def	Defender
H_p	Honeypot
R_n	Real network
Att	Attacker
M_l	Malicious
$AP_{i\in\{1,\ldots,n\}}$	i^{th} attack path
M_s	Secure migration
$\overline{M}$	No migration
$M_{\overline{s}}$	Unsecure mugration
M_f	Fictituous migration

4.1 Game formulation

The mathematical model developed is a Bayesian game with a finite set of players and actions, based on the following assumptions:

- players are assumed to be rational, making decisions that maximize their expected utility;
- actions are taken simultaneously by all players, without any sequential or turn-based order;
- all players possess complete knowledge of the payoff matrix, which outlines the outcomes and associated utilities for each combination of actions;
- there is no formation of coalitions between players prior to or during the game, implying that players act independently of each other.

In our security model, we consider two players: the defender and the attacker. The defender represents the cloud computing component, consisting of the honeypot and the MTD mechanism, which is responsible for

Table 6 System parameters

Notations	Meanings
L_i	Total lost associated to AP_i
C_i	Total cost associated to AP_i
C_m	Cost associated to VM migration
C_h	Cost associated to the honeypot deployment
α_s	Probability to identify the VM after a secure migration
$\alpha_{\bar{s}}$	Probability to identify the VM after an unsecure migration
θ	Probability to detect the real network

simulating the real network and migrating the VMs. To accurately capture the behavior of the honeypot, a Bayesian game is more suitable than a normal form game. The latter fails to account for the different types of players involved. However, in our specific context, it is essential to depict the dual nature of our security mechanism, which adds complexity to the detection of the real network. As a result, the defender can be categorized into two types. In terms of the defender's space of actions, there are only three options available: migrating the VM to a secure server, a less secure server, or not performing any migration at all.

On the other hand, the attacker refers to any external entity attempting to compromise the cloud computing environment by exploiting the attack surface, which is inherently malicious. The attacker's space of actions encompasses all attack paths depicted in Fig. 4. More precisely, the attack surface comprises all potential paths originating from nodes $\{12, 17, 18, 19, 20, 21, 22, 34, 7, 31, 27, 24, 25, 36\}$ and culminating at node 1. These paths are deemed as attack paths. For each attack path a total loss L and cost C is provided to quantitatively formulate the utility of the attacker and the defender.

The formal definition of a Bayesian game is as follows:

Definition 1 (Bayesian game) A Bayesian game is a tuple $\langle N, (A_i, \Theta_i, p_i, u_i)_{i \in N} \rangle$ where:

- N: a set of players ($|N| = n$); For each $i \in N$, we have:
- A_i: a set of actions, we note $A = \prod_{i=1}^{N} A_i$;
- Θ_i: a set of types, we note $\Theta = \prod_{i=1}^{N} \Theta_i$;
- p_i: a probability function such as, $p_i : \Theta_i \rightarrow \Delta(\Theta_{-i})$;
- u_i: a payoff such as: $u_i : A \times \Theta \rightarrow \mathbb{R}$.

In Table 5 (*respectively*, Table 6), the acronyms used throughout this paper are listed along with their corresponding meanings (*respectively*, the system parameters employed in the mathematical expressions are listed with their corresponding meanings).

In our model the components of the Bayesian game are:

Table 7 Payoff matrix of the Bayesian game

$Def = R_n$	..	AP_i	..
M_s		$-\alpha_s L_i - C_m - C_h$	$\alpha_s L_i - C_i$
$\overline{M}$		$-L_i - C_h$	$L_i - C_i$
$M_{\bar{s}}$		$-\alpha_{\bar{s}} L_i - C_m - C_h$	$\alpha_{\bar{s}} L_i - C_i$
$Def = H_p$	..	AP_i	..
M_f		$-C_h$	$-C_i$

Note: Since the attacker has one type M_l and the defender has two types R_n and H_p the payoff matrix will be composed from two submatrices (2×1)

- Players' set: $N = \{Def, Att\}$ with ($|N| = 2$);
- Players' types: $\Theta_{Def} = \{R_n, H_p\}$ and $\Theta_{Att} = \{M_l\}$;
- Actions associated to each player's type:
  - $A_{Def}^{R_n} = \{M_s, \overline{M}, M_{\bar{s}}\}$ and $A_{Def}^{H_p} = \{M_f\}$;
  - $A_{Att}^{M_l} = \{AP_i;\ i \in \{1, \ldots, n\}\}$.
- Probability distribution over player's types:
  - $Pr(Def = R_n / Att = M_l) = \theta \Rightarrow Pr(Def = H_p / Att = M_l) = 1 - \theta$;
  - $Pr(Att = M_l / Def = R_n) = Pr(Att = M_l / Def = H_p) = 1$.
- Regarding the payoff function, Table 7 provides a comprehensive overview of the utilities for all players. The utility function is divided into two parts, reflecting the fact that two distinct types characterize the defender.

In the rest of this paper, we adopt the following assumptions on the system parameters:

1. L_i, C_i, C_m and C_h are non-negative;
2. $0 \leqslant \alpha_s \leqslant 1$, $0 \leqslant \alpha_{\overline{s}} \leqslant 1$ and $0 \leqslant \theta \leqslant 1$;
3. $\forall i \in \{1, \ldots, n\}$ $C_i < L_i$;
4. $L_1 - C_1 \leqslant \ldots \leqslant L_i - C_i \leqslant \ldots \leqslant L_n - C_n$.

The hypotheses mentioned above can be explained as follows: A migration is deemed secure when a virtual machine is migrated to a secure server. In such cases, the probability of identifying the targeted virtual machine within the network is denoted as α_s. On the other hand, if an insecure migration takes place, the probability of identifying the virtual machine is denoted as $\alpha_{\overline{s}}$. Furthermore, an unsecure server has a larger attack surface, which results in providing more information compared to a secure server. Thus, we have $0 \leqslant \alpha_s \leqslant \alpha_{\overline{s}} \leqslant 1$.

Regarding the third assumption, all network attacks have a significantly greater negative impact than the cost invested in implementing them. To be more precise, even a simple attack can cause more damage than the cost invested in a sophisticated attack. Concerning the last assumption, there are no restrictions or loss of generality imposed on the model, and it solely contributes to solving the game.

The use of two distinct defender types stems from the multifaceted nature of the defender's role. Specifically, the integration of a honeypot within the analyzed system introduces heightened complexity, impeding the attacker's ability to discern the actual network. As a result, the likelihood of a successful intrusion is significantly reduced. Mathematically, this is modeled in the forth component of the Bayesian game as a probability distribution over player's types.

4.2 Bayesian game resolution

Resolving a Bayesian game consists of finding a Bayesian equilibrium or a set of Bayesian equilibria. In the following these notations will be used:

- The notation $a = (a_i, a_{-i})$ is used instead of $a = (a_1, \ldots, a_N)$and denotes the action profile played by N the players and is the profile played by $(N-1)$ the players except the i^{th} player. The same explanation goes with the vector $\theta = (\theta_i, \theta_{-i})$;
- $\Delta(E)$ is the set of probability distributions over a set E;
- If $\gamma \in \Delta(E)$ then the set defined as follows $\text{Supp}(\gamma) = \{e \in E / \gamma(e) \neq 0\}$ will be used.

The two definitions below introduce the notions related to Bayesian game resolution.

Definition 2 (Best response) A strategy a_i^* is denoted as a best response of the player i if: $\forall a_i \in A_i \quad u_i\left(a_i^*, a_{-i}\right) \geqslant u_i(a_i, a_{-i})$.

Table 8 numerical values of system parameters

Parameters	Numerical values
C_m	300
C_h	50
L	$[250, 1100, 1500]$
C	$[50, 350, 650]$

Definition 3 (Strictly dominated strategy) A strategy $a_i \in A_i$ of the player i is strictly dominated by $a_i' \in A_i$ if: $\forall a_{-i} \in A_{-i} \quad u_i(a_i, a_{-i}) \geqslant u_i\left(a_i', a_{-i}\right)$.

Definition 4 (Bayesian equilibrium)

1. Given a Bayesian game $\left\langle N, (A_i, \Theta_i, p_i, u_i)_{i \in N} \right\rangle$ a pure strategy for player i is a function which maps player i's type into its action set: $a_i : \Theta_i \rightarrow A_i$;
2. A mixed strategy for player i is: $\mu_i : \Theta_i \rightarrow \Delta(A_i)$: $\theta_i \mapsto \mu_i(.|\theta_i)$;
3. A Bayesian equilibrium is a mixed strategy profile $(\mu_i)_{i \in \mathbb{N}}$ such that of for every player $i \in \mathbb{N}$ and every type $\theta_i \in \Theta_i$, we have:

$$\mu_i(.|\theta_i) \in \underset{\gamma \in \Delta(A_i)}{argmax} \sum_{\theta_{-i} \in \Theta_{-i}} p_i(\theta_{-i}|\theta_i) \sum_{a \in A} \left[\prod_{j \in N \setminus \{i\}} \mu_j(a_j|\theta_j) \right] \times \gamma(a_i) u_i(a, \theta)$$

Theorem 1 *Let* α *and* θ *in* [0, 1].

We note by $AP_p = AP_p^{\alpha,\theta} = \underset{AP_i \in A_{Att}^{Ml}}{\arg\max} \theta L_i - C_i$ *and* $AP_q = AP_q^{\alpha,\theta} = \underset{AP_i \in A_{Att}^{Ml}}{\arg\max} \theta \alpha L_i - C_i$.

Then, we have $\mu_{Def}(M_f|H_p) = 1$ *since* $|A_{Def}^{H_p}| = 1$.

Concerning $\mu_{Att}(\cdot|M_l)$ *and* $\mu_{Def}(\cdot|R_n)$, *we have*:

- If $p = q$, we have $\text{Supp}(\mu_{Att}(\cdot|M_l)) = \{AP_p\}$ and

  – If $(1-\alpha)L_p > C_m$:
  $$\begin{cases} \mu_{Def}(M_s|R_n) = 1 \\ \mu_{Att}(AP_p|M_l) = 1 \end{cases}$$
  – If $(1-\alpha)L_p \leqslant C_m$
  $$\begin{cases} \mu_{Def}(\overline{M}|R_n) = 1 \\ \mu_{Att}(AP_p|M_l) = 1 \end{cases}$$

- If $p \neq q$, we have $\text{Supp}(\mu_{Att}(\cdot|M_l)) = \{AP_p, AP_q\}$ and

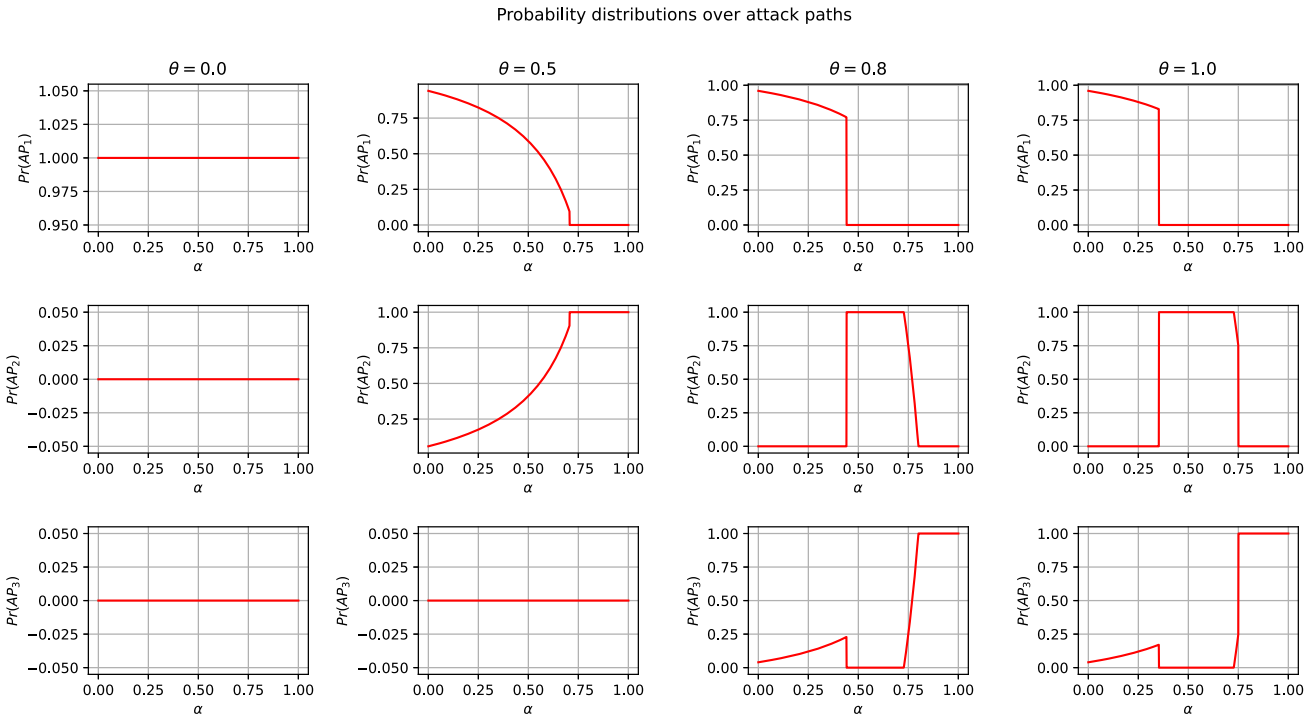

Fig. 5 Attacker's probability distribution over attack paths with respect to α

– If $(1-\alpha)L_q > C_m$:

∗ If $(1-\alpha)L_p > C_m$:

$$\begin{cases} \mu_{Def}(M_s|R_n) = 1 \\ \mu_{Att}(AP_q|M_l) = 1 \end{cases}$$

∗ If $(1-\alpha)L_p \leqslant C_m$:

$$\begin{cases} \mu_{Def}(M_s|R_n) = \mu_{Def}(\overline{M}|R_n) = \frac{1}{2} \\ \mu_{Att}(AP_q|M_l) = \mu_{Att}(AP_p|M_l) = \frac{1}{2} \end{cases}$$

– If $(1-\alpha)L_q \leqslant C_m$:

∗ $(1-\alpha)L_p < C_m$:

$$\begin{cases} \mu_{Def}(\overline{M}|R_n) = 1 \\ \mu_{Att}(AP_p|M_l) = 1 \end{cases}$$

∗ $(1-\alpha)L_p \geqslant C_m$:

$$\begin{cases} \mu_{Def}(M_s|R_n) = \frac{(1-\alpha)L_q - C_m}{(1-\alpha)(L_p - L_q)} \\ \mu_{Att}(AP_q|M_l) = \frac{1}{1-\alpha}\left(1 - \frac{C_p - C_q}{\theta(L_p - L_q)}\right) \end{cases}$$

5 Numerical results

The numerical results presented in this section are derived from identical order values of attack paths' characteristics and security parameters as those utilized in [43]. Table 8 summarizes those system parameters. In addition, we have $\forall\alpha,\theta[0,1]^2$, $Pr(M_{\overline{s}}) = 0$. Therefore, only $Pr(\overline{M})$ and $Pr(M_s)$ are plotted with respect to α and θ.

In Fig. 5, attacker's probability distribution with respect to the probability to identify the targeted VM after a secure migration is illustrated. For smaller values of θ, the attacker opts for the attack path with the lower cost, as he is unable to discern whether he is infiltrating a real network or a honeypot. This ambiguity arises because, after the reconnaissance phase, the attacker is unable to distinguish if the data gathered about the attack surface is from a honeypot or a real network. This is formally expressed as $\forall\alpha \in [0,1]$ $\Pr(AP_1) = 1$ for $\theta = 0$. As θ approaches 0.5 the attacker begins randomizing between AP_1 and AP_2. Moreover, if $\alpha > 0.75$ the attacker chooses the attack path AP_2 having

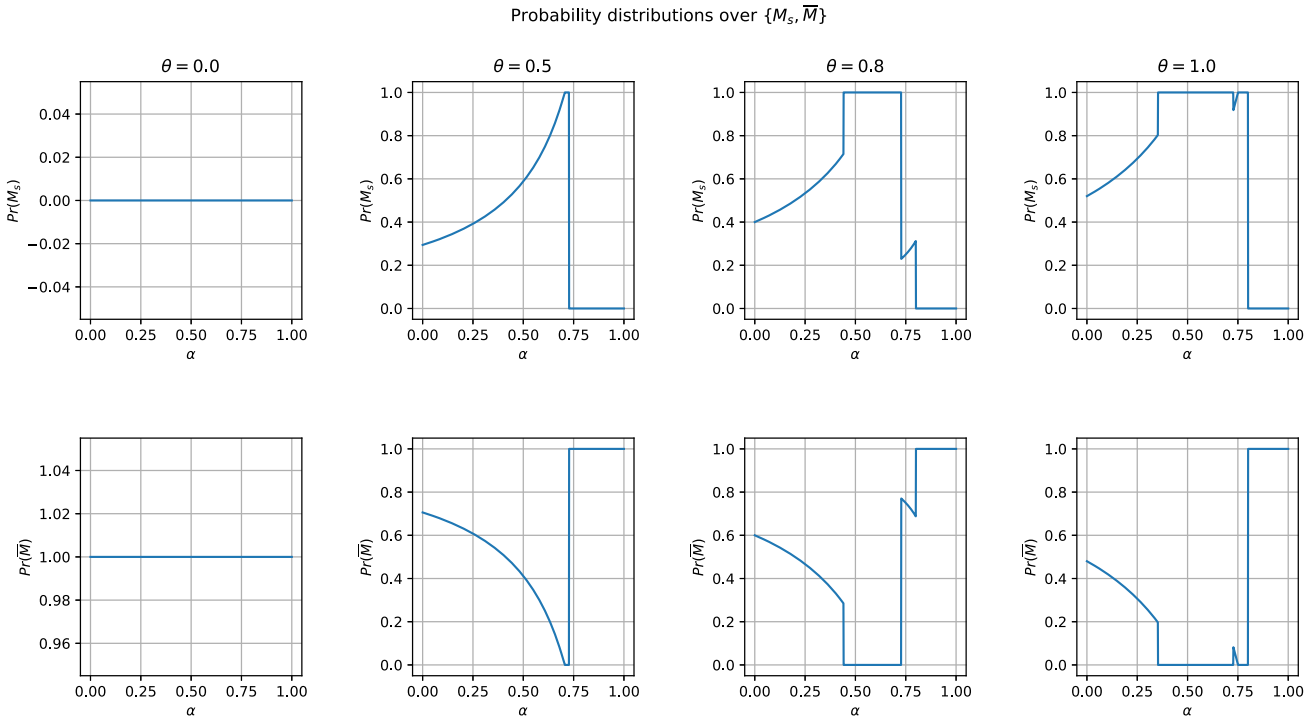

Fig. 6 Defender's probability distribution over M_s and $\overline{M}$ with respect to α

big impact on the VM than AP_1 despite the cost of the attack path AP_2 is greater than AP_1. In this scenario, the attacker is more confident about the data gathered during reconnaissance phase. In the other case when $\alpha < 0.75$, the attacker invest in AP_1 and this is due to the confusion made by the targeted VM migration. For $\theta \in \{0.8, 1\}$ and higher value of α, the attacker start investing in AP_3 with the highest impact on the targeted VM despite its cost wish is greater than those of AP_1 and AP_2. In this scenario, the targeted VM is completely discovered. Generally, figure 5 predicts the potential attack paths with respect to security system parameters quantitatively. Therefore, these results provide to the security network administrator the ability to detect insecure nodes in the network.

In Fig. 6, defender's probability distribution over M_s and $\overline{M}$ with respect to α is illustrated. For smaller value of θ, it is better to avoid the migration of the targeted VM. Moreover, secure migration in this scenario will cause only quality of service degradation and does not enhance security considerably. Quantitatively, this is show in the graph related to $\theta = 0$ in which we have $\forall \alpha \in [0, 1]$ $\Pr(\overline{M}) = 1$. Qualitatively, this is due to the ability of honeypot to confuse the attacker. For $\theta \in \{0.5, 1\}$ and $\alpha \in [0.4, 0.75]$, it is better to migrate the VM. In this case, the migration of the targeted VM has a great impact to secure the VM. When θ approaches 1 and $\alpha > 0.75$, the migration does not secure the VM. Indeed, the attacker has enough data to compromise it and urgent security measures should be established to avoid the attack. Based on security system parameters, the security network administrator is able to make a decision in which case the VM should be migrated and in which cases other security measures should be taken.

In Fig. 7, attacker's and defender's payoff with respect to α is are illustrated. For any value taken by α and θ if the attacker's payoff is negative, this latter will not have any attention to compromise the VM. Indeed, the attacker is rational and by the way he will not invest in any attack paths. From a defensive point of vue, the targeted VM is secure. For $\theta \in \{0.5, 0.8\}$ and α approaches 0.5 the payoff of the attacker is an increasing positive function. More precisely, he will invest in attack paths as described in Fig. 5. In this case, by combining the results of Figs. 5 and 7, we conclude in which scenarios the VM is targeted and which attack paths are potential. For value of $\theta = 1$ and α higher than 0.75, the attack surface of the targeted VM is clearly exposed to the attacker. Therefore, other measures of security should be established.

The proposed approach in this paper offer significant advantages in enhancing cloud security through the integration of Bayesian game theory and MTD techniques, such as virtual machine migration and honeypot deployment. However, several limitations and potential drawbacks need to be considered. Firstly, the cost and complexity of implementing these dynamic defense mechanisms can be high, including the resources needed

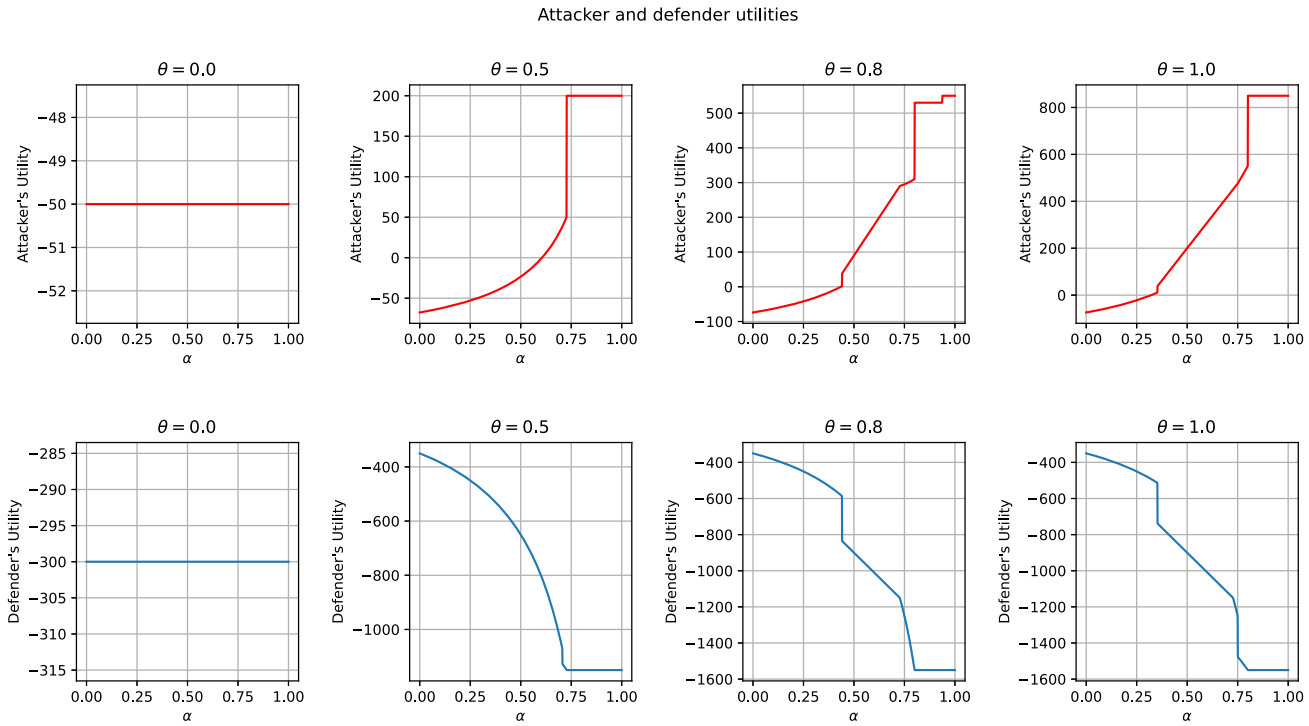

Fig. 7 Attacker's and defender's payoff with respect to α

for constant monitoring, migration, and honeypot maintenance. Additionally, the effectiveness of these strategies heavily relies on accurate and timely detection of threats, which can be challenging in large-scale and highly dynamic cloud environments. The inherent complexity of the game-theoretic models may also introduce computational overhead, potentially impacting the overall system performance. Furthermore, the approach assumes rational behavior from attackers, which may not always align with real-world scenarios where attackers could employ unpredictable strategies. Lastly, while the integration of MTD and honeypots enhances security, it does not eliminate the risk entirely, and there may still be unknown vulnerabilities that sophisticated attackers could exploit. Therefore, continuous evaluation and adaptation of these strategies are essential to address emerging threats and improve the resilience of cloud infrastructures.

6 Conclusion

In this work, attack graphs and Bayesian game theoretic approaches have been used to determine potential attack paths. It identifies which nodes in the network should be prioritized for security enhancement and identifies cases where a VM needs to be migrated based on system security parameters. Generally, these contributions assist the network administrator in deploying VM migration and honeypots in an optimized way. Our future work will aim to use machine learning and repetitive games to predict attacker's actions more efficiently and determine the scenarios in which case a VM should be migrated.

Author Contributions all authors contributed equally to this work

Data Availability Statement No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no Conflict of interest.

References

1. Butt, U.A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M.T., Albaqami, N.: Cloud security threats and solutions: a survey. Wirel. Person. Commun. **128**(1), 387–413 (2023)
2. El Kafhali, S., El Mir, I., Hanini, M.: Security threats, defense mechanisms, challenges, and future directions in cloud computing. Arch. Comput. Methods Eng. **29**(1), 223–246 (2022)
3. Tissir, N., El Kafhali, S., Aboutabit, N.: Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. J. Reliab. Intell. Environ. **7**, 69–84 (2021)
4. Tripathy, S., Sengupta, A., Jyotishi, A.: Looming Market Failure in Cloud Computing: A New Institutional Economics Perspective. Digital Policy, Regulation and Governance (2023)

5. Salah, K., El Kafhali, S.: Performance modeling and analysis of hypoexponential network servers. Telecommun. Syst. **65**, 717–728 (2017)
6. Alkasassbeh, M., Al-Haj Baddar, S.: Intrusion detection systems: a state-of-the-art taxonomy and survey. Arab. J. Sci. Eng. **48**(8), 10021–10064 (2023)
7. Tissir, N., El Kafhali, S., Aboutabit, N.: Cloud computing security classifications and taxonomies: a comprehensive study and comparison. In: 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), pp. 1–6 . IEEE (2020)
8. Zekri, M., El Kafhali, S., Aboutabit, N., Saadi, Y.: Ddos attack detection using machine learning techniques in cloud computing environments. In: 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), pp. 1–7 . IEEE (2017)
9. El Mir, I., Haqiq, A., Kim, D.S.: Collaborative detection and filtering techniques against denial of service attacks in cloud computing. J. Theor. Appl. Inform. Technol. **95**(24), 6902–6914 (2017)
10. Ilg, N., Duplys, P., Sisejkovic, D., Menth, M.: Survey of contemporary open-source honeypots, frameworks, and tools. J. Netw. Comput. Appl., 103737 (2023)
11. Dekel, E., Fudenberg, D., Levine, D.K.: Learning to play bayesian games. Games Econ. Behav. **46**(2), 282–303 (2004)
12. Zenitani, K.: Attack graph analysis: an explanatory guide. Comput. Secur. **126**, 103081 (2023)
13. Liu, J., Zhang, Y., Hu, H., Tan, J., Leng, Q., Chang, C.: Efficient defense decision-making approach for multistep attacks based on the attack graph and game theory. Math. Prob. Eng. **2020**, 1–12 (2020)
14. Zhu, Q., Başar, T.: Game-theoretic approach to feedback-driven multi-stage moving target defense. In: International Conference on Decision and Game Theory for Security, pp. 246–263. Springer (2013)
15. Lu, Z., Wang, C., Zhao, S.: Cyber deception for computer and network security: survey and challenges (2020). arXiv preprint arXiv:2007.14497
16. Singh, A., Kaur, H., Kaur, N.: A novel ddos detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in sdn network. Cluster Comput., 1–21 (2023)
17. Umamaheswari, A., Kalaavathi, B.: Honeypot tb-ids: trace back model based intrusion detection system using knowledge based honeypot construction model. Cluster Comput. **22**, 14027–14034 (2019)
18. Chiang, C.-Y.J., Venkatesan, S., Sugrim, S., Youzwak, J.A., Chadha, R., Colbert, E.I., Cam, H., Albanese, M.: On defensive cyber deception: a case study using sdn. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), pp. 110–115 . IEEE (2018)
19. Wang, L., Wu, D.: Moving target defense against network reconnaissance with software defined networking. In: Information security: 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings 19, pp. 203–217 . Springer (2016)
20. Jafarian, J.H., Al-Shaer, E., Duan, Q.: Openflow random host mutation: transparent moving target defense using software defined networking. In: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, pp. 127–132 (2012)
21. Sayed, M.A., Anwar, A.H., Kiekintveld, C., Kamhoua, C.: Honeypot allocation for cyber deception in dynamic tactical networks: a game theoretic approach. In: International Conference on Decision and Game Theory for Security, pp. 195–214 . Springer (2023)
22. El Mir, I., Chowdhary, A., Huang, D., Pisharody, S., Kim, D.S., Haqiq, A.: Software defined stochastic model for moving target defense. In: Proceedings of the Third International Afro-European Conference for Industrial Advancement—AECIA 2016, pp. 188–197 . Springer (2018)
23. Venkatesan, S., Albanese, M., Amin, K., Jajodia, S., Wright, M.: A moving target defense approach to mitigate ddos attacks against proxy-based architectures. In: 2016 IEEE Conference on Communications and Network Security (CNS), pp. 198–206 . IEEE (2016)
24. Sayed, M.A., Hemida, A., Kiekintveld, C., Kamhoua, C.: Strategic honeypot allocation in dynamic networks: a game-theoretic approach for enhanced cybersecurity (2024)
25. Kumar, K.C., Reddy, B.M., Tahaseen, N., Bista, B.B., Devi, S.G.: A cloud based honeycloud system for malicious detection using machine learning techniques. Educat. Admin. Theory Pract. **30**(4), 152–158 (2024)
26. Pawlick, J., Colbert, E., Zhu, Q.: A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. ACM Comput. Surv. (CSUR) **52**(4), 1–28 (2019)
27. Ren, J., Zhang, C.: A differential game method against attacks in heterogeneous honeynet. Comput. Secur. **97**, 101870 (2020)
28. Winterrose, M.L., Carter, K.M., Wagner, N., Streilein, W.W.: Adaptive attacker strategy development against moving target cyber defenses (2014). arXiv preprint arXiv:1407.8540
29. Abdallah, M., Naghizadeh, P., Hota, A.R., Cason, T., Bagchi, S., Sundaram, S.: Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs. IEEE Trans. Control Netw. Syst. **7**(4), 1585–1596 (2020)
30. Hasan, M.M., Rahman, M.A.: A signaling game approach to mitigate co-resident attacks in an iaas cloud environment. J. Inform. Secur. Appl. **50**, 102397 (2020)
31. Li, H., Shen, W., Zheng, Z.: Spatial-temporal moving target defense: a markov stackelberg game model (2020). arXiv preprint arXiv:2002.10390
32. Gill, K.S., Saxena, S., Sharma, A.: Gta-ids: game theoretic approach to enhance ids detection in cloud environment. Comput. Inform. **41**(3), 665–688 (2022)
33. Chen, L., Xiang, Z., Pan, B., Chen, D.: Defense mechanism based on game theory for securing cloud infrastructure against co-resident dos attacks. Int. J. Syst. Manag. Innov. Adop. **13** (2023)
34. Dong, M., Zhang, Z., Liu, Y., Zhao, D.F., Meng, Y., Shi, J.: Playing bayesian stackelberg game model for optimizing the vulnerability level of security incident system in petrochemical plants. Reliab. Eng. Syst. Saf. **235**, 109237 (2023)
35. Lee, D., Kim, D., Ahn, M.K., Lee, S.: Bayesian stackelberg game approach for cyber mission impact assessment. ICT Express (2023)
36. Zhang, H., Mi, Y., Liu, X., Zhang, Y., Wang, J., Tan, J.: A differential game approach for real-time security defense decision in scale-free networks. Comput. Netw. **224**, 109635 (2023)
37. Zhang, H., Mi, Y., Fu, Y., Liu, X., Zhang, Y., Wang, J., Tan, J.: Security defense decision method based on potential differential game for complex networks. Comput. Secur. **129**, 103187 (2023)
38. Hu, H., Liu, J., Tan, J., Liu, J.: Socmtd: selecting optimal countermeasure for moving target defense using dynamic game. KSII Trans. Internet Inform. Syst. (TIIS) **14**(10), 4157–4175 (2020)
39. Mi, Y., Zhang, H., Hu, H., Tan, J., Wang, J.: Optimal network defense strategy selection method: a stochastic differential game model. Secur. Commun. Netw. **2021**, 1–16 (2021)
40. Tan, J.-L., Lei, C., Zhang, H.-Q., Cheng, Y.-Q.: Optimal strategy selection approach to moving target defense based on markov robust game. Comput. Secur. **85**, 63–76 (2019)
41. Lei, C., Zhang, H.-Q., Wan, L.-M., Liu, L., Ma, D.-H.: Incomplete information markov game theoretic approach to strategy

generation for moving target defense. Comput. Commun. **116**, 184–199 (2018)
42. Huang, L., Zhu, Q.: A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. Comput. Secur. **89**, 101660 (2020)
43. Kandoussi, E.M., Hanini, M., El Mir, I., Haqiq, A.: Toward an integrated dynamic defense system for strategic detecting attacks in cloud networks using stochastic game. Telecommun. Syst. **73**(3), 397–417 (2020)
44. Samir, M., Azab, M., Samir, E.: Sd-cpc: Sdn controller placement camouflage based on stochastic game for moving-target defense. Comput. Commun. **168**, 75–92 (2021)
45. Zhu, Q., Başar, T.: Game-theoretic approach to feedback-driven multi-stage moving target defense. In: International Conference on Decision and Game Theory for Security, pp. 246–263. Springer (2013)
46. Maleki, H., Valizadeh, S., Koch, W., Bestavros, A., Van Dijk, M.: Markov modeling of moving target defense games. In: Proceedings of the 2016 ACM Workshop on Moving Target Defense, pp. 81–92 (2016)
47. Akshaya, S., Padmavathi, G.: Enhancing zero-day attack prediction a hybrid game theory approach with neural networks. Int. J. Intell. Syst. Appl. Eng. **12**(7s), 643–663 (2024)
48. Syed, N.F., Ge, M., Baig, Z.: Fog-cloud based intrusion detection system using recurrent neural networks and feature selection for iot networks. Comput. Netw. **225**, 109662 (2023)
49. Gill, K.S., Sharma, A., Saxena, S.: A systematic review on game-theoretic models and different types of security requirements in cloud environment: challenges and opportunities. Arch. Comput. Methods Eng. 1–34 (2024)
50. Kamhoua, C.A., Kwiat, L., Kwiat, K.A., Park, J.S., Zhao, M., Rodriguez, M.: Game theoretic modeling of security and interdependency in a public cloud. In: 2014 IEEE 7th International Conference on Cloud Computing, pp. 514–521 . IEEE (2014)
51. Thongthua, A., Ngamsuriyaroj, S.: Assessment of hypervisor vulnerabilities. In: 2016 International Conference on Cloud Computing Research and Innovations (ICCCRI), pp. 71–77 . IEEE (2016)
52. Ou, X., Govindavajhala, S., Appel, A.W., et al.: Mulval: a logic-based network security analyzer. In: USENIX Security Symposium, vol. 8, pp. 113–128 . Baltimore, MD (2005)

El Mehdi Kandoussi received the Ph.D. thesis in Computer Science from the Hassan First University of Settat, Morocco, in October 2020 and Engineering diploma in computer science from the University of Mohammed V in Rabat, Morocco, in September 2016. His research interests include cloud computing, game theory, and Markov decision process. He is Professor in The National Institute of Posts and Telecommunications (INPT) in Rabat, Morocco since 2020. M. Kandoussi does research in Computer science (resource allocation) and applied mathematics (modelling discrete system).

Adam Houmairi is currently a Ph.D. student in the school of applied science in Khouribga since 2022, he received a master of science and techniques in applied mathematics from Hassan First University of Settat, Morocco in 2017. He also received a degree in engineering from Grenoble INP ENSIMAG in 2014, he is an associate professor in preparatory classes since 2019. His research interests include cloud computing, queuing theory, and machine learning.

Iman El Mir is a professor at the Institute of Sciences of Sport, Hassan First University, Settat, Morocco. She earned her Ph.D. in Computer Science from Hassan First University in 2018. Her research focuses on security modeling and analysis of computers and networks, cloud data center security, security in software-defined networking, as well as machine learning and artificial intelligence. She has been involved in the NATO Project SPS-984425, titled "Cyber Security Analysis and Assurance using Cloud-Based Security Measurement System." Additionally, she has served as a Technical Program Committee member and organizing committee member for various international conferences and workshops, and has reviewed for several international journals.

Mostafa Bellafkih received the Ph.D. thesis in Computer Science from the University of Paris 6, France, in June 1994 and Doctorat Es Science in Computer Science (option networks) from the University of Mohammed V in Rabat, Morocco, in May 2001. His research interests include the network management, knowledge management, A.I., Data mining and Database. He is Professor in The National Institute of Posts and Telecommunications (INPT) in Rabat, Morocco since 1995. M. Bellafkih does research in Computer Communications (Networks), Information Systems (Business Informatics) and Intelligent System.