Computers & Security 92 (2020) 101742

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Moving target defense in cloud computing: A systematic mapping study

Matheus Torquato[a,b,*], Marco Vieira[a]

[a] Department of Informatics Engineering, University of Coimbra, Coimbra, Portugal
[b] Federal Institute of Alagoas, Campus Arapiraca, Arapiraca, Brazil

ARTICLE INFO

Article history:
Received 30 October 2019
Revised 25 January 2020
Accepted 1 February 2020
Available online 3 February 2020

Keywords:
Moving target defense
Cloud computing
Systematic mapping
Cyber security
Network security

ABSTRACT

Moving Target Defense (MTD) consists of applying system reconfiguration (e.g., VM migration, IP shuffling) to dynamically change the available attack surface. MTD makes use of reconfiguration to confuse attackers and nullify their knowledge about the system state. It also can be used as an attack reaction (e.g., using Virtual Machine (VM) migration to move VMs away from a compromised host). Thus, MTD seems to be a promising technique to tackle some of the cloud computing security challenges. In this systematic mapping study, we aim to investigate the current research state of Moving Target Defense in the cloud computing context, and to identify potential research gaps in the literature. Considering five major scientific databases in the computer science domain, we collected 224 papers related to the area. After disambiguation and filtering, we selected 95 papers for analysis. The outcome of such analysis offers a comprehensive overview of the current research. We can highlight some relevant research opportunities. First, only a few works present advances in the theoretical field of Moving Target Defense in cloud computing. Second, the proposal and evaluation of multi-layer Moving Target Defense mechanisms is still an open problem. Thirdly, there is a need for frameworks to support MTD evaluation, which may include a benchmark for comparing alternative MTD strategies. Finally, the study of potential impacts of Moving Target Defense in context-oriented clouds is a barely explored topic.

1. Introduction

Cloud computing is a computing paradigm that enables ubiquitous, on-demand network access to a configurable set of resources (e.g., computing, storage, network, and services) (Mell et al., 2011). Cloud computing reduces the up-front cost for its users, allowing a gradual increase or decrease of resources allocation, adapting the available computing power to the existing needs (Armbrust et al., 2010). Due to its characteristics, many companies and organizations rely on cloud computing to run their applications.

Existing surveys show that cloud computing security is at the top of users' concerns (RightScale, 2018). Besides that, cloud computing security and privacy persist as significant research challenges (Krutz and Vines, 2010; Ren et al., 2012).

In this context, Moving Target Defense (MTD) has emerged as a low-cost technique to improve cloud computing resiliency and security. The United States Department of Homeland Security defines MTD as *the concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts. MTD assumes that perfect security is unattainable. Given that starting point, and the assumption that all systems are compromised, research in MTD focuses on enabling the continued safe operation in a compromised environment and to have systems that are defensible rather than perfectly secure* (hls, 2018).

In this paper, we aim to investigate the current research state of MTD in cloud computing. To achieve this goal, we adopted a systematic mapping approach (Petersen et al., 2008; 2015). From systematic maps, we can understand the focus of community research efforts and also perceive what areas are barely explored. The systematic mapping process aims to reduce bias in papers classification by applying a well-defined methodology. Mapping studies provide a good overview of a research topic and are useful before starting more deep research works (Kitchenham et al., 2010).

The current literature provides comprehensive surveys and review papers on Moving Target Defense. Lei et al. (2018a) focus on the characteristics of moving target defense techniques. Cai et al. (2016b) presents a comprehensive survey on Moving Target Defense. Besides these two works, two relevant surveys in the

* Corresponding author.
E-mail addresses: mdmelo@dei.uc.pt, matheus.torquato@ifal.edu.br (M. Torquato), mvieira@dei.uc.pt (M. Vieira).

https://doi.org/10.1016/j.cose.2020.101742
0167-4048/

area were recently published (Sengupta et al., 2019b; Zheng and Namin, 2019). Two books from Jajodia et al. in this same topic can also be found in the literature (Jajodia et al., 2012; 2011). Different from all these works, our paper is focused on the cloud computing context. Besides that, instead of surveying the papers, our goal is to use a structured approach (i.e., systematic mapping) to provide a comprehensive overview of MTD in the cloud.

Our analysis shows a growing interest in MTD in the cloud computing context. Current research is focused on proposing and evaluating MTD techniques based on environment reshuffle (like VM migration or dynamic network reconfiguration). There are few papers regarding MTD theory, and there is a need for unified methodologies to support MTD evaluation and comparison. Also, the combination of MTD strategies requires further research. In practice, this paper presents a comprehensive overview of MTD in cloud computing research. The diagrams and charts presented intend to provide useful information for the community on the current state of the research in the area.

The rest of this paper is organized as follows. Section 2 presents some background about cloud computing security. Section 3 presents motivations for conducting this research. Section 4 introduces the methodology adopted for map construction. Section 5 presents the results in terms of the papers collected from the scientific databases. Section 6 presents the maps obtained. Section 7 discusses the maps and the main observations. Finally, Section 8 concludes the paper.

2. Cloud computing security

Cloud computing architecture and intrinsic characteristics raise several security concerns. For example, Popović and Hocenski (2010) show that the cloud security concerns that range from the *location of the encryption and decryption keys* to the *auditability of VMs*. Due to the relevance of this question, cloud computing security usually appear as a significant research challenge (Buyya et al., 2018; Ren et al., 2012).

One of the challenging problems for cloud security is the asymmetric advantage of attackers over defenders. Attackers can perform a series of actions (e.g., repeated attacks, vulnerability analysis) until they achieve their goal. So, the attackers can try to exploit a specific system vulnerability while the defenders have to protect all the possible attack venues (Cai et al., 2016b). Besides that, the generally static nature of data centers facilitates the attacker to obtain enough information to improve the chance of attack success.

Moving Target Defense applies dynamic environment reconfiguration capable of confusing attackers or reacting to an attack in progress. For example, to minimize the attackers' asymmetric advantage, we can apply a dynamic network address shuffle (Fleck et al., 2018). Moreover, as an attack reaction, we can use VM migration to save benign clients from the security attack (Jia et al., 2014).

3. Motivation

Fig. 1 shows the Google search trends for the term "Moving Target Defense" in the last ten years. It is possible to notice a growing interest in the field in the last ten years. As we will show in this paper, the same occurs in the number of papers published in the last years. Due to the urgency in the development of innovative techniques to protect cloud computing systems, the MTD attracted significant attention because of its flexibility. As mentioned earlier, it is possible to deploy MTD to confuse attackers and also to react to attacks in progress.

However, compared to the established defense mechanisms as firewalls and Intrusion Detection Systems (IDS) (Bonguet and Bellaiche, 2017), MTD technique is a newer technology and the related

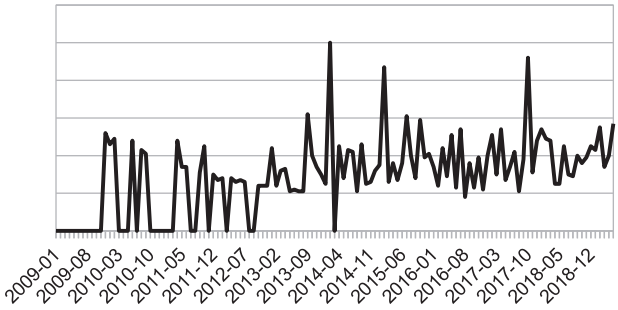

Fig. 1. Google trends - "Moving Target Defense" - Jan 1, 2009 to July 5, 2019.

research in the area is incipient. MTD draws attention because of the idea of accepting imperfect security (hls, 2018) and applying dynamic changes in the environment to protect it. Nevertheless, there are challenges in the MTD deployment as how to apply the dynamic changes, when to apply them, and how to evaluate their effectiveness (more details of MTD in the cloud research opportunities in Section 7).

Recent papers tackled such challenges. For example, the papers (Alavizadeh et al., 2019; Hong et al., 2018) presented evaluation mechanisms for MTD. Sengupta et al. (2019a) leveraged from a Markov Game to provide optimal strategies for security resources placement. Das et al. (2019) used a process to obfuscate VM migration in the cloud environment, reducing the attacker's chance to recognize it. Peng et al. (2014b) propose MTD techniques based on polymorphism, rapid provisioning of defenses, and defensive mechanisms to facilitate unauthorized access detection.

The usual first step of research projects (as Ph.D. studies) is to understand the state-of-the-art in the related field. The systematic mapping aims to bring an overview of such state-of-the-art, usually focusing on specific aspects of the literature. Different from systematic reviews, which discuss the related papers in detail, the systematic mappings focus on specific aspects and perform a more concise analysis of the papers. The main advantage of the systematic mappings is to usually provide faster results, as they focus on the desired papers' aspects. Besides that, the visual data (maps) facilitates the understanding of the state of the literature.

The current literature of MTD in the cloud lacks a systematic mapping. This work intends to fill this gap proposing a mapping from the last ten years of the research in the area. The scientific may leverage our work for understanding the current state of the MTD in cloud research, as well as on the definition of future research lines.

4. Methods

The systematic mapping process is based on the work by Petersen et al. (2008). Fig. 2 presents the process steps and outcomes, which will be described in the following sections.

4.1. Research questions

The main goal of this systematic mapping study is to provide an overview of recent research on Moving Target Defense mechanisms in cloud computing environments. To reach this goal, we propose three generic research questions:

- *RQ1:* How has the frequency of publication on moving target defense in cloud computing changed in the last ten years?
- *RQ2:* In which forums have research on moving target defense on cloud computing been published?
- *RQ3:* What are the most researched techniques for moving target defense on cloud computing?

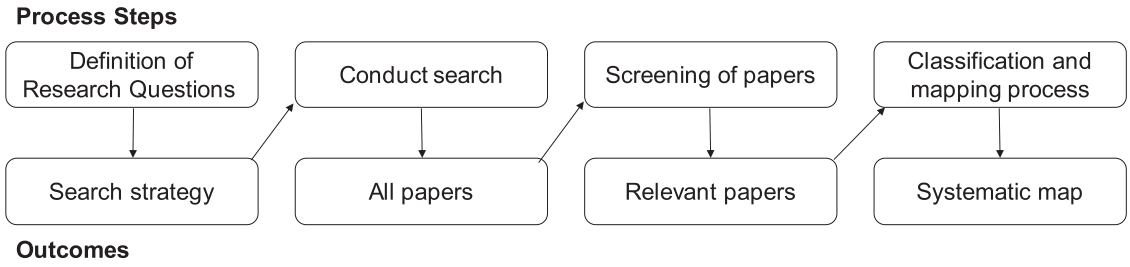

Fig. 2. Systematic mapping process.

The first two questions aim to give an overview of publication frequency and relevant forums of publication. The third question, which is the most important, seeks to offer a bigger picture of the relations of MTD techniques and cloud computing.

We also analyzed the considered papers to find the most prominent authors from the field (i.e., authors with more publications) and to verify the existence of related research of the same set of authors (i.e., identifying papers and their potential extensions).

4.2. Scientific databases and search strategy

We selected five relevant online computer science computer databases to find the papers related to MTD in the cloud. We decided to use them instead of generic databases, such as *Scopus* and *Web of Science*, because some papers may be missing from these generic platforms (e.g., early access papers). We neglected the *Google Scholar* database because it indexes non-peer reviewed papers. The list of the selected databases is the following:

- ACM Digital Library;
- IEEE Xplore Digital Library;
- ScienceDirect;
- SpringerLink;
- Online Wiley Library.

The search string is the following:

("moving target defense") AND ("cloud")

The first part of the search string is related to moving target defense, and the second is related to cloud computing. We decided to neglect the use of the acronym "MTD" in the search process because it is an ambiguous acronym. MTD can be related to Moving Target Defense, Managing Technical Debt, Mixture Transition Distribution, Mean Texture Depth, or Machine-Type Device. Thus, we assume that relevant works have at least one direct mention of the term "moving target defense".

In the second part of the search string, we decided to use only the word "cloud" instead of its derivatives (e.g., IaaS, Cloud Computing, Cloud environment). With this, we assume that the papers within our research scope mention the word "cloud" directly.

4.3. Screening of papers

We determined the inclusion and exclusion criteria to filter the search results. Our goal is to select the relevant research of MTD in the cloud in the last ten years (i.e., as in *RQ1*). Thus, our paper selection process intends to cover the peer-reviewed papers about the subject. The research on MTD in the cloud is relatively new when compared to consolidated areas (as performance evaluation, for example), meaning that incipient research may have been published in small conferences or workshops. Therefore, we do not apply filters related to the rank/quality of the considered venues of publication. Finally, we also removed the survey papers from the search results as we intend to analyze the individual contributions from the papers instead of a compilation of papers. The adopted filtering strategy is summarized below.

- *Inclusion criteria*
  - Research papers about moving target defense techniques applied in cloud computing.
    - Papers with direct reference to cloud computing and moving target defense in their titles, abstracts, keywords or introduction.
  - Papers published in journals, magazines or conference proceedings.
- *Exclusion criteria*
  - Papers published before 2009.
  - Papers not written in the English language.
  - Surveys.

We applied these criteria in a step-by-step process using the available filters on the webpage of each scientific database considered. We decided to include only papers from journals, magazines, and conference proceedings because these are usually peer-reviewed. However, we highlight that some considered papers from the Springer database are also published as book chapters.

4.4. Classification

Following the classification presented in Cai et al. (2016a) and Okhravi et al. (2013), we propose a classification with four categories: (i) MTD research area; (ii) MTD strategy; (iii) evaluation metrics; and (iv) platform considered. These categories aim to cover the meaningful aspects of each paper, considering our research questions. Our classification approach is transverse in all the proposed categories, meaning that a paper classification can comprise more than one group of each proposed category. The details of each category are discussed in the following paragraphs.

4.4.1. MTD research area

In this category, we aim to classify the type of research published observing the classification proposed in Cai et al. (2016a). The category has three groups, Theory, Strategy, and Evaluation, as follows:

- **Theory** - Find answers to fundamental questions regarding MTD techniques.
  - How to create effective MTD system?
  - What capabilities and features are essential to MTD systems?
- **Strategy** - Propose a technique for MTD.
- **Evaluation** - Measure the effectiveness of existing (or proposed) strategies.

As mentioned before, we consider that a paper can be classified in more than one category. For example, some papers propose and evaluate a mechanism for MTD on the cloud. Therefore, these papers are classified as *Strategy + Evaluation (S+E)*.

4.4.2. MTD strategies

While the research area category is quite generic, we assume that MTD strategies are more focused on cloud computing environments. We organize the papers using the groups proposed by Okhravi et al. (2013). We have thus three groups:

- ***Dynamic application*** - which comprises dynamic *data* (change data format, syntax or encoding), dynamic *software* (dynamic changes on the application code), and dynamic *runtime environment* (address space randomization or instruction set randomization).
- ***Dynamic platform*** - dynamic changes on the platform configurations, including Operating System (OS) version, CPU architecture or OS instance. We can deploy a *Dynamic Platform* MTD in the cloud using VM migration or VM placement techniques.
- ***Dynamic Network*** - change network properties (e.g. IP address or network protocols) dynamically.

4.4.3. Evaluation metrics

The deployment of an MTD mechanism implies costs for system performance while improving the system security. Therefore, we intend to understand which evaluation metrics are currently used in MTD in cloud research. We propose only two groups for this category:

- ***Performance***, evaluation comprises performance metrics, such as response time, system overhead, *etc*;
- ***Security***, evaluation covers security aspects, such as attack success rate, survivability, *etc*.

4.4.4. Platform considered

This category has no predefined groups. We aim to fill the category using a bottom-up approach. Thus, we propose the category groups after the analysis of the papers. This category can reveal the correlation between cloud computing and other platforms (e.g., Software Defined Networks or Virtualized Containers).

4.5. Threats to validity and limitations

There are threats to validity in systematic mapping research. It is important to highlight the adopted approaches to avoid or minimize them. In the scope of our work, we can highlight the following threats to validity: (i) *weak search string*; (ii) *scientific database limitation*; and (iii) *classification bias*.

About threat (i), weak search strings may result in a reduced search result lacking relevant papers of the considered area. We decided to use a generic search string instead of the composition of specific search strings (as presented in Section 4.2). Therefore, we collected a reasonable amount of papers from scientific databases. The drawback of applying generic search strings is the increased subjective classification effort. When using the generic search string, we ended up finding many papers about MTD that also mention the word “cloud” as a concept or related work. We carefully classified these papers to avoid mistakes in the paper selection process.

About threat (ii), we decide to include five relevant scientific databases in the computer science area, as presented in previous systematic mapping studies (Fernandez et al., 2011; Roberto et al., 2016).

Finally, about threat (iii), as the analysis of paper inclusion/exclusion was made by the authors, the classification may be biased. However, we did put a reasonable effort to reduce classification bias by analyzing more paper content than just the abstract. Besides that, to improve our classification process, we performed two separate rounds of the full systematic mapping process, one in November 2018 and a confirmation round in July 2019. In the confirmation round, we analyzed all the papers from the previous round (to confirm the classification). Besides that, we added the papers published between the rounds. The results presented here are from the confirmation round.

Besides the threats to validity, we emphasize the following limitations in our research approach. Firstly, our research focuses on the deployment of MTD techniques in the cloud computing environment. As we mentioned earlier, we used a generic search string to find the relevant papers in the context. However, there may be other papers which do not mention ”cloud” directly but apply to the virtualized environment. These papers will require a more in-depth analysis, which is out of the scope of this paper.

Moreover, considering the number of collected papers, we performed the second step of papers filtering manually (exclusion of surveys, editorials, keynote, and duplicate entries). Thus, our approach has some scalability issues. A procedure to overcome this limitation is the development of a software (script) capable of conducting automated paper collection and filtering.

5. Results

The search was made between 5 and 16 of July 2019 and resulted in 224 papers. The first step was to apply the selection criteria using the automated filters provided in each database webpage. Following the proposed criteria, the automated filters help to exclude papers published before 2009 and papers that were not published in journals, magazines, or conference proceedings. This step resulted in a set of 163 papers. The second step of the process was performed manually and consisted of the exclusion of editorial papers, keynote papers, surveys, or duplicated entries. The manual work is as follows. We downloaded all the papers and performed a quick analysis of them to notice whether they are editorial, keynote, or survey papers. We removed all the papers in these categories, along with the duplicated entries. Unfortunately, we have to conduct this work by hand because the automated search bases do not offer the filtering for these types of papers. This step reduced the to 95 the set of papers eligible for analysis. The step-by-step process for each paper is presented in Fig. 3.

Fig. 3 shows that the most relevant database is the IEEEXplore, which provided 40 papers for the analysis (42.1% of the total). The rest of the databases provided: SpringerLink - 29 papers (30.52%), ScienceDirect - 14 papers (14.73%), ACM Digital Library - 10 papers (10.52%), and Wiley Online Library - 2 papers (2.1%).

RQ1 is related to the frequency of publication of papers on MTD in Cloud computing. Fig. 4 shows the annual trend since 2011. We did not find any published in 2009 and 2010. It is possible to observe a growing research interest in MTD in cloud computing. Note that the data for 2019 is still incomplete (because of the date of the search), so the number of publications is expected to increase.

Table 1 presents the most relevant publication forums. It provides the answer to *RQ2. ACM Workshop on Moving Target Defense* is the flagship forum with five papers. We noticed that the publication forums are diverse, as more than 80% of the papers are from forums that provided less than three papers for our analysis. Some papers from the *Procedia Computer Science* journal are extended versions of previous conference papers.

We also analyzed the distribution of papers according to the type of publication forum. Fig. 5 presents the proportion of papers published in the three types of forums. As expected, papers in conferences and workshops represent the majority of the published papers. Journals and magazine papers usually pass through a rigorous review process, which can lead to fewer papers published in such forums.

Each paper was classified using the scheme presented in Section 4. The complete list of the selected works is available on-

Table 1
List of the most relevant publication forums.

Forum	Type of forum	Number of papers	Percentage of the total
ACM Workshop on Moving Target Defense	Workshop	5	5.26%
Procedia Computer Science	Journal	4	4.21%
IEEE International Conference on Cloud Computing	Conference	3	3.16%
Frontiers of Information Technology & Electronic Engineering	Journal	3	3.16%
Future Generation Computer Systems	Journal	3	3.16%
Other 64 forums	-	77	81.05%

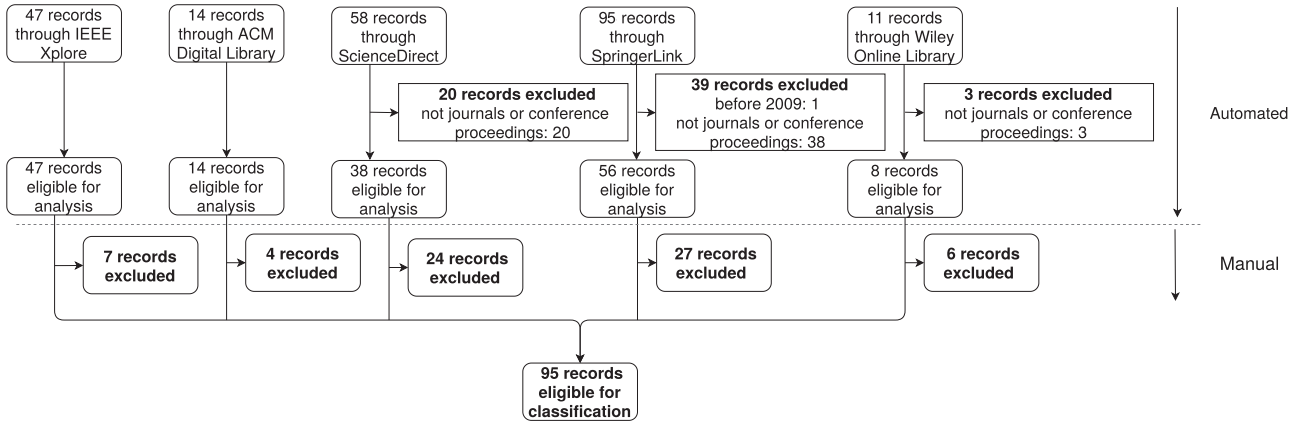

Fig. 3. Paper selection process.

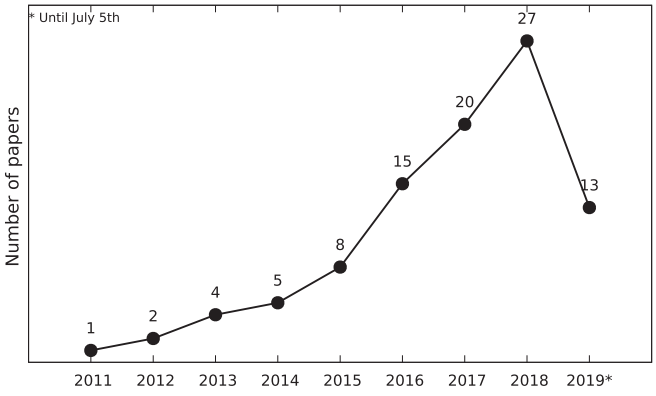

Fig. 4. Publications over time with annual trend.

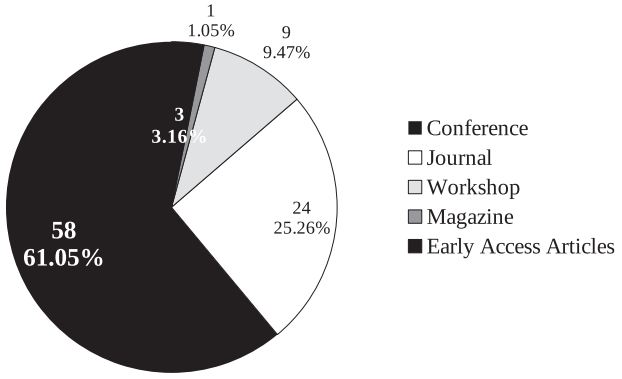

Fig. 5. Publications classification - type of forum.

line[1]. The research community can send new entries or suggestions for improving the classification using a link on the same web page.

[1] https://www.matheustorquato.com/publications/systematic-map-of-moving-target-defense-on-cloud-computing.

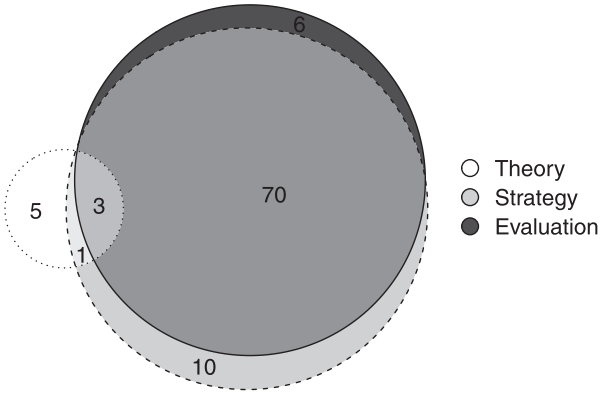

Fig. 6. Research area classification.

6. Mapping

This section provides an overview of Moving Target Defense in cloud computing research. We present charts and diagrams with the distribution of publications regarding the classification mentioned earlier.

6.1. Research area - papers distribution

The first map is a Venn Diagram of the distribution of papers in terms of theory, strategy, and evaluation (see Fig. 6). We noticed that most papers propose an MTD strategy and present its evaluation. As we have books and seminal papers to support MTD theory (Jajodia et al., 2012; 2011; Zhuang et al., 2014), the scientific community seeks to offer more approaches to enhance the available set of MTD mechanisms. However, theoretical papers usually provide more generic contributions on the use of MTD in other scenarios (not only cloud computing). For example, Leslie et al. (2015) propose a model based on game theory to support resources configuration to reduce the likelihood of a secu-

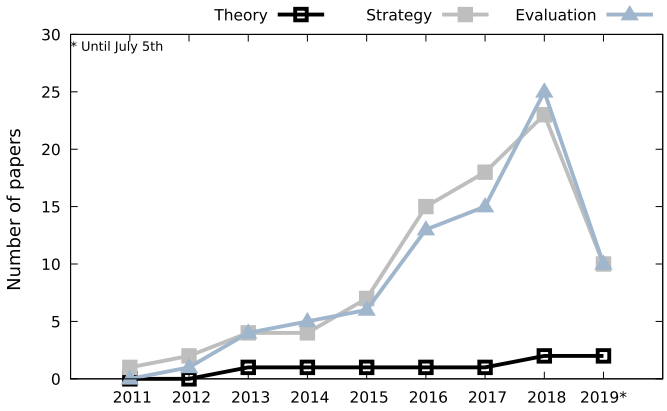

Fig. 7. Research area classification - publications over time.

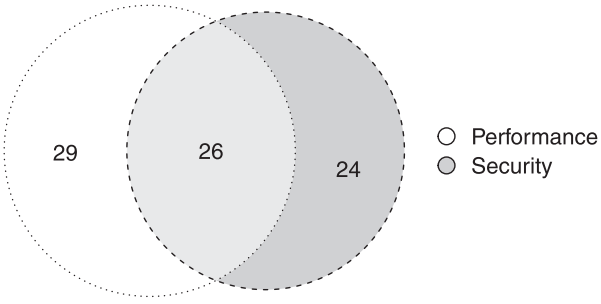

Fig. 8. Evaluation approaches - papers distribution.

rity attack. Lei et al. (2018b) also propose an approach based on game theory. Their proposal consists of an incomplete information Markov game theory comprising a moving attack surface and optimal strategy selection. The papers (Peng et al., 2014a; Song et al., 2019; Wang et al., 2016) are in the intersection between theory, strategy, and evaluation. Besides proposing an MTD strategy and its evaluation, they present a robust theoretical framework with models and algorithms.

Papers that propose generic evaluation methods are useful to support the comparison of MTD techniques. The papers from Alavizadeh et al. (2018a, 2018b, 2017) provide a modeling framework for the evaluation of MTD in cloud environments. The authors cover relevant security aspects as return on the attack, attack cost, and the probability of attack success. Their results also comprise a comparison between a system with and without MTD deployments.

We also studied the evolution in terms of the number of papers published over time. The plot in Fig. 7 is inclusive, meaning that the paper is counted in each research area that it resides. For example, if a paper is about an MTD strategy and its evaluation, we count this paper in the STRATEGY category and also in the EVALUATION category. It is noticeable that papers on theory received less attention from the research community in the last years. Theoretical papers focused on the aspects of cloud computing and how to deploy effective MTD in the cloud are an exciting aspect for future research.

6.2. Evaluation metrics - papers distribution

Fig. 8 presents a Venn diagram with the distribution of the metrics found in the selected papers. We noticed a balanced distribution of papers in the proposed classification. Papers that include a performance evaluation usually focus on the overhead caused by the proposed (or evaluated) MTD strategy. For example, Yang and Cheng (2018) present an MTD based on Software Defined Network (SDN). Among their results, the authors compared the response time of the application when using their proposal with the traditional MTD strategies. Wang et al. (2016) propose a cost-effective MTD against Distributed Denial of Service (DDoS) and Covert Channel Attacks. Their performance evaluation covers the cost per minute of using different variations of MTD algorithms.

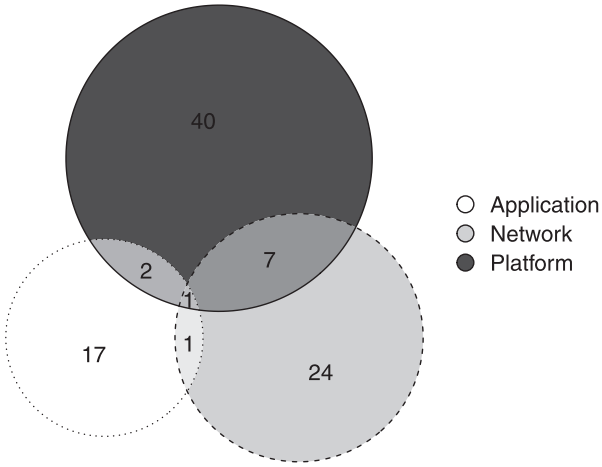

Fig. 9. Strategy classification.

The specific assumptions of each research impose barriers for the comparison of different MTD strategies. The security evaluation metrics considered in the works analyzed tend to be related to specific aspects to characterize the proposed MTD effectiveness. The metrics are usually defined by the authors and applied in their specific context. For example, the study from Sianipar et al. (2018) is focused on the Meltdown and Spectre vulnerabilities. Therefore, their results are based on Spectre and Meltdown effectiveness while applying their approach. Wang et al. (2014) propose an MTD solution as a DDoS defense. The evaluation comprises the percentage of clients saved based on the number of shuffles. Wahab et al. (2019) propose a comprehensive framework for MTD deployment in the cloud. Their framework comprises several techniques and methods, including a risk assessment methodology and a machine learning approach to collect information from malicious activities. In the evaluation, the authors use two primary metrics: percentage of attack detection and survived services.

The most recurrent security metric is related to the MTD impact in the attack success rate (Debroy et al., 2016; Ma et al., 2016; Nguyen et al., 2018; Zhang et al., 2016b). However, it is still challenging to set up a direct comparison between the papers due to their particular assumptions. The development of a unified approach for MTD evaluation is an open problem.

6.3. Strategy - papers distribution

This section presents an overview of the type of MTD strategies applied in cloud computing. The results presented here provide answers to *RQ3*. Fig. 9 presents a Venn diagram with the distribution of the proposed MTD strategies. As mentioned in Section 4, each set in the Venn diagram corresponds to MTD strategies related to the dynamic application, dynamic network, and dynamic platform.

We noticed that most of the MTD techniques leverage cloud computing inherent features. For example, MTD based on the dynamic platform usually relies on Virtual Machine (VM) migration for the environment reconfiguration. In this context, VM migration is usually used to defend against side-channel attacks (Adili et al., 2017; Azab et al., 2017; Kashkoush et al., 2018; Moon et al., 2015; Yang et al., 2019; Zhang et al., 2012).

Liu et al. (2018) present an MTD approach against side-channel attacks based on dynamically scheduling VM computing resources. Agarwal and Duong (2019) propose a different MTD solution to defend against side-channel attacks using a VM placement technique. They propose an algorithm to reduce the probability of malicious VM co-location. Also using VM placement techniques, Ahmed and Bhargava (2016) propose a MTD framework based on the creation and deletion (*reincarnation*) of VMs. To improve security, the authors dynamically change the OS instance on the VM in each *reincarnation* round. Jia et al. (2014) present an MTD mechanism to isolate attacked servers from benign clients during DDoS attacks. Their approach consists of turning victim servers into moving targets. Penner et al. work (Penner and Guirguis, 2017) leverage on both VM migration and VM placement techniques to provide a comprehensive MTD mechanism for cloud computing.

Dynamic network approaches are usually based on network address hopping techniques (El Mir et al., 2017; Groat et al., 2013; Luo et al., 2016). Kurra et al. (2013) present an MTD mechanism based on data partitioning and key hopping. Using key hopping mechanisms, the authors can reduce the length of keys to improve system performance while maintaining system security levels. Fleck et al. (2018) propose dynamic changes on the IP addresses of proxies to thwart the reconnaissance phase of attacks. Lysenko et al. (2018) also propose dynamic network configurations to protect a Corporate Area Network.

Regarding MTD techniques related to the dynamic application approach, we highlight that the most used technique is *Software Behavior Encryption* (SBE). SBE is usually applied using a dynamic selection of functionally-equivalent software variants at runtime (Dsouza et al., 2013; Hosseinzadeh et al., 2015; Le Goues et al., 2013). The oldest paper in our classification (Azab and Eltoweissy, 2011) also applies SBE in the context of Cyber-Physical Systems (CPS). The authors used the *ChameleonSoft*, a biological-inspired MTD framework that provides software diversity at runtime.

Finally, we highlight that just one paper (Chung et al., 2015) propose a framework (SeReNe) comprising all the three layers (application, network, and platform). However, SeReNe is still in a conceptual phase and lacks practical implementation and evaluation.

6.4. Platforms - papers distribution

In this category, we aim to understand whether the papers are only focused on cloud computing or are also considering other platforms. We find this category useful to identify cross-platform MTD strategies or to perceive how cloud may support the application MTD in other scenarios. We found out that the majority of papers are focused only on cloud computing instead of considering the use of cloud computing in conjunction with other platforms (e.g., Software Defined Networking or Virtualized Containers). However, there is a non-negligible set of papers considering these other platforms. An interesting example is a paper from Kahla et al. (2018), which proposes a technique for Fog computing and the Internet of Things (IoT). Some papers leverage the flexibility of Software Defined Networks (SDN) to propose more robust MTD solutions (Chowdhary et al., 2016; Urias et al., 2015; Villarreal-Vasquez et al., 2017). Due to lightweight virtualization overhead, some research works aim to deploy MTD using virtualized containers (Jin et al., 2019; Torkura et al., 2018). The overall results are presented in Fig. 10.

We highlight the paper from Pacheco et al. (2016), which applies MTD on top of the cloud but focusing on the smart city context. The authors compared the performance levels with and without using MTD. Lei et al. paper (Lei et al., 2018b) has a generic context. Thus, it is hard to classify it in a single category of this classification. Therefore, we decided to exclude this paper from the classification of this specific subsection of our systematic mapping.

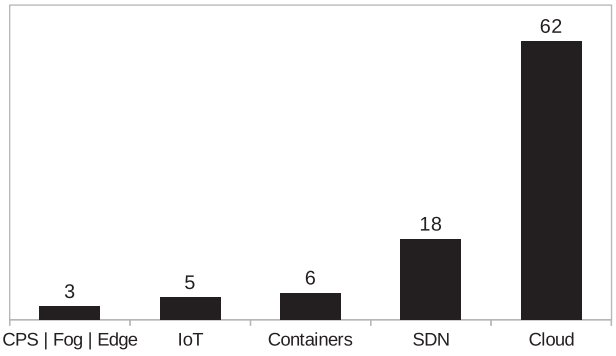

Fig. 10. Considered platform category.

6.5. Research area and strategy - classification relationship

The bubble chart in Fig. 11 presents the relationship between the research area and strategy categories of the selected papers. Bubble charts simplify the identification of research gaps and the areas that received the most attention from the research community.

As mentioned earlier, most papers propose an MTD strategy and its evaluation (*S+E* category). Moreover, among these papers, the majority use dynamic platform strategies. There are three theoretical papers (Bazm et al., 2017; Lei et al., 2018b; Leslie et al., 2015) that study generic MTD theory without focusing on specific strategies. Some papers propose MTD strategies but lack the evaluation of their effectiveness. MTD Theory receives less attention than the other areas from the research community. The paper from Casola et al. (2018) was classified as theory and strategy because, besides presenting a security SLA-driven MTD framework, it presents a strong theory about cloud applications and security SLAs.

6.6. Platform and strategy - classification relationship

Fig. 12 presents the relationship between platforms and strategies. We noticed that the papers from the cloud category usually apply dynamic platform techniques, as presented in Section 6.3. Besides that, we noticed that MTD approaches for virtualized containers also tend to leverage from dynamic platform techniques. For example, Azab et al. (2016a,b) present an MTD based on the live migration of virtualized containers to avoid security attacks.

The majority of the papers that use dynamic network MTD approaches leverages the flexibility of the SDN paradigm. The strategies vary from usual IP mutation (Chang et al., 2018; Zhang et al., 2016a) and port hopping (Chowdhary et al., 2018) to route randomization (Aydeger et al., 2019; Karim et al., 2019).

6.7. Authors analysis

Some of the considered papers in our systematic mapping are closely related. For example, there are papers from the same authors published in conferences and journals, which have similar goals (e.g., Kashkoush et al., 2017; Kashkoush et al., 2018). In such cases, we consider both papers in our analysis (i.e., conference and journal versions). As our *RQ1* is related to the frequency of paper publication, we decided to maintain both versions in our analysis to provide a more precise overview of the literature in the last ten years.

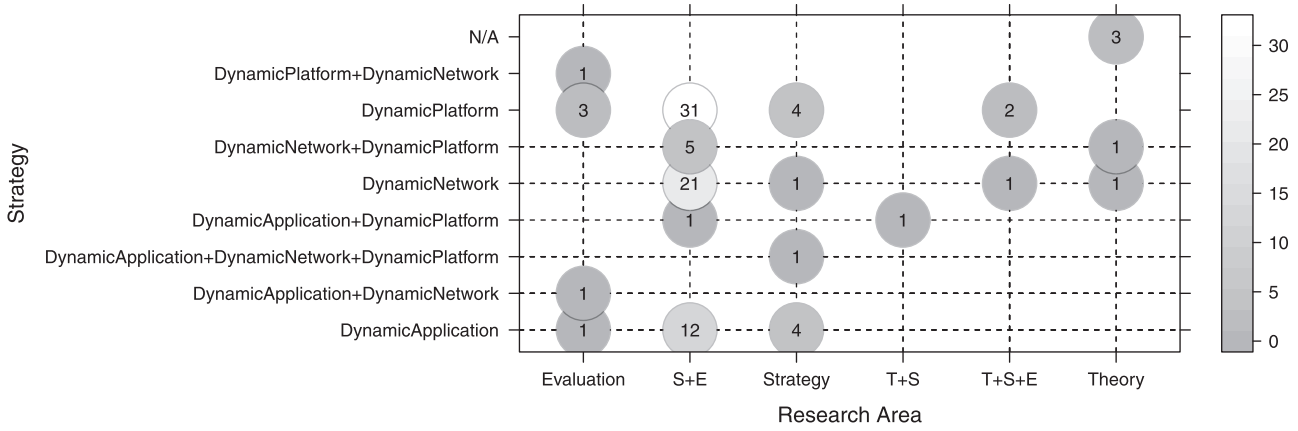

Fig. 11. Relationship between Research Area and Strategy categories.

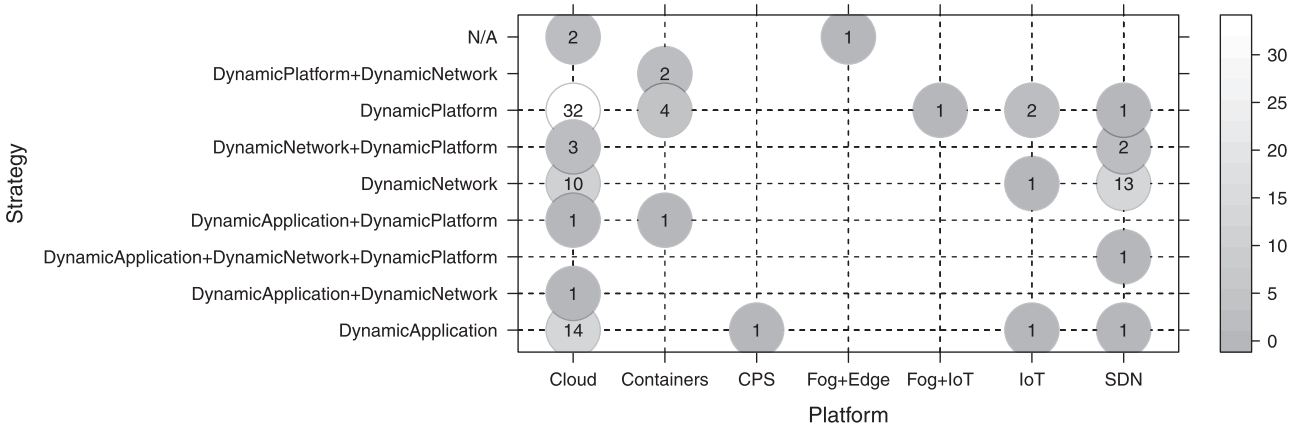

Fig. 12. Relationship between considered platforms and strategy categories.

However, to highlight the possible relationship between the publications from the same authors, we conducted an author analysis on the considered papers. This analysis aims to find the papers from the same set of authors and to verify possible relationships between them. Besides that, the analysis output also provides the most prominent authors on the field (i.e., authors with most publications).

Mir et al. published two related papers with evaluation approaches for MTD deployments in the cloud (El Mir et al., 2016; 2017). Wang et al. published papers about MTD deployments for defending cloud computing from Denial of Service attacks (Jia et al., 2014; Wang et al., 2014; 2016). As mentioned earlier, Kashkoush et al. published the related papers (Kashkoush et al., 2017; 2018) about Moving Target Defense to avoid co-residency attacks. Hooman Alavizadeh is one of the most active authors in the MTD evaluation research area. He and his co-authors published papers applying modeling in the MTD deployments evaluation (Alavizadeh et al., 2018a; 2018b; 2017). Jajodia et al. provide interesting insights into the deployment of MTD on cloud databases (Jajodia et al., 2015; 2016).

Fig. 13 presents a *wordcloud* with the names of all the authors of the selected papers. In this *wordcloud*, the font size of the author's name varies according to the number of publications from the author (i.e., big-sized font names represent that the author has more publications than the authors with small-sized font names). Thus, this *wordcloud* is useful to highlight the most prominent authors on the scope of our systematic mapping.

Finally, we highlight the following authors as the most prominent authors on MTD in the cloud in from 2009 to July 2019: **Mohamed Azab** (Virginia Military Institution, USA and Informatics Research Institute of Alexandria, Egypt.) published eight of the considered papers; **Dijiang Huang** (Arizona State University, USA) published seven of the considered papers; and, **Ankur Chowdhary** (Arizona State University, USA), **Dong Seong Kim** (The University of Queensland, Australia), and **Salim Hariri** (The University of Arizona, USA) with six published papers.

7. Discussion

Moving target defense attracted the attention of the cloud security research community in the last years, e.g., the number of publications per year increased 35% from 2017 to 2018. The number of publications on July 5th, 2019, is already about 50% of the publications in 2018. Considering that relevant venues, such as the *2019 ACM Workshop on Moving Target Defense* and the *2019 IEEE International Conference on Cloud Computing*, are still not indexed till the date of this paper writing, the number of papers published in 2019 may surpass the number of publications in 2018. Actually, in the same period of 2018 (January 1st to July 5th), only seven papers were published, while in 2019, 13 papers were published. The publication forums in the last ten years are diverse, meaning that the research community is still consolidating the primary forums of interest.

While applying or proposing MTD mechanisms for cloud computing, the researchers leverage on cloud and virtualization features, including VM placement and migration techniques. The problem with this approach is that these MTD techniques rely only on platform modification. Therefore, some more well-prepared at-

Fig. 13. Word cloud with the selected papers' authors.

tackers may develop security attacks targeting higher layers, such as application confidentiality or user privacy. However, the use of cloud and virtualization capabilities reduces the cost of MTD implementation due to the use of cloud embedded features. Besides that, the mappings show that authors have a strong interest in proposing and evaluating MTD mechanisms.

There is a significant research effort in expanding MTD from cloud computing to other platforms. The relationship between cloud and those platforms is mutual. Some works use the cloud to enable MTD in another specific platform (like Cyber-Physical Systems and IoT). Some other works use other platforms to improve the security levels of the cloud (e.g., using SDN).

In the following paragraphs, we highlight four relevant research opportunities on MTD in cloud computing. This is a non-exhaustive list, but it provides the significant research gaps found in our systematic mapping study.

Research opportunity 1 - ***Theoretical research about MTD in Cloud computing***. The majority of the theoretical papers found are generic. MTD theories that consider the characteristics of clouds and their virtualized environments represent a research opportunity. For example, a relevant MTD problem is the *MTD timing problem*, where one tries to define optimal schedules to perform MTD actions taking into account the desired system attributes (e.g., security, performance or sustainability).

Research opportunity 2 - ***A unified framework for MTD evaluation***. The development of security benchmarks is a complex problem due to the inherent unpredictability of the attackers. However, previous research (Dumitraș and Shou, 2011; Vieira and Madeira, 2005) provides directions for the design of such benchmarks. The current research on MTD in the cloud focuses on proposing new techniques to avoid (or reduce the likelihood) of specific security threats. The problem is that, without unified evaluation metrics, it is hard to compare and decide among the available MTD methods. Proposing a unified MTD evaluation approach may be an insurmountable challenge. However, starting proving evaluation approaches for specific scenarios (e.g., MTD in the cloud that applies VM migration to avoid side-channel attacks) seems to be an interesting research opportunity.

Research opportunity 3 - ***Multi-layer MTD***. As mentioned earlier, researchers mainly explored cloud features as enabling mechanisms for MTD deployments. There is still a gap in the development of multi-layer MTD frameworks for cloud computing. Just applying dynamic platform and network techniques are not enough to mitigate sophisticated attacks that aim at the system confidentiality or users' privacy. The development of a self-adaptive framework capable of dynamic multi-layer MTD selection is an interesting research challenge.

Research opportunity 4 - ***Impact of MTD in context-oriented clouds***. As presented in Buyya et al. (2018), there is a need for holistic evaluations in cloud computing environments. Applying MTD in context-oriented clouds may impose severe system overhead. Although the current research in MTD in the cloud is covering diverse platforms, we noticed a research gap in the evaluation of the MTD impact in context-oriented clouds. For example, some Infrastructure-as-a-Service (IaaS) clouds are devoted to offering *high-availability* to its clients. Let us suppose that, besides high availability, the system also needs to improve security levels. The evaluation of the possible impacts of applying MTD in such scenarios seems to be an interesting research problem.

8. Conclusions

This work presented a systematic mapping of Moving Target Defense in cloud research. To achieve this goal, we collected 224 papers from five computer science scientific databases. The selection process resulted in 95 papers for analysis. The papers were classified according to four main properties: research area, strategy, evaluation metrics, and platforms.

We present here simplified answers to our research questions. *RQ1: How has the frequency on moving target defense on cloud computing changed in the last ten years?* We noticed a growing interest in the MTD in cloud research in the last ten years. *RQ2: In which forums have research on moving target defense on cloud computing been published?* The most relevant conference in the area is the *ACM Workshop on Moving Target Defense*, and the most relevant journal is *Procedia Computer Science. RQ3: What are the most investigated techniques in moving target defense on cloud computing research?* In the dynamic platform papers, the most used technique is VM migration. In dynamic network papers, the most used technique is the network address randomization. A significant number of dynamic network papers rely on SDN flexibility to perform dynamic network changes. Finally, the most used technique in dynamic application papers is Software Behavior Encryption.

The complete list of selected papers is available online.[2] The research community can send new suggestions for paper inclusion or classification corrections.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work has been partially supported by Portuguese funding institution FCT - Foundation for Science and Technology, Ph.D. grant SFRH/BD/146181/2019 and project ATMOSPHERE, funded by the European Commission under the Cooperation Programme, Horizon 2020 grant agreement no 777154.

[2] https://www.matheustorquato.com/publications/systematic-map-of-moving-target-defense-on-cloud-computing .

References

Adili, M.T., Mohammadi, A., Manshaei, M.H., Rahman, M.A., 2017. A cost-effective security management for clouds: a game-theoretic deception mechanism. In: Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on. IEEE, pp. 98–106.

Agarwal, A., Duong, T.N.B., 2019. Secure virtual machine placement in cloud data centers. Fut. Gener. Comput. Syst. 100, 210–222.

Ahmed, N.O., Bhargava, B., 2016. Mayflies: a moving target defense framework for distributed systems. In: Proceedings of the 2016 ACM Workshop on Moving Target Defense. ACM, pp. 59–64.

Alavizadeh, H., Hong, J.B., Jang-Jaccard, J., Kim, D.S., 2018. Comprehensive security assessment of combined MTD techniques for the cloud. In: Proceedings of the 5th ACM Workshop on Moving Target Defense. ACM, pp. 11–20.

Alavizadeh, H., Jang-Jaccard, J., Kim, D.S., 2018. Evaluation for combination of shuffle and diversity on moving target defense strategy for cloud computing. In: 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, pp. 573–578.

Alavizadeh, H., Kim, D.S., Hong, J.B., Jang-Jaccard, J., 2017. Effective security analysis for combinations of MTD techniques on cloud computing (short paper). In: International Conference on Information Security Practice and Experience. Springer, pp. 539–548.

Alavizadeh, H., Kim, D.S., Jang-Jaccard, J., 2019. Model-based evaluation of combinations of shuffle and diversity MTD techniques on the cloud. Fut. Gener. Comput. Syst..

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., et al., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58.

Aydeger, A., Saputro, N., Akkaya, K., 2019. A moving target defense and network forensics framework for ISP networks using SDN and NFV. Fut. Gener. Comput. Syst. 94, 496–509.

Azab, M., Eltoweissy, M., 2011. Defense as a service cloud for cyber-physical systems. In: Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on. IEEE, pp. 392–401.

Azab, M., Eltoweissy, M., Attiya, G., et al., 2017. Towards online smart disguise: real–time diversification evading co-residency based cloud attacks. In: 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC). IEEE, pp. 235–242.

Azab, M., Mokhtar, B., Abed, A.S., Eltoweissy, M., 2016. Toward smart moving target defense for linux container resiliency. In: Local Computer Networks (LCN), 2016 IEEE 41st Conference on. IEEE, pp. 619–622.

Azab, M., Mokhtar, B.M., Abed, A.S., Eltoweissy, M., 2016. Smart moving target defense for linux container resiliency. In: Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on. IEEE, pp. 122–130.

Bazm, M.-M., Lacoste, M., Südholt, M., Menaud, J.-M., 2017. Side-channels beyond the cloud edge: new isolation threats and solutions. In: Cyber Security in Networking Conference (CSNet), 2017 1st. IEEE, pp. 1–8.

Bonguet, A., Bellaiche, M., 2017. A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. Future Internet 9 (3), 43.

Buyya, R., Srirama, S.N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., Gelenbe, E., Javadi, B., Vaquero, L.M., Netto, M.A., et al., 2018. A manifesto for future generation cloud computing: research directions for the next decade. ACM Comput. Surv. 51 (5), 105.

Cai, G., Wang, B., Luo, Y., Li, S., Wang, X., 2016. Characterizing the running patterns of moving target defense mechanisms. In: Advanced Communication Technology (ICACT), 2016 18th International Conference on. IEEE, pp. 191–196.

Cai, G., Wang, B., Hu, W., Wang, T., 2016. Moving target defense: state of the art and characteristics. Front. Inf. Technol. Electron.Eng. 17 (11), 1122–1153.

Casola, V., De Benedictis, A., Rak, M., Villano, U., 2018. A security SLA-driven moving target defense framework to secure cloud applications. In: Proceedings of the 5th ACM Workshop on Moving Target Defense. ACM, pp. 48–56.

Chang, S.-Y., Park, Y., Babu, B.B.A., 2018. Fast ip hopping randomization to secure hop-by-hop access in sdn. IEEE Trans. Netw. Serv. Manage. 16 (1), 308–320.

Chowdhary, A., Alshamrani, A., Huang, D., Liang, H., 2018. MTD analysis and evaluation framework in software defined network (mason). In: Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, pp. 43–48.

Chowdhary, A., Pisharody, S., Huang, D., 2016. SDN based scalable MTD solution in cloud network. In: Proceedings of the 2016 ACM Workshop on Moving Target Defense. ACM, pp. 27–36.

Chung, C.-J., Xing, T., Huang, D., Medhi, D., Trivedi, K., 2015. Serene: on establishing secure and resilient networking services for an SDN-based multi-tenant datacenter environment. In: Dependable Systems and Networks Workshops (DSN-W), 2015 IEEE International Conference on. IEEE, pp. 4–11.

Das, S., Mahfouz, A.M., Shiva, S., 2019. A stealth migration approach to moving target defense in cloud computing. In: Proceedings of the Future Technologies Conference. Springer, pp. 394–410.

Debroy, S., Calyam, P., Nguyen, M., Stage, A., Georgiev, V., 2016. Frequency-minimal moving target defense using software-defined networking. In: Computing, Networking and Communications (ICNC), 2016 International Conference on. IEEE, pp. 1–6.

Dsouza, G., Hariri, S., Al-Nashif, Y., Rodriguez, G., 2013. Resilient dynamic data driven application systems (RDDDAS). Procedia Comput. Sci. 18, 1929–1938.

Dumitraş, T., Shou, D., 2011. Toward a standard benchmark for computer security research: the worldwide intelligence network environment (wine). In: Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security. ACM, pp. 89–96.

El Mir, I., Chowdhary, A., Huang, D., Pisharody, S., Kim, D.S., Haqiq, A., 2016. Software defined stochastic model for moving target defense. In: International Afro-European Conference for Industrial Advancement. Springer, pp. 188–197.

El Mir, I., Haqiq, A., Kim, D.S., 2017. A game theoretic approach for cloud computing security assessment using moving target defense mechanisms. In: Proceedings of the Mediterranean Symposium on Smart City Applications. Springer, pp. 242–254.

Fernandez, A., Insfran, E., Abrahão, S., 2011. Usability evaluation methods for the web: asystematic mapping study. Inf. Softw. Technol. 53 (8), 789–817.

Fleck, D., Stavrou, A., Kesidis, G., Nasiriani, N., Shan, Y., Konstantopoulos, T., 2018. Moving-target defense against botnet reconnaissance and an adversarial coupon-collection model. In: 2018 IEEE Conference on Dependable and Secure Computing (DSC). IEEE, pp. 1–8.

Groat, S., Moore, R., Marchany, R., Tront, J., 2013. Securing static nodes in mobile-enabled systems using a network-layer moving target defense. In: 2013 1st International Workshop on the Engineering of Mobile-Enabled Systems (MOBS). IEEE, pp. 42–47.

Hong, J.B., Enoch, S.Y., Kim, D.S., Nhlabatsi, A., Fetais, N., Khan, K.M., 2018. Dynamic security metrics for measuring the effectiveness of moving target defense techniques. Comput. Secur. 79, 33–52.

Hosseinzadeh, S., Laurén, S., Rauti, S., Hyrynsalmi, S., Conti, M., Leppänen, V., 2015. Obfuscation and diversification for securing cloud computing. In: International Workshop on Enterprise Security. Springer, pp. 179–202.

Jajodia, S., Ghosh, A.K., Subrahmanian, V., Swarup, V., Wang, C., Wang, X.S., 2012. Moving Target Defense II: Application of Game Theory and Adversarial Modeling, 100. Springer.

Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., Wang, X.S., 2011. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, 54. Springer Science & Business Media.

Jajodia, S., Litwin, W., Schwarz, T., 2015. Numerical SQL value expressions over encrypted cloud databases. In: Database and Expert Systems Applications. Springer, pp. 455–478.

Jajodia, S., Litwin, W., Schwarz, T., 2016. On-the-fly AES256 decryption/encryption for trusted cloud SQL DBS: position statement. In: 2016 27th International Workshop on Database and Expert Systems Applications (DEXA). IEEE, pp. 19–23.

Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A., Powell, W., 2014. Catch me if you can: a cloud-enabled DDoS defense. In: 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, pp. 264–275.

Jin, H., Li, Z., Zou, D., Yuan, B., 2019. Dseom: a framework for dynamic security evaluation and optimization of MTD in container-based cloud. IEEE Trans. Depend. Secure Comput..

Kahla, M., Azab, M., Mansour, A., 2018. Secure, resilient, and self-configuring fog architecture for untrustworthy IoT environments. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, pp. 49–54.

Karim, Z., Sebbara, A., Baddic, Y., Boulmalfa, M., 2019. Secure multipath mutation SMPM in moving target defense based on SDN. Procedia Comput. Sci..

Kashkoush, M., Azab, M., Eltoweissy, M., Attiya, G., 2017. Towards online smart disguise: Real-time diversification evading co-residency based cloud attacks. In: 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), pp. 235–242. doi:10.1109/CIC.2017.00039.

Kashkoush, M.S., Azab, M., Attiya, G., Abed, A.S., 2018. Online smart disguise: real–time diversification evading coresidency-based cloud attacks. Cluster Comput. 1–16.

Kitchenham, B., Brereton, P., Budgen, D., 2010. The educational value of mapping studies of software engineering literature. In: Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering-Volume 1. ACM, pp. 589–598.

Krutz, R.L., Vines, R.D., 2010. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing.

Kurra, H., Al-Nashif, Y., Hariri, S., 2013. Resilient cloud data storage services. In: Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference. ACM, p. 17.

Le Goues, C., Nguyen-Tuong, A., Chen, H., Davidson, J.W., Forrest, S., Hiser, J.D., Knight, J.C., Van Gundy, M., 2013. Moving Target Defenses in the Helix Self-regenerative Architecture. In: Moving Target Defense II. Springer, pp. 117–149.

Lei, C., Zhang, H.-Q., Tan, J.-L., Zhang, Y.-C., Liu, X.-H., 2018. Moving target defense techniques: a survey. Secur. Commun. Netw. 2018.

Lei, C., Zhang, H.-Q., Wan, L.-M., Liu, L., Ma, D., 2018. Incomplete information Markov game theoretic approach to strategy generation for moving target defense. Comput. Commun. 116, 184–199.

Leslie, D., Sherfield, C., Smart, N.P., 2015. Threshold flipthem: when the winner does not need to take all. In: International Conference on Decision and Game Theory for Security. Springer, pp. 74–92.

Liu, L., Wang, A., Zang, W., Yu, M., Xiao, M., Chen, S., 2018. Shuffler: Mitigate cross-VM side-channel attacks via hypervisor scheduling. In: International Conference on Security and Privacy in Communication Systems. Springer, pp. 491–511.

Luo, Y.-B., Wang, B.-S., Cai, G.-L., Wang, X.-F., Zhang, B.-F., 2016. High performance low latency network address and port hopping mechanism based on netfilter. In: International Conference on Intelligent and Interactive Systems and Applications. Springer, pp. 239–244.

Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., 2018. Self-adaptive system for the corporate area network resilience in the presence of botnet cyber-attacks. In: International Conference on Computer Networks. Springer, pp. 385–401.
Ma, D., Lei, C., Wang, L., Zhang, H., Xu, Z., Li, M., 2016. A self-adaptive hopping approach of moving target defense to thwart scanning attacks. In: International Conference on Information and Communications Security. Springer, pp. 39–53.
Mell, P., Grance, T., et al., 2011. The NIST definition of cloud computing.
Moon, S.-J., Sekar, V., Reiter, M.K., 2015. Nomad: mitigating arbitrary cloud side channels via provider-assisted migration. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1595–1606.
Moving, 2018. Target Defense. https://www.dhs.gov/science-and-technology/csd-mtdAccessed: 2018-12-09
Nguyen, M., Pal, A., Debroy, S., 2018. Whack-a-mole: Software-defined networking driven multi-level DDoS defense for cloud environments. In: 2018 IEEE 43rd Conference on Local Computer Networks (LCN). IEEE, pp. 493–501.
Okhravi, H., Rabe, M., Mayberry, T., Leonard, W., Hobson, T., Bigelow, D., Streilein, W., 2013. Survey of Cyber Moving Target Techniques. Technical Report. Massachusetts Inst of Tech Lexington Lincoln Lab.
Pacheco, J., Tunc, C., Hariri, S., 2016. Design and evaluation of resilient infrastructures systems for smart cities. In: 2016 IEEE International Smart Cities Conference (ISC2). IEEE, pp. 1–6.
Peng, W., Li, F., Huang, C.-T., Zou, X., 2014. A moving-target defense strategy for cloud-based services with heterogeneous and dynamic attack surfaces. In: Communications (ICC), 2014 IEEE International Conference on. IEEE, pp. 804–809.
Peng, W., Li, F., Zou, X., 2014. Moving target defense for cloud infrastructures: lessons from botnets. In: High Performance Cloud Auditing and Applications. Springer, pp. 35–64.
Penner, T., Guirguis, M., 2017. Combating the bandits in the cloud: a moving target defense approach. In: Cluster, Cloud and Grid Computing (CCGRID), 2017 17th IEEE/ACM International Symposium on. IEEE, pp. 411–420.
Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M., 2008. Systematic mapping studies in software engineering.. In: EASE, 8, pp. 68–77.
Petersen, K., Vakkalanka, S., Kuzniarz, L., 2015. Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. 64, 1–18.
Popović, K., Hocenski, Ž., 2010. Cloud computing security issues and challenges. In: The 33rd International Convention MIPRO. IEEE, pp. 344–349.
Ren, K., Wang, C., Wang, Q., 2012. Security challenges for the public cloud. IEEE Internet Comput. 16 (1), 69–73.
RightScale, 2018. Rightscale 2018 State of the Cloud Report.
Roberto, R., Lima, J.P., Teichrieb, V., 2016. Tracking for mobile devices: a systematic mapping study. Comput. Graph. 56, 20–30.
Sengupta, S., Chowdhary, A., Huang, D., Kambhampati, S., 2019. General sum Markov games for strategic detection of advanced persistent threats using moving target defense in cloud networks. In: International Conference on Decision and Game Theory for Security. Springer, pp. 492–512.
Sengupta, S., Chowdhary, A., Sabur, A., Huang, D., Alshamrani, A., Kambhampati, S., 2019b. A survey of moving target defenses for network security. arXiv:1905.00964.
Sianipar, J., Sukmana, M., Meinel, C., 2018. Moving sensitive data against live memory dumping, spectre and meltdown attacks. In: 2018 26th International Conference on Systems Engineering (ICSEng). IEEE, pp. 1–8.
Song, F., Zhou, Y.-T., Wang, Y., Zhao, T.-M., You, I., Zhang, H.-K., 2019. Smart collaborative distribution for privacy enhancement in moving target defense. Inf. Sci. 479, 593–606.
Torkura, K.A., Sukmana, M.I., Kayem, A.V., 2018. A cyber risk based moving target defense mechanism for microservice architectures. In: 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom). IEEE, pp. 932–939.
Urias, V.E., Stout, W.M., Loverro, C., 2015. Computer network deception as a moving target defense. In: Security Technology (ICCST), 2015 International Carnahan Conference on. IEEE, pp. 1–6.
Vieira, M., Madeira, H., 2005. Towards a security benchmark for database management systems. In: 2005 International Conference on Dependable Systems and Networks (DSN'05). IEEE, pp. 592–601.
Villarreal-Vasquez, M., Bhargava, B., Angin, P., Ahmed, N., Goodwin, D., Brin, K., Kobes, J., 2017. An MTD-based self-adaptive resilience approach for cloud systems. In: Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on. IEEE, pp. 723–726.
Wahab, O.A., Bentahar, J., Otrok, H., Mourad, A., 2019. Resource-aware detection and defense system against multi-type attacks in the cloud: repeated Bayesian stackelberg game. IEEE Trans. Depend. Secure Comput..
Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., Stavrou, A., 2014. A moving target DDoS defense mechanism. Comput. Commun. 46, 10–21.
Wang, H., Li, F., Chen, S., 2016. Towards cost-effective moving target defense against DDoS and covert channel attacks. In: Proceedings of the 2016 ACM Workshop on Moving Target Defense. ACM, pp. 15–25.
Yang, C., Guo, Y., Hu, H., Wang, Y., Tong, Q., Li, L., 2019. Driftor: mitigating cloud-based side-channel attacks by switching and migrating multi-executor virtual machines. Front.Inf. Technol. Electron.Eng. 20 (5), 731–748.
Yang, Y., Cheng, L., 2018. An SDN-based MTD model. Concurren. Comput. e4897.
Zhang, L., Wang, Z., Fang, J., Guo, Y., 2016. A SDN proactive defense scheme based on IP and MAC address mutation. In: International Wireless Internet Conference. Springer, pp. 51–60.
Zhang, M., Wang, L., Jajodia, S., Singhal, A., Albanese, M., 2016. Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks. IEEE Trans. Inf. Forensics Secur. 11 (5), 1071–1086.
Zhang, Y., Li, M., Bai, K., Yu, M., Zang, W., 2012. Incentive compatible moving target defense against VM-colocation attacks in clouds. In: IFIP International Information Security Conference. Springer, pp. 388–399.
Zheng, J., Namin, A.S., 2019. A survey on the moving target defense strategies: an architectural perspective. J. Comput. Sci. Technol. 34 (1), 207–233.
Zhuang, R., DeLoach, S.A., Ou, X., 2014. Towards a theory of moving target defense. In: Proceedings of the First ACM Workshop on Moving Target Defense. ACM, pp. 31–40.

Matheus Torquato is a Ph.D. candidate at the University of Coimbra. His research interests comprise subjects like Cloud Computing, Performance, Dependability, and Security Modeling. His current research focuses in the design and development of analytical models to evaluate performance, dependability, and security of moving target defense deployments in cloud computing. He received his Master Degree in Computer Science from the Federal University of Pernambuco. He is currently on leave from his teaching activities at the Federal Institute of Alagoas, Campus Arapiraca to pursue Ph.D. at the University of Coimbra. His website is http://www.matheustorquato.com.

Marco Vieira received the Ph.D. degree from UC, Portugal, in 2005. He currently is a Full Professor with the University of Coimbra, Coimbra, Portugal. His research interests include dependability and security assessment and benchmarking, fault injection, software processes, and software quality assurance, subjects in which he has authored or coauthored more than 200 papers in refereed conferences and journals. He has participated and coordinated several research projects, both at the national and European level. He has served on program committees of the major conferences of the dependability area and acted as referee for many international conferences and journals in the dependability and security areas.