Moving Target Defense on Cloud Computing Systems: A Survey

1st Austin J Derbique
School of Computing, Informatics, and Decision Systems Engineering
Arizona State University
Tempe, USA
aderbiqu@asu.edu

***Abstract*—The usage of cloud computing for hosting workloads has risen dramatically in recent years. With the rise of applications deployed across the cloud, attack surfaces grow immensely and so does the complexity in network configurations. Moving Target Defense (MTD) is a paradigm aimed at reconfiguring or shuffling the application's configuration such that an attacker's knowledge about the system state is nullified or reduced. In this survey, we discuss motivations for MTD as a way to protect cloud applications from attackers, as well as anaylyze existing literature on the topic. There are several classifications and categories of MTD that will be discussed. Next, an evaluation of various case studies is performed to find commonalities between literature and address research gaps that can be used for future work. Finally, we look at existing challenges on the topic and what is needed for these challenges to be overcome.**

***Index Terms*—Moving Target Defence, MTD, Cloud Computing, Security Analysis**

I. Introduction

This survey provides an overview of existing research of moving target defense in respect to cloud computing by studying techniques threat models, and various technical details required for general understanding of the domain. As defined by the United States Department of Homeland Security, moving target defense (MTD) is ”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.” [8] MTD is primarily focused on modifying systems in such a way that operations may continue safely in a compromised environment.

A. The Rise of Cloud Computing

Prior to the rise of cloud computing and modern virtualization, physical servers were required to run applications. A simple web server required a dedicated machine, often sitting in a server rack somewhere. These highly static systems were expensive to acquire, stand up, and maintain. In 2006, Amazon introduced its web-based retail services company Amazon Web Services (AWS) [10]. This was the first major business to launch a public cloud offering. Popularity soared as users could now dynamically instantiate virtual machines (VMs) to deploy their code at the click of a button. As seen in Figure 1, the amount of revenue in the cloud computing industry has grown substantially in recent years. Popular cloud providers include Amazon's AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and Oracle Cloud [23]. While all clouds have different interfaces, they all functionally achieve the same goal: provide compute, storage, and networking.

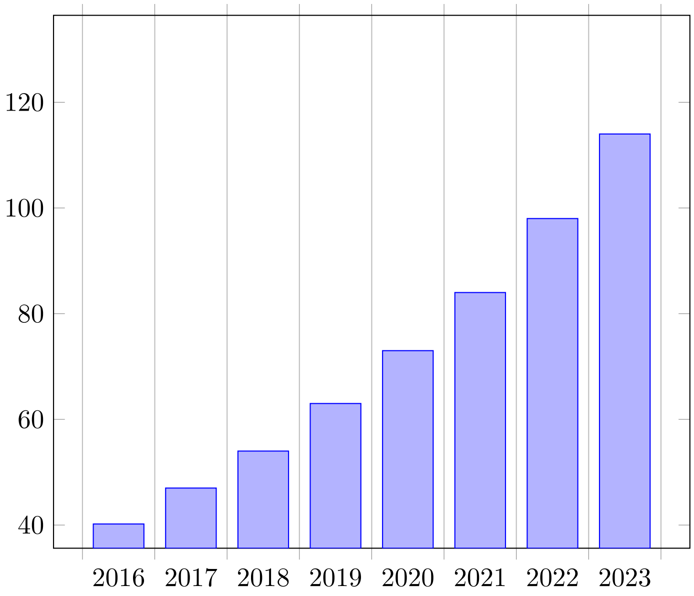

Fig. 1. Projected Cloud Computing Revenue (in billions USD) [16]

This large migration of applications from on-premise environments to the cloud presents several important security concerns. In a traditional environment, a server might be isolated in an on-premise environment, accessible only to the organization's intranet. This drastically limited the attack surface to either users already on the network, or forcing attackers through the organization's firewall from the public internet. This shift to public cloud computing now means that an organization's applications are running on a network physically separate from their locality. This network may or may not be logically connected to their on premise network. In both scenarios, application endpoints, data, and other sensitive information are at risk of being exposed to attackers. Because of this, efforts to prevent, mitigate, and deceit attackers from compromising cloud applications is more prominent than ever before.

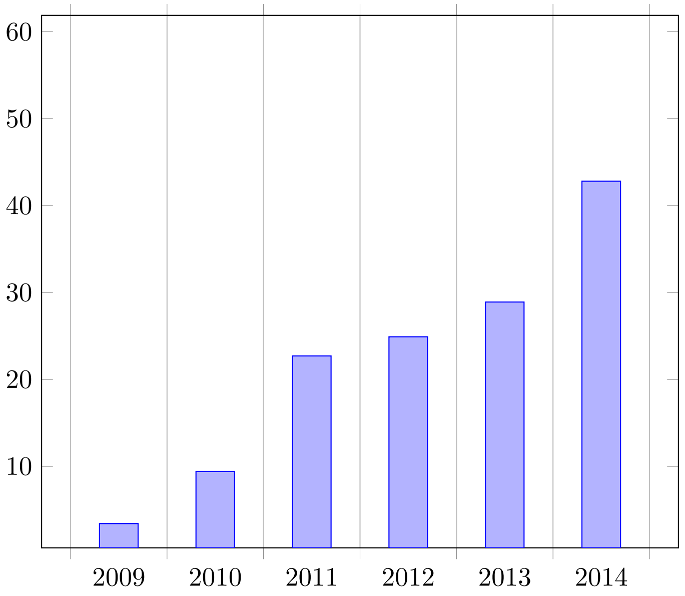

Fig. 2. Annual number of cyber attacks worldwide (in millions) [20]

B. The Need for Better Defense

As seen in Figure 2, the annual number of cyber attacks is rising year over year [20]. It is shown that cyber attacks typically follow financial assets, which for cloud computing, is expected to rise to over 1 trillion USD by 2026 [9] [22]. Research shows that attackers are becoming more creative with their methodologies, too. It was found that with a plethora of Internet-of-Things (IoT) devices easily available to hackers, attacks can be carried out inducing largescale botnets capable of causing serious damage [12].

As briefly mentioned in the previous section, existing applications in the cloud utilizing Infrastructure as a Service (IaaS) are largely static and homogeneous. This is because IaaS requires a user to maintain the operating system and all layers abstracted on top of it. For example, when creating a virtual machine using Amazon Elastic Compute Cloud (EC2), ease-of-use typically funnels users into selecting from only a handful of instance types and operating system combinations. While easy to use, this leads to a lack of heterogeneity, decreasing uncertainty of the system for a potential attacker.

II. Moving Target Defense

Moving Target Defense is a paradigm that has only been around for the last decade or so. First research began around 2009, shortly after cloud computing began to take off. In this section, we first explore existing research surveys of MTD literature. This includes MTD Techniques, architectural perspectives, and systematic mapping studies of what topics are covered. Next, we will formulate several research questions to answer questions not answered in existing surveys. Finally, we will perform analysis of several research papers across the MTD domain to try and answer the research questions we formulated in the previous subsection.

A. Existing Surveys

To gain a broader understanding of existing research on Moving Target Defense, we examine three existing surveys. The first is a systematic mapping study, the second studying defenses from an architectural perspective, and the third a survey on various MTD techniques.

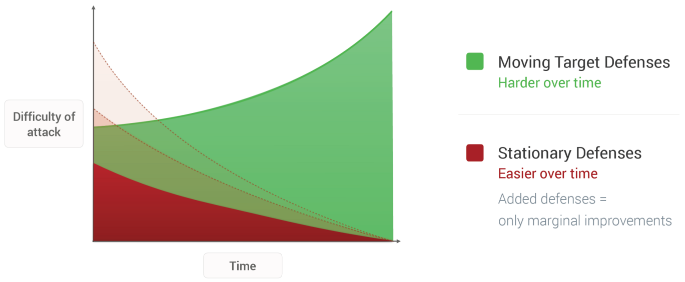

Fig. 3. MTD Paradigm Shift [6]

- **MTD Systematic Mapping Study:** In *"Moving target defense in cloud computing: A systematic mapping study"*, the authors analyze MTD literature based on publication type, classification, category, and method [24]. Out of 224 papers related to MTD, 95 papers were filtered for analysis. The data science performed in this survey found that out of these papers, 40 publications were related to platform MTD, 24 network, and 17 on application. This is visible in Figure 4. Given the nature of MTD, a large portion of literature dealt with platform based defenses, such as migrating VMs or replicating data. Network and application based MTD methods are determined to be less represented in literature. Other categories surveyed include evaluation approaches. These included papers focused on performance versus security. In MTD, there is an inverse relationship between performance and security. The more security you introduce into a system, the higher the overhead cost is, effectively reducing performance. Finally, the mapping study found an overwhelming amount of research on MTD exists within formulating strategies of defenses, not necessarily with theory or evaluation. This opens up the discussion of why more work isn't being performed on constructing new theoretical research on MTD or evaluation techniques regarding the performance of a given strategy.
- **MTD Architectural Survey:** In *"A Survey on the Moving Target Defense Strategies: An Architectural Perspective"*, the authors evaluate existing literature by breaking down MTD architectures into three categories: operating system level approaches, software/application level approaches, and network level approaches. This survey is thorough and useful, but does not address problems modern cloud systems experience today. Put another way, the authors focus on architectures at a micro scale, but do not consider MTD techniques of large scale, distributed systems. While covering MTD in a general sense, more

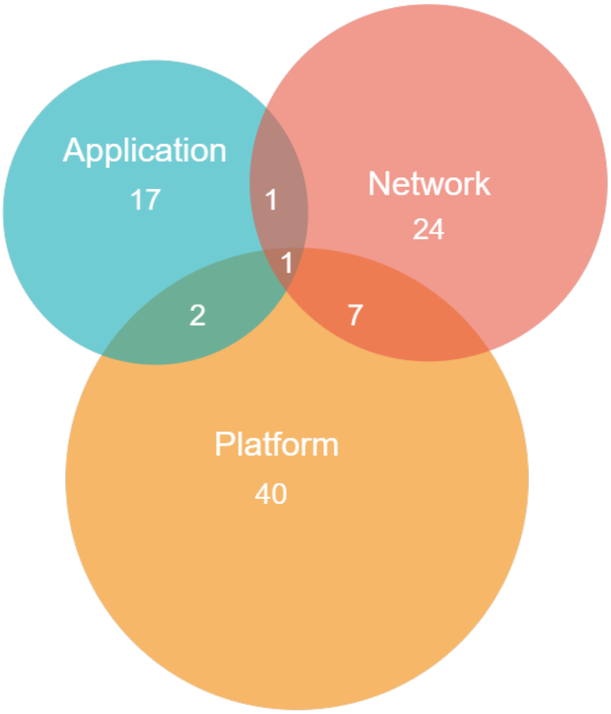

Fig. 4. MTD Classifications in Literature [24]

research must be performed on how MTD architectural perspectives play out in a cloud networked environment.

- **MTD Techniques Survey:** In *"Moving Target Defense Techniques: A Survey"*, a survey is conducted across the broad spectrum of moving target defense research areas. [13]. Providing a strong background on theory and architecture design, the authors discuss various theoretical topics such as Attack Surfaces and Attack Graphs. Various techniques are also covered which covers Stategy fomulation based on Game Theory, Complete Information Assumption, and Evolution Theory. Finally, the survey covers applications of MTD in different conditions such as traditional networks, IoT, and Software Defined Networks. While covering a broad range of topics, coverage on MTD techniques and how they relate to cloud networks remains largely absent. Overall, the survey provides strong fundamental understanding, but does not offer insights into how MTD can defense against large attacks, or how MTD can benefit from an ocean of cloud computing resources.

B. Research Questions

While the above surveys provide great foundations understanding of moving target defense, these works are largely focusing on MTD from a classical networking perspective. Currently, there are no known surveys covering literature specific to cloud systems. This presents a research gap on an overall survey of cloud focused MTD literature, leading to several important research questions that need to be asked.

TABLE I

RESEARCH QUESTIONS

Research Question
With modern Infrastructure as a Service (IaaS) technologies such as Amazon EC2 which isolate users from one another, is MTD still needed?
Is MTD an effective deterrent for other service types? Name Function as a Service (FaaS) and Software as a Service (SaaS).
How can MTD leverage the scalability of cloud resources to better defend against attackers?

III. EXISTING WORKS

Because MTD is a rather broad research area, it is easiest to quantify the works by category and classification.

- **Classification:** The classification of an MTD technique refers to what the defense is trying to accomplish. This may include preventing the attack, mitigating the attack, deceiving the attacker, recovering from an attack, or some combination of each.
- **Category:** The category refers to the layer of which the MTD strategy or technique refers to. Categories include system based MTD which comprises of software (Application, Operating System, Services) and hardware (processors, chip architectures, FPGAs), and Network-based MTD. These types of categories include the MAC layer, IP layer, as well as transport layers such as TCP or UDP.

In this section, we go into more detail about each classification and category and discuss relevant work and how it applies to cloud computing.

A. Classifications

- **Prevention:** Preventative strategies (sometimes referred to as proactive) attempts to stop an attack before it even happens. In the scope of MTD, this means increasing an attacker's uncertainty of the system to the extent as if the attack were completely random [19]. There are many ways of increasing uncertainty of the system. One common technique is migrating a virtual machine from one location, effectively shuffling the known state of the world [2]. Other techniques include encrypting sensitive information so that an attacker is unable to steal information required to carry out an attack. In *Y. Magdy et al.*, the authors utilize blockchain and public key encryption to obfuscate the public IP addresses of systems in order to proactively prevent an attack [14]. Proactive attacks are common in literature, however most of them tend to deal with the migration technique mentioned previously.
- **Mitigation:** Unlike MTD prevention, existing works in MTD mitigation accept that complete attack prevention cannot be guaranteed. These types of attacks typically try and prolong the attacker long enough that loss to the system is minimized. Often times, prevention and mitigation are used as the same piece. In *W. Peng et al.*, a strategy is devised to increase heterogeneity of the

system, effectively holding out an attack as long as possible [18]. The reason this paper is classified as mitigation and not proactive is because of the snapshot-and-restore functionality proposed. A downside to solutions like this is if the system was vulnerable before the backup, it will be vulnerable after the snapshot is restored. (If a piece of software is exploitable). Other strategies include replicating the data to minimize risk sensitive data is deleted.

- **Deception:** Moving Target Defense Deception techniques involve deceiving the attacker in such a way that the attacker thinks they are carrying out an attack on the real system, where in reality the attack is being carried out on a decoy node or some other system that does not pose a risk to the application. The most notable type of deception technique is to include a honeypot for attackers to try to exploit. In *Jun-Gyu Park et al.*, the authors develop a system called Ghost-MTD which via protocol mutation, creates a deception system luring attackers to false decoy nodes that return real looking, but fake responses [17]. It is common for these deception systems to then blacklist the attacker by removing them from the system or adding them to the firewall. While deception is an effective technique in MTD, it often involves a lot of overhead to configure. It is also not guaranteed that an attacker will fall for the traps. In *Ankur, Chowdhary et al.*, MTDs are modeled using Markov game theory to intelligently determine the best place for placing intrusion detection systems [7].
- **Recovery:** MTD Recovery strategies aim to ensure a system is properly returned to an uncomporrised state following an attack. While straight forward, this is a research area that appears to be lacking. Cloud systems are typically large and spread across many nodes, often making the known state of the system difficult to determine, let alone following a recent attack. In *Y. Magdy et al.*, a blockchain is used to record current states of the world [14]. This is especially important for federated cloud systems where heterogeneity is high. Blockchain applications for the purposes of MTD guarantees transparency and immutability of the known state, making it easier to see what resources have been compromised or tampered with.

B. Categories

There are also several different MTD categories. In this context, categories refers to the attack or defense vector used by a given MTD strategy.

- **System-Based MTD:** Nearly all of the works published on the topic of cloud computing are system based. This is due to the high degree of virtualization of compute and network components. Most of these works lay within either the application of operating system level. The system-based MTD brings interesting challenges, however. When performing entire virtual machine migrations like in *W. Peng et al.*, it is seen that such operations require a lot of computational power and often take time for a virtual machine replacement to occur [18]. It is well known that MTD's largest challenge is appropriately determining how much change is required in a system to thwart an attack, without doing more than what's necessary due to the waste of computational resources and degradation of performance. In essence, the challenge is the inverse relationship between security and performance.
- **Network-Based MTD:** Network-Based moving target defense focuses on transport layers and routing rather than platform specific resources like the operating system or application itself. In *M. Villarreal-Vasquez et al.*, the authors devise a live monitoring system to dynamically detect deviations from normal behavior in the network [25]. This is achieved through software-defined networking for on the fly open-flow table modifications as well as a modified k-means clustering algorithm for detecting network or service anomalies. Network-based MTD has the benefit of being more *real time* than platform based systems which usually incur a performance degradation or downtime when defense is enacted. Figure 5 shows a typical pattern used in Network-Based MTD, where trusted clients are capable of using the software application normally, whereas an attacker or untrusted client is routed to a drain or decoy node. For this to work, however, the untrusted client must be successfully identified.

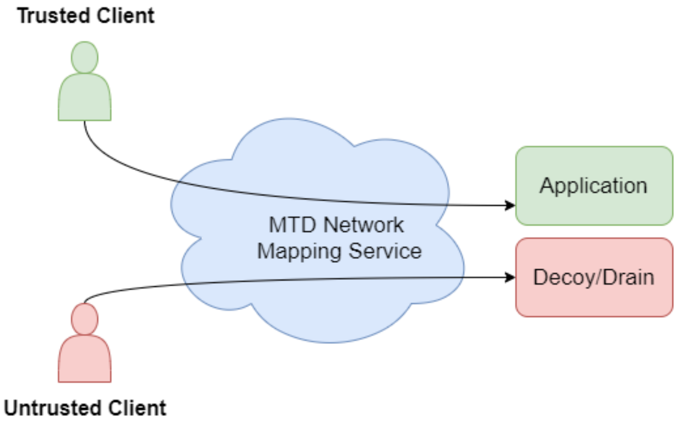

Fig. 5. Network-Based MTD [11]

IV. Additional Case Studies of MTD for Cloud Systems

Below are a number of different published papers representing various segments of literature in MTD regarding cloud systems. This includes the paper title with appropriate citation, motivation for why the paper was written, overall analysis of the paper and how to make sense of the information provided, and finally date published and relevant tags for the paper.

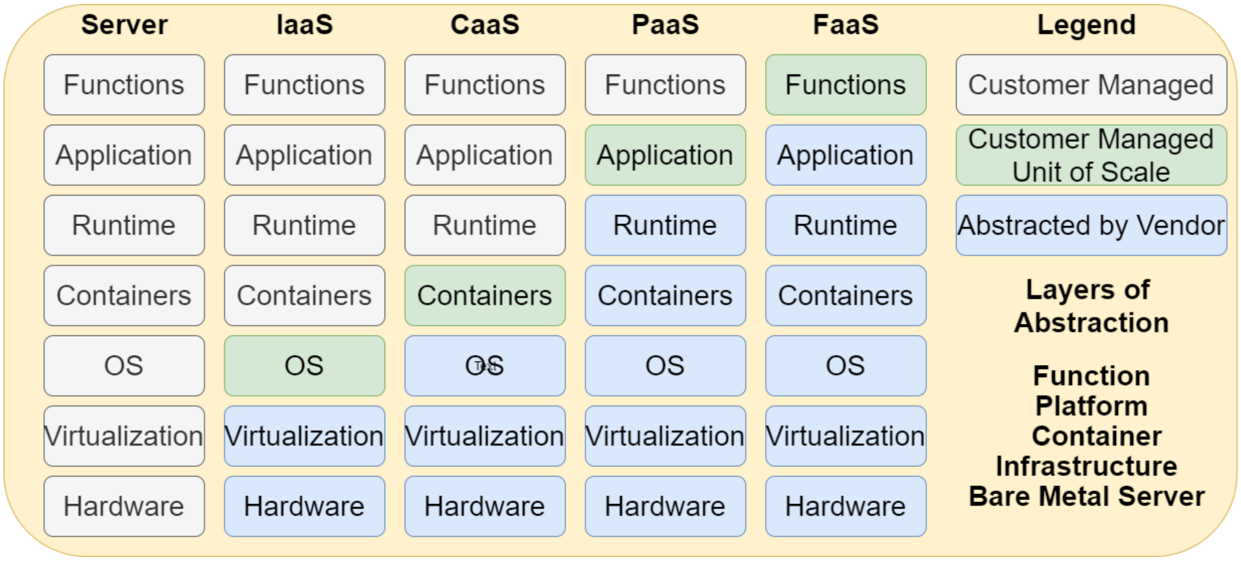

Fig. 6. Cloud Abstractions [15]

V. Evaluation of MTD Research for Cloud Computing

With various works cited, it is time to try and answer the research questions created in the previous section.

- **RQ One: With modern Infrastructure as a Service (IaaS) technologies such as Amazon EC2 which isolate users from one another,is MTD still needed?:** In short, yes. Various techniques utilizing *side-channel attacks* have been proven to exploit virtual machines and containers to expose information about their colocated neighbors [4]. While this is true for infrastructure-as-a-service, there is no published work if this holds true for managed container-as-a-service platforms as well. It is also unknown if such defense mechanisms are necessary when the end user is not responsible for runtime. Namely function-as-a-service (FaaS).
- **RQ Two: Is MTD an effective deterrent for other service types? Namely function-as-a-service (FaaS) and software-as-a-service(SaaS):** Moving target defense aims to increase heterogeneity in a computer system in order to make the attack surface more difficult for an attacker. By abstracting more layers away, the more heterogeneous a system becomes. Therefore, it is natural to include that while a FaaS or SaaS application will be completely defensible by themselves, it certainly would not hurt to include MTD techniques.
- **RQ Three: How can MTD leverage the scalability of cloud resources to better defend against attackers?:** One part that did not really come up in MTD literature for cloud systems was leveraging managed services offered by cloud providers. A tremendous amount of work can be delegated to managed services such as Amazon Cloudwatch for logging or Elastic Search Cluster [1]. By decoupling work performed by a system, computational overhead is minimized, therefore maximising performance. Better leveraging cloud resources for network-based MTD and real time, dynamic decision making would likely have a large performance gain from utilizing the aforementioned managed cloud services.

A. Challenges

Given that MTD is still relatively new to the field of computer science (one decade old), there are still open challenges faced. While a lot of research is conduced on strategies of implementing MTD using various techniques, far fewer works are published on the topic of MTD evaluation. Simply put, MTD is still in its early stages of maturity and a standardized procedure for evaluating a given technique has not yet been established. Currently, the best way to evaluate an MTD approach is to compare it to static systems, which may not accurately reflect the real world or algorithms produced in other MTD literature. Therefore, it is difficult to tell if progress is being made in the field due to the difficulty of comparing MTD techniques across literature pieces.

VI. Looking Forward

A great amount of work has been published on the topic of MTD techniques utilizing system-based MTD and network-based MTD. While this is true and categories have maturely been identified, a new sub genre of the field needs to be created to better evaluate MTD effectiveness and performance within different abstraction layers of computing. To simply say cloud computing is too generic. More research needs to be conducted on PaaS, FaaS, and SaaS applications. According to AWS Well Architected, micro-service architecture is soon taking precedence over IaaS as applications are decoupled, risk is reduced, and attack surfaces are distributed into smaller pieces [5].

Paper Title	Motivation	Analysis	Published	Tags
Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud [2]	A concern for security leads to the authors exploring the Shuffle and Diversity MTD technique for use in the cloud. Difficult complexity arises from generating formal graphical attack models leading the authors to use Hierarchical Attack Representation Model (HARM) which is more scalable and adaptable for evaluating effectiveness of MTD techniques.	Shuffle techniques aim to reconfigure the system's components in order to change the attack surface. Diversity MTD techniques aim to increase difficulty of attacks by changing a computer system's component variant. While the paper focuses on these two techniques, the real value ascertained from this literature is within the continued development of the HARM technique for effectively evaluating MTD effectiveness. Security metrics for both the attacker and defender can be calculated. A possible shortcoming of this approach is the need to have full observabilty of the environment to accurately perform threat analysis.	November 2019	Proactive MTD, Platform Classification, VM-LM
An MTD-Based Self-Adaptive Resilience Approach for Cloud Systems [25]	The authors realize that virtual machine migration is slow and resource intensive. The need to monitor resources live for anomaly detection is also presented as a focus of research.	The approach presented in this paper utilizes Software Defined Networking as a means of dynamically updating openflow tables to switch VMs rather than perform traditional VM migrations. Cutover time was reduced from 7s to 250ms in the paper's evaluation. One such issue with this paper's approach is that it does not address the centralized control aspect of SDN. If an attacker gained access to the control plane itself, the MTD technique would prove to be ineffective.	September 2017	Proactive, Reactive MTD, Application Classification, SDN, Unsupervised Learning
Anonymous blockchain Based Routing For Moving-target Defense Across Federated Clouds [14]	While heterogeneity is typically regarded as a good property to have, it can make trust difficult, especially in multi cloud or cloud federated environments. One of the attack vectors used in this type of environment is colocation. The authors seek a way to minimize the amount of information leakage attackers can use for illegitimate purposes.	The main attack focused on in this paper is the co-residency attack where VMs or containers (called capsules in the paper) leak information to malicious neighbors. The proposed solution includes encrypting certain information such as public IP address so that attackers are unable to properly trace the capsule. Routing and change information is stored on an anonymous blockchain, where only owners of the capsule have a keypair capable of decrypting the information. Analyzing the evaluation section, it can be concluded that the method works, however performance of the system is not conducted. In a real world setting, it is unlikely this approach would operate quickly enough for a realistic use case.	May 2020	Proactive MTD, Platform Classification, IP Address Obfuscation, Blockchain, Federated Cloud
Ghost-MTD: Moving Target Defense via Protocol Mutation for Mission-Critical Cloud Systems [17]	Network-based MTD (NMTD) techniques show promise, but is an under researched topic. Rather than use platform based MTD, the authors look for how to better defend against attackers by developing a deception technique based around network protocol mutation.	With a focus on low operational overhead, the authors devise a technology called Ghost-MTD which allows only the user who is aware of the protocol mutation patterns the ability to correctly communicate with the webservice modules. This is achieved by generating a one-time bit sequence (OTBS) for each user and using that preshared key as a seed to determine the next mutation. Potential attackers that are unable to guess the key are redirected to a decoy node. Analyzing this approach, it is concluded that the technique is both proactive and deceptive. A shortcoming to the approach is that if the attacker ever gets ahold of that preshared key, future mutations can be predicted and the defense is useless.	April 2020	Deception MTD, Network-Based MTD, Protocol Mutation, One time Bit Sequence (OTBS)
Markov Game Modeling of Moving Target Defense for Strategic Detection of Threats in Cloud Networks [7]	This paper seeks to find an effective way at placing intrusion detection systems without incurring unnecessary overhead from monitoring and attack graph computation. Using two-player Markov game theory as a platform, the paper devises a strategy of pitting the attacker and defender against each other in order to build a better ITD mechanism for cloud networks.	This paper addresses security problems in a cloud network by modeling the cloud system as a Markov game. By assuming both players have full observability of the game state, worst case scenarios of a silent attacker are accounted for. Tying decisions a player can make to actionable moves from an attack graph, a defender can determine when and where to dynamically place an intrusion detection system. Therefore, the approach presented in the paper effectively reduces the number of ITD systems, cutting down on resource overhead. One of the challenges this paper disucsses are zero attacks, as the markov game is based on CVE metrics. If the attack is unknown to the CVE database, there is no way to detect intrusion, and therefore no way to successfully provide moving target defense. This approach would need to be combined with other approaches for a holistic MTD technique.	February 2019	Intrusion Detection System, Markov Game Modeling, Attack Graph Representation

TABLE II
ANALYSIS OF RELATED WORKS

Paper Title	Motivation	Analysis	Published	Tags
Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud [21]	With a rise of cloud deployed applications and known CVE metrics, an intelligent intrusion detection system for identifying attackers with a low overhead cost appears feasible.	The authors of this paper address the problem of placing a fixed number of intrusion detection systems (IDS) in a large cloud environment using MTD. By pitting the attacker and defender against each other in the form of Stackleberg game theory, equilibrium between defense and offense can be determined to appropriately adjust the security of the system. One issue with this strategy is the lack of coverage for zero day attacks.	June 2014	Proactive, Detection Systems, IDS, Stackelberg Games
MIGRATE Towards a Lightweight Moving-Target Defense Against Cloud Side-Channels [4]	The authors use side-channel attacks as a basis for developing a unique MTD technique that is cross-vm compatible. Building off previous work, the authors look to see how MIGRATE can be an effective means at protecting against co-residency attacks by obfuscating sensitive data in shared memory.	MIGRATE targets the placement vector of an adversary's virtual machine into a colocated environment. The authors strive to excessively complicate the attacker process of placing the VM/container on the same host as the victim. MIGRATE adjusts the ARP table for the NAT to point to a new server instead of an old server, reducing overhead of a VM migration away from the colocated attack VM.	May 2016	Proactive MTD, Platform Classification, Co-location
Combating the Bandits in the Cloud: A Moving Target Defense Approach [19]	This paper's motivation is to decrease knowledge of an attacker by developing a set of MTD strategies that randomize an VM's location. Specificaly focused on Multi-Armed Bndit Problems, the paper develops three models and evaluates results.	Multi-armed Bandit problem is the concept where an attacker attempts to maximize their reward from a slot machine style attack. The authors believe that the best form of defense reduces a strategic attack's effectiveness to that of a random attack. Unlike other papers which strategize a simple VM migration for MTD, this paper evaluates three methods. A complete restructure, a hide max method, and duplicate and deactivate. While the first restructures all resources, hidemax only migrates the VM that rewards the attacker the highest. Results proved similar efficacy between these first two methods, meaning satisfactory MTD can be achieved without migrating all VMs for an application.	May 2017	Proactive MTD, Platform Classification, VM-LM, Multi-Armed Bandit
Comprehensive Security Assessment of Combined MTD Techniques for the Cloud [3]	Moving target defense is known to be a proactive solution, but the effectiveness of security resistance is hard to measure. An appropriate assessment is required to better understand a holistic security analysis and effectiveness of MTD.	The authors analyze security aspects of multiple techniques including shuffle, diversity, and redundancy. Analysis is also performed on some well known MTD algorithms such as HARM. This paper acknowledges the limitations of cost and performance by doing this kind of in depth analysis. Therefore, the work is helpful for research purposes, but is unlikely to become a viable technique dynamically used in the field.	October 2018	MTD Modeling, Computer Systems Organization, Cloud Computing
Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds [26]	Knowing that side channel attacks are an issue faced by computing infrastructure, the authors seek to migrate VMs on a periodic basis to increase attack complexity for an adversary.	This paper aims to model the migration benefit and cost of moving virtual machines around in a network on a regular basis. The migration strategy developed is based on the Vickrey-Clarke-Groves (VCG) mechanism which seeks to maximize social welfare for a VM. One challenge discovered in this paper is the increased cost of migrating virtual machines on a regular basis. This includes both performance and availability, but the cost in USD of continuously performing migrations.	2012	Proactive MTD, Platform Classification, VM-LM, VCG Mechanism
A moving-target defense strategy for Cloud-based services with heterogeneous and dynamic attack surfaces [18]	Many cloud applications are developed in a homogeneous fashion due to the ease of administration, however this significantly decreases an attacker's uncertainty of the application. The authors aim to formulate a cloud-based probabilistic MTD service deployment strategy exploiting the dynamics and heterogeneity of attack surfaces to better protect against attackers.	The goal of the authors' service model is to device a service deployment strategy to hold out an attack as long as possible. One of the challenges is the stated assumptions of performing a snapshot-and-restore service migration model rather than refresh model. This introduces longer downtime for an application due to the increased overhead cost of first creating a snapshot and then restoring. This model also resets the machine back to its vulnerable, potentially compromised state. Work to increase heterogeneity would be required for a real-world solution.	June 2014	Proactive MTD, Platform Classification, VM-LM

TABLE III
ANALYSIS OF RELATED WORKS

VII. Conclusion

In this survey, we have highlighted that cloud computing is growing at a tremendous pace and so are cyber attacks. Because of this, the need for better defense is necessary to ward off attackers. Given the large pool of resources available via cloud computing, it is a natural fit for moving target defense to take hold in the cloud. We have analyzed existing surveys on the topic and identified important research questions pertinent to MTD and cloud computing. With MTD research becoming more prevalent, it is important that research is not simply repeated, but used to explore new and exciting domains. Future research opportunities have been proposed in order for us to better understand the moving target defense paradigm. In conclusion, moving target defense research has matured quite a bit since 2009, but still has a long way to go before mature enough for mass adoption in the cloud system space.

Declaration of Competing Interest

The author declares that there is no competing financial interest or personal relationships that could appear to influence the work reported in this paper.

Acknowledgement

The author thanks Dr. Dijiang Huang for his guidance as a research professor and insights into writing a well articulated technical survey.

References

[1] URL: https://aws.amazon.com/.

[2] Hooman Alavizadeh, Dong Seong Kim, and Julian Jang-Jaccard. "Model-based evaluation of combinations of Shuffle and Diversity MTD techniques on the cloud". In: *Future Generation Computer Systems* 111 (2020), pp. 507–522. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2019.10.009. URL: https://www.sciencedirect.com/science/article/pii/S0167739X19315183.

[3] Hooman Alavizadeh et al. "Comprehensive Security Assessment of Combined MTD Techniques for the Cloud". In: *Proceedings of the 5th ACM Workshop on Moving Target Defense*. MTD '18. Toronto, Canada: Association for Computing Machinery, 2018, pp. 11–20. ISBN: 9781450360036. DOI: 10.1145/3268966.3268967. URL: https://doi.org/10.1145/3268966.3268967.

[4] M. Azab and M. Eltoweissy. "MIGRATE: Towards a Lightweight Moving-Target Defense Against Cloud Side-Channels". In: *2016 IEEE Security and Privacy Workshops (SPW)*. 2016, pp. 96–103. DOI: 10.1109/SPW.2016.28.

[5] Alfred M. Brooks. *Architecture*. 1963. URL: https://aws.amazon.com/architecture/well-architected/.

[6] Mike Burshteyn. *Moving Target Defense - recent trends*. July 2018. URL: https://blog.cryptomove.com/moving-target-defense-recent-trends-253ce784a680.

[7] Ankur Chowdhary et al. *Markov Game Modeling of Moving Target Defense for Strategic Detection of Threats in Cloud Networks*. 2019. arXiv: 1812.09660 [cs.AI].

[8] *CSD-MTD*. Sept. 2018. URL: https://www.dhs.gov/science-and-technology/csd-mtd.

[9] Facts amp; Factors. *Global Cloud Computing Market Size amp; Share Will Reach USD 1025.9 Billion by 2026: Facts amp; Factors*. Jan. 2021. URL: http://www.globenewswire.com/news-release/2021/01/22/2162789/0/en/Global-Cloud-Computing-Market-Size-Share-Will-Reach-USD-1025-9-Billion-by-2026-Facts-Factors.html.

[10] Keith D. Foote. *A Brief History of Cloud Computing*. June 2017. URL: https://www.dataversity.net/brief-history-cloud-computing/.

[11] Dijiang Huang, Ankur Chowdhary, and Sandeep Pisharody. "7.2.2.1 Network Level MTD". In: *Software-defined networking and security: from theory to practice*. CRC Press/Taylor et Francis Group, 2019.

[12] Minhaj Ahmad Khan and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges". In: *Future Generation Computer Systems* 82 (2018), pp. 395–411. DOI: 10.1016/j.future.2017.11.022.

[13] Cheng Lei et al. "Moving Target Defense Techniques: A Survey". In: *Security and Communication Networks* 2018 (2018), pp. 1–25. DOI: 10.1155/2018/3759626.

[14] Y. Magdy et al. "Anonymous blockchain Based Routing For Moving-target Defense Across Federated Clouds". In: *2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR)*. 2020, pp. 1–7. DOI: 10.1109/HPSR48589.2020.9098983.

[15] John McKim. *Abstracting the Back-end with FaaS*. Sept. 2016. URL: https://serverless.zone/abstracting-the-back-end-with-faas-e5e80e837362.

[16] Kramer Michael J. *A Comparison of Three Cloud Strategies: Amazon, Microsoft, Google*. Aug. 2020. URL: https://www.investopedia.com/slug-placeholder-4587679.

[17] Jun-Gyu Park et al. "Ghost-MTD: Moving Target Defense via Protocol Mutation for Mission-Critical Cloud Systems". In: *Energies* 13.8 (2020). ISSN: 1996-1073. DOI: 10.3390/en13081883. URL: https://www.mdpi.com/1996-1073/13/8/1883.

[18] W. Peng et al. "A moving-target defense strategy for Cloud-based services with heterogeneous and dynamic attack surfaces". In: *2014 IEEE International Conference on Communications (ICC)*. 2014, pp. 804–809. DOI: 10.1109/ICC.2014.6883418.

[19] T. Penner and M. Guirguis. "Combating the Bandits in the Cloud: A Moving Target Defense Approach". In: *2017 17th IEEE/ACM International Symposium on*

Cluster, Cloud and Grid Computing (CCGRID). 2017, pp. 411–420. DOI: 10.1109/CCGRID.2017.23.

[20] *Phishing, Ransomware and Co. – An increasing threat: oneclick*™. Feb. 2021. URL: https://oneclick-cloud.com/en/blog/trends-en/increasing-threat-of-cyber-crime/.

[21] Sailik Sengupta et al. "Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud". In: *Decision and Game Theory for Security*. Ed. by Linda Bushnell, Radha Poovendran, and Tamer Başar. Cham: Springer International Publishing, 2018, pp. 326–345. ISBN: 978-3-030-01554-1.

[22] *The Money Behind the Malware*. URL: https://www.sophos.com/en-us/security-news-trends/security-trends/money-behind-malware-threats.aspx.

[23] *Top 25 Cloud Computing Service Provider Companies (2021)*. URL: https://www.guru99.com/cloud-computing-service-provider.html.

[24] Matheus Torquato and Marco Vieira. "Moving target defense in cloud computing: A systematic mapping study". In: *Computers Security* 92 (2020), p. 101742. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2020.101742. URL: https://www.sciencedirect.com/science/article/pii/S0167404820300286.

[25] M. Villarreal-Vasquez et al. "An MTD-Based Self-Adaptive Resilience Approach for Cloud Systems". In: *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*. 2017, pp. 723–726. DOI: 10.1109/CLOUD.2017.101.

[26] Yulong Zhang et al. "Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds". In: *Information Security and Privacy Research*. Ed. by Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 388–399. ISBN: 978-3-642-30436-1.

Austin Derbique received a Bachelor of Science in Computer Science from Utah State University, Logan, Utah, USA in 2017. Upon graduation, he began work as a cloud engineer for a global satellite communications company. As a certified solutions architect on Amazon Web Services, Austin is knowledgeable with compute, storage, and networking. He is currently pursuing a Master of Science in Computer Science at Arizona State University where his research primarily focuses on future blockchain applications.