Cloud Network Security: A Survey on Threats, Existing Solutions and the Path forward

Kaveri Subramaniam
School of Computing and Augmented Intelligence
Arizona State University
Tempe, Arizona

***Abstract*—From sharing and storing images, music and documents to causing an explosion in entrepreneurship globally to now migrating legacy businesses and government applications, the Cloud surely has come a long way in barely the past two to three decades. But with this rapid growth all around the world both physically and virtually providing ease of use, high compute and scalability, it would be presumptuous to assume it has escaped the watchful eye of those who do not share the best of intentions. Adversaries are also able to use the resulting technology to collaborate better and achieve their goals with lesser resources. They now not only have a larger surface area but also a greater reward should they be able to take control of a large number of resources from a minuscule backdoor and escalate their way through this architecture. The ever increasing adoption of cloud, pattern of attacks over the past decade and a drastic change in development and the legal system in order to manage such infrastructure has piqued interest in adopting cloud-special modifications of Network security as we know it today. This paper goes through the familiar route of looking at attack vectors, lessons learned from recent attacks, detection and prevention of vulnerabilities from the perspective of the Cloud. In addition, this paper hopes to bring awareness to the modifications of existing network security concepts specifically for the Cloud, possible adoption strategies by businesses and new branches of ground breaking research that have spawned out of motivation to preserve confidentiality and integrity without sacrificing the high availability and resilience that the Cloud already provides. Keywords-Cloud; Cloud security; Threat; Vulnerability; Cloud provider;**

I. Introduction

Cloud computing has evolved from storage in GDrive and iCloud to a handful of basic components or services which when combined can create infinite services. the NIST cloud computing reference architecture defines five major actors[1]

- cloud consumer
- cloud provider
- cloud carrier
- cloud auditor
- cloud broker

Another security concerning decision would be how the cloud services would be deployed. A cloud infrastructure can be deployed majorly as a:

- Private cloud: Such clouds are dedicated to one consumer implying network and resource isolation. They may be on-site or off-site and can be managed by a third party cloud provider. This is usually used by government organisation or those in the finance and auditing sector that need more control over their infrastructure and have more critical functions.
- Public cloud: This is used to host services that can be accessed by the general public over a public network and the world wide web. Tenants share resources and network. While this may be the most efficient use of resources, from a security perspective it also means that a DDoS attack on one tenant could bring the other tenant down in absence of appropriate precautionary measures by both the cloud provider and the tenants.
- Hybrid cloud: It's a combination of two best suited for when the business may not have many services but some services are critical.

For the sake of this paper, the Cloud implies a "public" cloud and the cloud providers refer to those that provide these public cloud services. However, this does not mean that the private cloud does not offer the services in Section 4.

Based on NIST's definition of cloud infrastructure, the cloud architecture is made up of 3 vertical layers - the service layer, the virtual control layer and the physical layer, and horizontal support layers.[1]

The service layer is what is rented out to consumers in three different forms - Software as a Service, Platform as a Service and Infrastructure as a Service referring to how much control of the stack the consumer may have. IaaS, PaaS and SaaS can integrate with each other or may not even require the lower or higher layers depending on what the services are and other service the consumer has rented out[1]. The control layer contains virtual compute, storage, network as well as the control plane for the above layers to allow dynamic provisioning, access control and translation between the virtual and physical layer[1]. The physical layer has the physical compute, storage and network components like routers, switches, bridges, gateways, firewalls and other provisions in the data center[1]. The support system consists of parts that all of these layers will use like APIs, IAM, KMS, Network Services, Cost Monitor, Logging, Monitoring and Alerting. Most of these are important for cloud security analysis as we will see in later sections.

From a security perspective we see that there are two questions we need to answer - what is the scope of the business and how much infrastructure can the business control. The "deeper" cloud architecture the businesses can control, the more security

we gain in terms of isolation but more components means there is more surface area for attacks and requires higher resources from the business end to secure these components since the responsibility of the cloud provider for those components also decreases. There is a balance between the two that the business as a consumer must decide on based on whether the cloud provider or the consumer is better suited to protect those components and whether the consumer has the adequate resources to manage security as the business scales. It was this flexibility and scalability of the Cloud that caused a massive adoption of the cloud from the early 2010s for entrepreneurs and post the pandemic era for mid-size, large-size and government organizations. As Foundry notes in it's Executive summary outlining the 2022 research findings

> The massive pandemic-driven shift to remote work has kicked the evolution toward cloud-first IT infrastructure into high gear. The majority (69%) of companies have accelerated their cloud migration over the past 12 months, and the percentage of companies with most or all IT infrastructure in the cloud is expected to leap from 41% today to 63% in the next 18 months. In addition, with 60% agreeing that cloud capabilities helped them achieve increased and sustainable revenue in the last year, it is no surprise that next year, organizations plan to allocate an average 32% of their IT budgets to cloud strategy, according to Foundry's annual cloud computing survey. [2, p.2]

This paper is organised to the entire lifecycle of vulnerabilities from their initiation to their impact to how we can tackle them and secure networks on the Cloud. In Section 2, we will study where these vulnerabilities arise from by taking a look at the work of the OWASP project[3]. Section 3 will cover threats that have happened in the past and study their impact. Having proved sufficient motivation as to why Cloud network security deserves special attention, Sections 4 and 5, which are the bulk of the paper will focus on existing resources and what businesses, legal and software teams can do to prevent these vulnerabilities. Finally, Section 6 looks extensively on ongoing diverse research in cloud network security to get an idea of what changes we can expect in Cloud Network security in the upcoming decade or so. The paper ends with a summary reiterating the importance of cloud network security with a broader overview than what was laid out by the limited scope of the previous sections.

II. Threat Vectors

There can be innumerable threat vectors in an architecture as big as the cloud. Each individual system by itself has a host of threat vectors. Add a public global network and we have a very large surface area for attacks to seep in from any corner. The most efficient way to approach this problem would be to first address the most common attacks and secure systems both from top down to bottom up. The two great sources of such information would be the OWASP Project[3] and security related conference papers that summarize this concept with proofs

A. OWASP TOP 10 in Cloud Security

The Open Web Application Security Project was started for non-profit to raise awareness of software security through tools, research, education, training and their extensive community.[3] They are well known for the OWASP top-10 vulnerabilities list which is constantly updated to reflect the top vulnerabilities we see today. For the purpose of this paper, we will discuss some of the vulnerabilities from their new project called OWASP Cloud-Native Application Security Top 10, started in July 2021, within the scope of Cloud Network Security.[4]

As of now, the top 10 vulnerabilities with a brief overview of their impact are:[4]

1) CNAS-1: Insecure cloud, container or orchestration configuration: This has lead to leaking of secrets from publicly accessible s3 buckets, secret resources being accessed from a container using a host and exploiting misconfigurations in Infrastructure as a Code

2) CNAS-2: Injection flaws: This led to serverless data code injection, SQL injections from hosted webpages and OS command injection.

3) CNAS-3: Improper authentication and authorization: This allowed unauthenticated API access and privilege escalation and gaining control through the nodes in Orchestration as a Service.

4) CNAS-4: CI/CD pipeline and software supply chain flaws: This has lead to installation of untrusted images, violating integrity of images, using the pipeline from test environments to gain unauthorized access to production environments

5) CNAS-5: Insecure secrets storage: This has lead to sniffing unencrypted API keys, access to unencrypted storage, access to poorly protected secrets on nodes.

6) CNAS-6: Over-permissive or insecure network policies: Improper network segmentation, pod to pod communication, lack of traffic monitoring allows, unencrypted communications allows for easy sniffing and man in the middle and DDoS attacks.

7) CNAS-7: Using components with known vulnerabilities and CNAS-8: Improper assets management: This can lead to taking advantage of old resources with well-known existing vulnerabilities.

8) CNAS-9: Inadequate 'compute' resource quota limits: Not setting resource limits can allow an attacker with easy access to that system to drown other services in the region.

9) CNAS-10: Ineffective logging and monitoring: This allows attacks to persist in the system and remain undetected for long periods of time.

B. Notable Research Statistics

This section mainly takes a look at research which focuses solely on threat vectors in Cloud Network Security and an analysis of where these vulnerabilities lie. The conclusions

seems to align with that of OWASP. Hanqian Wu et al[5] in their paper on 'Network security in VMs for the Cloud' describe all of the vulnerabilities that are inherent in a VM and it's virtual network and what the possible solutions could be. These vulnerabilities included, but were not limited to[5]:

- VMs: VMs monitoring each other and maybe the host, Rootkits, vulnerabilities associated with Snapshot restoration, no resources available in VM if host was attacked by DoS, remote management vulnerabilities
- Virtual Network: Sniffing virtual network through virtual "hub" when in bridge mode, spoofing virtual network through virtual "switch" when in route mode (specific to Xen hypervisor)

Bernd Grobauer et al[6] in a whitepaper on understanding cloud computing vulnerabilities first define the 4 indicators that constitute a cloud computing vulnerability which were - core-technology vulnerabilities, essential cloud characteristic vulnerabilities, defects in known security controls and prevalent vulnerabilities in cloud offerings. They then explain vulnerabilities in 8 cloud components across the entire architecture starting from compute and to storage to Authentication and Authorization to APIs. Notably some of these vulnerabilities were - poor key management, outdated images, shared network components like DNS, DHCP and IP protocol across tenants, weak authentication, improper authorization, insufficient logging and monitoring, inability to tailor network infrastructure due to virtualisation and VM escape vulnerabilities.

Summarizing the above vulnerabilities and having an idea about their statistics, we can see how they each affect atleast two or all of Confidentiality, Integrity and Availability. In future sections, we will see how these threats have led to compromise in real life and how such analysis has equipped cloud providers to come up with cloud-native solutions and what steps businesses and developers can take to detect and prevent them.

III. Threats experienced in the Real World

As we have seen in the previous sections, most of the errors are due to human errors. What differentiates the level impact of such errors in on-prem businesses versus cloud-native businesses is that, due to it's nature as we discussed in the introduction section, the Cloud promises high availability. It has a lot more clients that are hierarchically dependent on each other and one minor disruption could cause a "Domino" effect. Due to this, a common trait of such vulnerabilities is that the pressure to fix these vulnerabilities across the servers in the minimum time possible is of the utmost importance as the financial impact is exponential with respect to the amount of time between the attack and the fix. We take a look at such examples in the recent past.

Tavis Ormandy of Google's Project Zero[7] contacted Cloudflare on February 17th, 2017 to identify a security issue with their edge servers. The edge servers were operating through the end of a buffer in very specific cases, returning memory containing private information such as HTTP cookies, authentication tokens, HTTP POST bodies, and other sensitive data. Search engines had cached some of that information. A cross-functional team was created to work with Google and other search engines to erase any cached HTTP answers. Having a worldwide workforce allowed people to work on the problem 24 hours a day. They resolved in under 7 hours overall. The greatest period of impact was from February 13 and February 18 with around 1 in every 3,300,000 HTTP requests through Cloudflare potentially resulting in memory leakage. Parallels were drawn to the Heartbleed problem in 2014 that permitted unauthorized third parties to access data stored in the memory of web server programs, even data protected by TLS. Cloudbleed is believed to have affected as many users as Heartbleed. Some of their notable clients were Uber, OKCupid and Fitbit.[8]

Wiz discovered an Azure Cosmos database vulnerability on August 12th 2021[9],a series of flaws in Cosmos DB's Jupyter Notebook functionality that let an attacker to steal the credentials for the target Cosmos DB account, including the Primary Key, which grants access to the database account's administrative privileges. Using these credentials, data in the target Cosmos DB account may be viewed, modified, and deleted via different channels. As a result, every Cosmos DB asset with the Jupyter Notebook functionality turned on was at risk. The vulnerability has been named "ChaosDB," and according to Wiz researchers the it had a trivial exploit that didn't require any previous access to the target environment, and impacted hundreds of businesses, including multiple Fortune 500 companies. Microsoft took measures to remediate the issue within 48 hours of responsible disclosure. Due to additional security systems in place, Microsoft claims it has not leaked any information. Wiz recommended that all consumer assume they have been compromised and change their credentials nevertheless.

Raymond Pompon [10] in an article on Cloud Breaches notes many cloud breaches due to errors from the consumer end discussing the Captial One Cloud breach as a "Swiss Cheese incident" where a multifaceted cloud security architecture was breached as the vulnerabilities in each layer looked like the holes in Swiss cheese. The article then proceeds to provide many Cloud database leaks due to either no passwords or misconfigurations and AWS S3 bucket leaks due to misconfiguration and improper access control.

IV. Existing Integration by Cloud Providers

When Cloud computing started to gain popularity, the major focus was on bringing as many new businesses onboard as possible. The focus has now shifted to move older on-prem applications and government related applications to the Cloud leading to Cloud security to be of the utmost importance. Many older Cloud providers like AWS and Azure are now directing their efforts towards bringing System security services as a part of their cloud offering, many third-party security offerings like Hashicorp's Vault have spawned and newer Cloud providers like OCI have based their entire architecture on secure cloud infrastructure for government and older larger organisations.

In this section, we will focus on the architecture of some of these services.

A. Identity and Access Management

Identity and access management provides all of the Authentication and Authorization requirements for the cloud services. Similar to the way authentications and authorization works on Linux, authorization on IAM have 4 major components:

- Users: To identify who is accessing the resource (may be a human or a resource)
- Groups: To organise Users and assign roles and
- Roles: An abstraction where we can assign the capacity (what they can can cannot do) and responsibility (what they should do) of the user through Policies
- Policies: Access based on Create, Read, Update and Delete operations on resources including IAM itself.
- Credentials: Imported from KMS for authorization

Here we note that resources could be anything - virtual subnets, compute, storage, environments, infrastructure code, or even IAM roles themselves etc. If it can be searched, it's a resource and it can have and should have IAM policies. But it is not just policies that make the abstractions easy. This allows them to also map the right users, groups and roles to the keys stored in the Key Management System and the resources that they are authorized to use. This allows seamless working with Authentication as we will see in the next section. As mentioned later, it is important to have efficient IAM to assign the least privilege possible and the strongest authentication possible to protect malicious insiders from entering the Cloud ecosystem of that business.

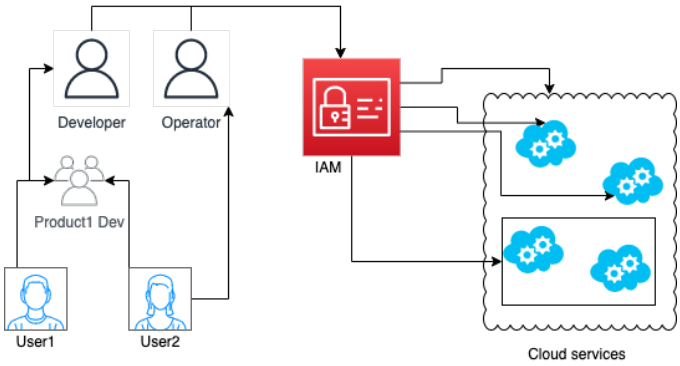

Fig. 1. IAM Example Usage Flow

B. Key Management Systems

While IAM manages authorization, Key Management Systems help implement authorization more effectively through authentication. It also works the other way around, authorization is required to access these keys as keys are also a 'resource'. There are different types of keys that can be specified. There are digital certificates, key-value stores, public-private key pairs, encryption keys for keys. The Key Management System offers a centralized system that then allows us to define, who can access these keys, how these keys will be organised for access through APIs and also handle passing these keys through secure tunnels across different resources without any intervention. Other features would include dynamically generating secrets on demand, encrypting files on demand and extensive auditing features. Based on the scope of the business, it is important to note that IAM and Key Management for lower resources is the responsibility of the cloud provider and out of the control of the business. This is one of the areas businesses can look into to decide whether they find the lower layers secure enough or they'd like to implement a more secure architecture themselves or using other third-party services.

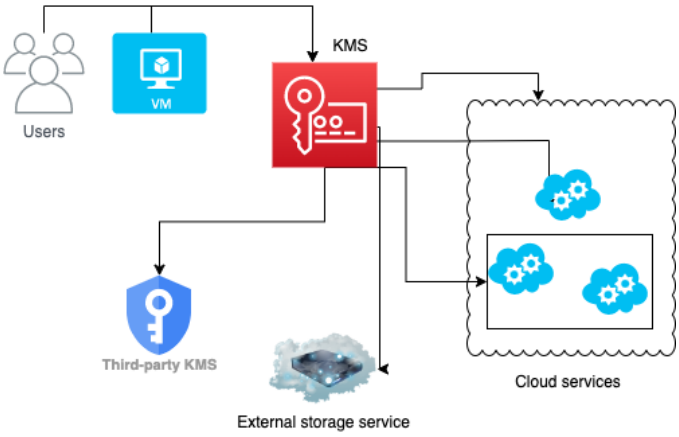

Fig. 2. KMS Example Usage Flow

C. Firewall as a Service

Firewall as a Service implements Next Generation Firewall services for all components in the Cloud at various levels. It can provide not only firewall policies and dropping packets but also packet inspection which can also analyse the contents of the packet. Since this is a more centralized large scale service, FWaaS can also learn from all these attacks or refer to external databases for zero-day threats and act on packets accordingly. FWaaS also seamlessly integrates with SSL, IPSec and other such tunneling protocols, FWaaS can be powerful to log , monitor and prevent attacks from getting into the systems. As mentioned before, FWaaS can be deployed at various levels of the businesses' architecture so this also avoids propagation of threat should the adversary still bypass outer levels due to some other vulnerabilities. FWaaS can also be made to scale according to the components. Given that this would be entirely the responsibility of the cloud provider, they can make sure that FWaaS will always remain up-to-date with the latest technology, protocols and attack information on a much more frequent basis than if the business were to handle that alone. This has become ever more important after the pandemic when employees have begun to move out of office and into more remote settings thus requiring that such security strategies also be deployed "outside" the confines of the business infrastructure to provide security without compromising on speed or making the system too complex to maintain.

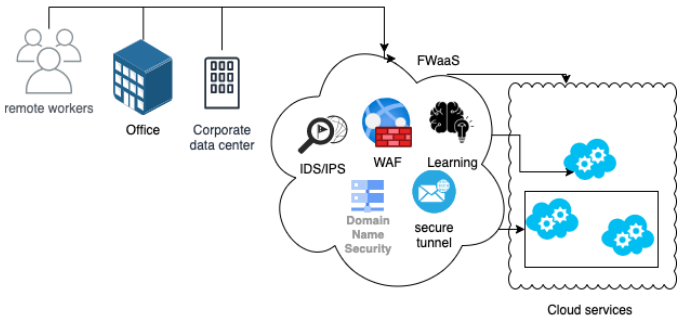

Fig. 3. FWaaS Example Usage Flow

D. Logging, Monitoring and Alarms

While this may not impact Confidentiality or Integrity directly, logging, metrics and Alarms are extremely important to ensure Availability of a service. Cloud providers use a combination of these three to provide a centralised management of logs, metrics and alarms. Every resource will have their own resource metadata which allows for filtering, the logs are then sent through a central api to the metrics database or external third-party metrics service on which we can define alarms based on different metrics, like scale, resource quota limits, traffic, downtime, frequency of downtime over a period of time, etc. Having these Alarms can then allow the businesses to specify what automated actions can be taken to revive or secure the system and quickly identify vulnerabilities and even intrusions into the system. One can also specify who can see these logs, how these logs should be pre-processed to hide data based on laws in the region and also how to archive these logs securely until the customer stops their subscription. In the next sections we will see how logs both led to sensitive data being leaked out due to misconfigurations but the same centralization of logs led to reduction in time from the time of the attack to the time vulnerabilities were identified and fixed from months to just minutes.

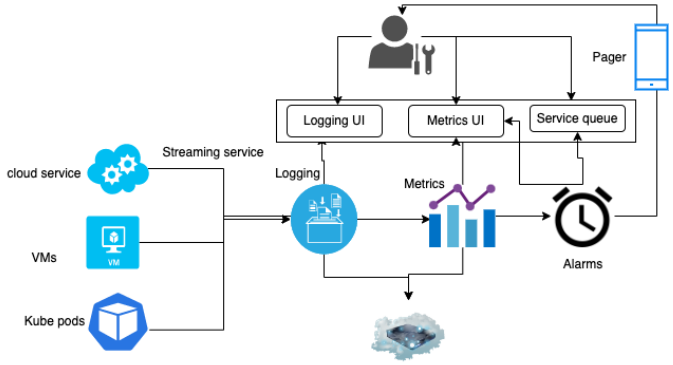

Fig. 4. Logging, Monitoring and Alarms Example Usage Flow

As we can see, Cloud networks have multiple layers of security - Access Control Lists, segmenting sections of the network and encapsulating them with different layers of security, change management for keys, edge security and IAM based on the latest technology and learned behaviour of the network, data protection through encryption and tunneling and continuous logging, monitoring and alarms. Since the top Cloud providers have innumerable clients, they also face extreme legal pressure to protect their customer's sensitive data. So rest assured, using Network Security provided by the Cloud has many more perks. Equipped with these overviews, the next section will discuss how this architecture can be used carefully to extract the most benefit for businesses.

V. Best Practices by Users and Clients

So far we looked at the overall architecture of the Cloud, possible threat vectors at each level and services available to businesses that are Cloud native or planning to migrate, this section will culminate all this knowledge and provide actionable steps on what would be an efficient way to get started on securing the businesses' infrastructure. For a business yet to migrate or in the early stages of migration, it's a very good idea to not put all eggs in one basket. Doing so leads to as Vendor Lock-in and as the business scales, it becomes harder to migrate. We have seen through the examples of CloudBleed and ChaosDB, how the impact of attacks can cascade down the hierarchy. Here we sacrifice ease of development and maintenance for higher Availability (A in CIA). Another area for such a business to look at would be to automate the entire lifecycle right from the very beginning. These are aimed at the DevOps and Security or DevSecOps team and the board members and can be done in the following ways:

- It is essential to choose the right layer of Cloud to abstract upon based on the scope of the business plan. Cloud providers, third-party cloud based-services and open source products have a huge community of developers and professionals who are experts in specific domains and can provide quick, easy and affordable support.
- Leverage Configuration Management Systems like CloudFront and Terraform that can not only manage the entire infrastructure at once but also specify roles, scope and responsibilities to each component and integration to KMS. This ensures that the components are abstracted, their dependencies are well-defined and their visibility can be fine-tuned. This securely handles failure through backup services or cascade aborts and restarts in the right order.
- Leverage Orchaestration services. This ensures fault tolerance, service and network security and resilience around microservices as opposed to running them on standalone compute.
- Have different pipelines, regions and environments for development, testing, pre-prod and prod. It does go without saying that most businesses these days do adhere to this standard and it's worth a mention. As an extension, building logging and alerting plugins for developers to use based on this architecture can streamline log extraction and analysis.

- Ensure that resources that no longer active will be separated and stored securely based on regional and global customer data privacy laws like GDPR. This holds true both for customer data as well as customer resource metadata wherever applicable in order to preserve confidentiality and integrity (as in CIA). Law is increasing becoming an core part of Cloud network security and increases in complexity since resources and data are spread and stored globally.
- Enforce company-wide compliance and raising awareness through training and thorough documentation. Cross-country IT Laws are still under development and revision. Until we reach a stability point, it becomes the responsibility of the business to keep it's employees aware and compliant to the latest standards globally.

Moving to cloud-native applications and enforcing the above means that as a developer in the product teams, the responsibility and skill-set required will now extend to accommodate these changes in the way services are developed, tested and deployed. The bare minimum requirement of a developer would be to stay up-to-date on compliance training and adhere to the new standards of developing features and applications for the cloud. In addition to this, what can truly make the entire business secure is if the developers themselves take the initiative to be more judicious with resource clearing, adequate logging, configuration management and keep themselves informed of the latest technologies and laws surrounding cloud-native applications. This by itself will resolve some the highest vulnerabilities we see today, including but not limited to, misconfigurations or insecure configurations, improper Authentication and Authorization, insufficient logging and inadequate resource quota limits and prevent vulnerabilities from escalating both through the pipeline and across environments.

VI. Ongoing and Future Work

Based on the vulnerabilities we have seen on the cloud to date, we can notice patterns in the sense that since most of cloud is "public" cloud, most on-prem solutions for security vulnerabilities to systems are either insufficient or unnecessarily complicated to accommodate for the cloud. This has piqued curiosity to come up with cloud-native solutions for existing on-prem solutions or to modify the underlying virtual architecture completely so as to remove the threat vectors right at the source.

Guanyu Li et al. [11] have built Iso-Unik, a lightweight multi-process unikernel. Unikernels are a lightweight solution to containers where the libraries between the kernel and applications are stripped to the bare minimum, called libOS, thus providing more security like preventing any access to the shell and meant to run a single process. But this limitation is also what prevented it from scaling to multiprocess applications. For this reason, Iso-Unik was proposed which uses the Intel MPK feature to create a Unikernel that can leverage multiprocess architecture without the need of modification to existing hypervisor and can provide fast compute and forking. They have proved that this implementation does not damage application performance. the overhead was shown to be only 2.5% to 6.3% in Tiny Server, 0.4% in Nginx.

Omar Jamal Ibrahim and Wesam S. Bhaya [12] have come up with an Software Defined Network based Intrusion Detection System that used an SVM classifier to detect attacks. An ODL controller was used to integrate the SDN network into the real-world network. The ODL controller was hosted with a virtual switch on the Mininet cloud network, and the Open Flow Protocol was built and used to interface with it. The ODL controller manages the knowledge transfer from Mininet to the actual network. The accuracy of anomaly detection in SDN networks was improved by the SVM classifier. In comparison to other classifiers, the proposed work indicated that SVM with grid search was statistically significant. In terms of accuracy and False Alarm Ratio metrics, the suggested model beat previous techniques in the literature. The suggested machine learning SDN IDS model had a detection rate of 99.8% of the attack detection accuracy.

Fei Chen et al [13] have developed the first of it's kind step-by-step method to generate a publicly verifiable secure cloud storage protocol given any publicly verifiable secure linear network coding protocol. They claim this to be

> the first publicly verifiable secure cloud storage protocol which is secure without using the random oracle heuristic.[13, p.12]

The main feature of secure cloud storage protocol was to enable the user to check the integrity of the data without possessing the data or being forced to trust the Cloud provider for it. their approach would allow for SCS protocols to be produced automatically from existing secure network coding protocols since the existing solution are performed on an ad hoc basis with low success.

Dijiang Huang et al.[14] provides a secure cloud framework for Mobile computing with the motivation that mobile users can rely on the cloud to perform computationally intensive operations such as searching, data mining, and multimedia processing. MobiCloud would not only provides typical compute services, but it also improve the ad hoc network's functioning by considering mobile devices as service nodes. The proposed architecture would improve communication by tackling network concerns such as trust management, safe routing, and risk management. The increased processing power and connection could enable the development of a new class of apps.

As we have seen here there is motivation from modifying the underlying infrastructure through areas like revising virtualization, building new cloud-native protocols from existing native protocols and modifying existing on-prem security concepts to make it cloud native, to extending the cloud with features like edge computing.

VII. Summary

The Cloud in itself is very young. Since the adoption of services was quite rapid, before most of the developers could get a hold of what the public cloud was, most businesses had already on-boarded onto them due to it's appeal. Over

the years, based on the attacks, it is quite evident that on-prem security solutions can only protect the network to some extent since most on-prem infrastructure are secure from the public internet physically. In this paper, we hope to draw out the similarities between systems and the cloud in terms of their infrastructure yet highlight differences when it comes to the vulnerabilities, threat vectors and areas to be cautious on. One such drastic difference is that while on-prem solutions frequently deal with web application attacks, the cloud exposes the entire underlying virtual infrastructure and seemingly insignificant issues like outdated images, misconfigurations, leaked data from logs seem to take the upper hand. With this in mind, we address existing solutions from cloud providers, what businesses need to focus on more strictly to secure their architecture and what new protocols and features we can look forward to in terms of network security on the cloud.

REFERENCES

[1] F. Liu et al., "NIST Cloud Computing Reference Architecture — NIST," NIST, Sep. 08, 2011. https://www.nist.gov/publications/nist-cloud-computing-reference-architecture (accessed May 04, 2022).

[2] "2022 Cloud Computing Executive Summary," 2022 Cloud Computing Executive Summary. https://resources.foundryco.com/download/cloud-computing-executive-summary (accessed May 04, 2022).

[3] "OWASP Foundation — Open Source Foundation for Application Security," OWASP Foundation — Open Source Foundation for Application Security. https://owasp.org/ (accessed May 04, 2022).

[4] "OWASP Cloud-Native Application Security Top 10 — OWASP Foundation," OWASP Cloud-Native Application Security Top 10 — OWASP Foundation. https://owasp.org/www-project-cloud-native-application-security-top-10/ (accessed May 04, 2022).

[5] H. Wu, Y. Ding, C. Winer, and L. Yao, 'Network security for virtual machine in cloud computing', in 5th International conference on computer sciences and convergence information technology, 2010, pp. 18–21.

[6] B. Grobauer, T. Walloschek, and E. Stocker, 'Understanding cloud computing vulnerabilities', IEEE Security privacy, vol 9, 2nd ed, pp. 50–57, 2010.

[7] "Incident report on memory leak caused by Cloudflare parser bug," Cloudflare Blog, Feb. 23, 2017. https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/ (accessed May 04, 2022).

[8] "Cloudbleed - Wikipedia," Cloudbleed - Wikipedia, Feb. 24, 2017. https://en.wikipedia.org/wiki/Cloudbleed (accessed May 04, 2022).

[9] R. Lakshmanan, "Critical Cosmos Database Flaw Affected Thousands of Microsoft Azure Customers," The Hacker News, Aug. 27, 2021. https://thehackernews.com/2021/08/critical-cosmos-database-flaw-affected.html (accessed May 04, 2022).

[10] R. Pompon, "Is the Cloud Safe? Part 2: Breach Highlights for the Past 3 Years," F5 Labs, Dec. 30, 2019. https://www.f5.com/labs/articles/threat-intelligence/is-the-cloud-safe–part-2–breach-highlights-for-the-past-3-years (accessed May 04, 2022).

[11] G. Li, D. Du, and Y. Xia, 'Iso-UniK: lightweight multi-process unikernel through memory protection keys', Cybersecurity, vol. 3, 1st ed, pp. 1–14, 2020.

[12] O. J. Ibrahim and W. S. Bhaya, 'Intrusion Detection System for Cloud Based Software-Defined Networks', in Journal of Physics: Conference Series, 2021, vol. 1804, 1st ed, pp. 012007.

[13] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, 'Secure cloud storage meets with secure network coding', IEEE Transactions on Computers, vol 65, 6th ed, pp. 1936–1948, 2015.

[14] D. Huang, X. Zhang, M. Kang, and J. Luo, 'MobiCloud: building secure cloud framework for mobile computing and communication', in 2010 fifth IEEE international symposium on service oriented system engineering, 2010, pp. 27–34.