# REVIEW ON-PUBLIC-CLOUD PLATFORMS, PERSISTENT CONCERNS ABOUT CYBERSECURITY

[1]Dr.J.Balamurugan,
Assistant Professor, School of Management Studies,St.Peter Institute of Higher Education and Research, Chennai.
[2]Dr.R.SenthamilSelvan,
Associate Professor, Annamacharya Institute of Technology and Sciences (Autonomous), JNTUA, Tirupati, Andhra Pradesh
[3]Dr.D.Devaiah,
Professor and Principal, Nigama Engineering College, Karimnagar.
[4]Mr.A.BasiReddy,
Assistant Professor, School of Computing, MohanBabu University, Tirupati, Andhra Pradesh.
[5]Dr.G.R.Anil,
Assistant Professor, Department of CSE, Vardhanman College of Engineering, Hyderabad.
Email:*drjbalamuruganpdf@gmail.com, selvasenthami2614@gmail.com, deva7167@gmail.com, basireddy.a@gmail.com

**ABSTRACT:**

After a long period of experimentation, leading enterprises are getting serious about adopting the public cloud at scale. Over the last several years, many companies have altered their IT strategies to shift an increasing share of their applications and data to public-cloud infrastructure and platforms.[1] However, using the public cloud disrupts traditional cyber security models that many companies have built up over years. As a result, as companies make use of the public cloud, they need to evolve their cyber security practices dramatically in order to consume public-cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide.

**Keywords:** Infrastructure as a service (IaaS) and platform as a service (PaaS), software as a service (SaaS), cyber security

## I.INTRODUCTION

While adoption of the public cloud has been limited to date, the outlook for the future is markedly different. Just 40 percent of the companies we studied have more than 10 percent of their workloads on public-cloud platforms; in contrast 80 percent plan to have

more than 10 percent of their workloads in public-cloud platforms in three years, or plan to double their cloud penetration. We refer to these companies as “cloud aspirants”. It have concluded that the public cloud offers more technical flexibility and simpler scaling for many workloads and implementation scenarios. In some cases, using the public cloud also reduces IT operating costs [1-5].

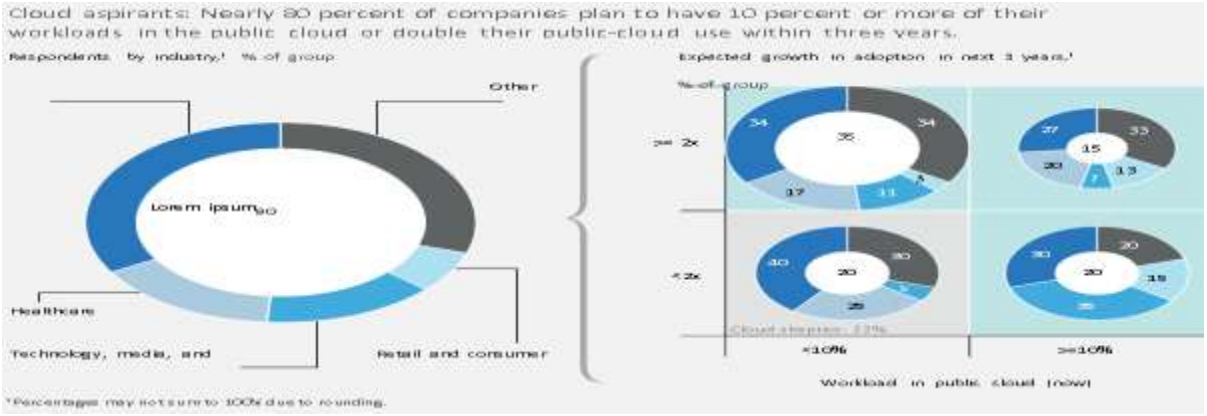


**Fig.1: Cloud Aspirants**

Despite the benefits of public-cloud platforms, persistent concerns about cybersecurity for the public cloud have deterred companies from accelerating the migration of their workloads to the cloud. In our research on cloud adoption from 2016, executives cited security as one of the top barriers to cloud migration, along with the complexity of managing change and the difficulty of making a compelling business case for cloud adoption.

Interestingly, our research with chief information security officers (CISOs) highlights that they have moved beyond the question, “Is the cloud secure?” In many cases they acknowledge that cloud-service providers’ (CSPs) security resources dwarf their own, and are now asking how they can consume cloud services in a secure way, given that many of their existing security practices and architectures may be less effective in the cloud. Some on-premises controls (such as security logging) are unlikely to work for public- cloud platforms unless they are reconfigured [6-9]. Adopting the public cloud can also magnify some types of risks. The speed and flexibility that cloud services provide to developers can also be used, without appropriate configuration governance, to create unprotected environments, as a number of companies have already found out to their embarrassment.

In short, companies need a proactive, systematic approach to adapting their

cybersecurity capabilities for the public cloud. After years of working with large organizations on cloud cybersecurity programs and speaking with cybersecurity leaders, we believe the following four practices can help companies develop a consistent, effective approach to public- cloud cyber security [10]:

**1. Developing a cloud-centric cyber security model.** Companies need to make choices about how to manage their perimeter in the cloud and how much they will rearchitect applications in a way that aligns with their risk tolerance, existing application architecture, resources available, and overall cloud strategy [11].

**2. Redesigning the full set of cyber security controls for the public cloud.** For each individual control, companies need to determine who should provide it and how rigorous they need to be.

**3. Clarifying internal responsibilities for cybersecurity, compared to what providers will do.** Public cloud requires a shared security model, with providers and their customers each responsible for specific functions [12-13]. Companies need to understand this split of responsibilities—it will look very different from a traditional outsourcing arrangement—and redesign internal processes accordingly.

**4. Applying DevOps to cybersecurity.** If a developer can spin up a server in seconds, but has to wait two weeks for the security team to sign off on the configuration, that attenuates the value of the public cloud's agility. Companies need to make highly automated security services available to developers via APIs, just as they are doing for infrastructure services.

## II.DEVELOPING A CLOUD-CENTRIC CYBERSECURITY MODEL

For a company that has only begun to use the public cloud, it can be tempting to build a public-cloud cybersecurity model using the controls it already has for on-premises systems. But this can lead to problems, because on-premises controls seldom work for public-cloud platforms without being reconfigured [5]. And even after being reconfigured, these controls won't provide visibility and protection across all workloads and cloud platforms. Recognizing these limitations, cloud aspirants are experimenting with a range of security strategies and architectures, and a few archetypes are emerging.

The most effective approach is to reassess the company's cybersecurity model in terms of two considerations: how the network perimeter is defined and whether application architectures need to be altered for the public cloud. The definition of the perimeter determines the topology and the boundary for the cloud-cybersecurity model. And choices regarding application architecture can guide the incorporation of security controls within the applications. These two key choices also inform one another. A company might opt, for example, to make its applications highly secure by adding security features that minimize the exposure of sensitive data while the data are being processed and making no assumptions about the security controls that are applied to a given environment.

## III.DESIGN OF PERIMETER SECURITY

The following three models for perimeter design

**Backhauling.** Backhauling, or routing traffic through on-premises networks, is how half of cloud aspirants manage perimeter security. This model appeals to companies that require internal access to the majority of their cloud workloads and wish to tailor their choices about migrating workloads to fit the architecture they have. Companies with limited cloud-security experience also benefit from backhauling because it allows them to continue using the on-premises security tools that they already know well. But backhauling might not remain popular for long: only 11 percent of cloud aspirants said they are likely to use this model three years from now.

**Adopting CSP-provided controls by default.** This model is the choice of 36 percent of cloud-aspirant companies we studied. Using a CSP's security controls can cost less than either of the other perimeter models, but makes it more complex to secure a multicloud environment [6]. For larger and more sophisticated organizations, using CSP-provided controls appears to be a temporary measure: 27 percent of cloud aspirants say they will use this model in three years (down from 36 percent today).

**Cleansheeting.** Cleansheeting involves designing a "virtual perimeter" and developing cloud-specific controls from solutions offered by various external providers. Used by around 15 percent of cloud-aspirant companies, this approach enables companies to apply the best perimeter-security solutions they can find, switching them in and out as needed [7]. Since changing solutions creates technical demands, companies typically

practice cleansheeting when they have enough in-house cybersecurity expertise to select vendors and integrate their solutions. Although those efforts can slow the migration of workloads into the cloud, cleansheeting appears to be on the rise, with 47 percent of cloud aspirants saying they will use cloud-specific controls in three years. Despite the high cost and complexity of cleansheeting, organizations choose this approach so they can support multicloud environments and replace point solutions more easily as their needs evolve.

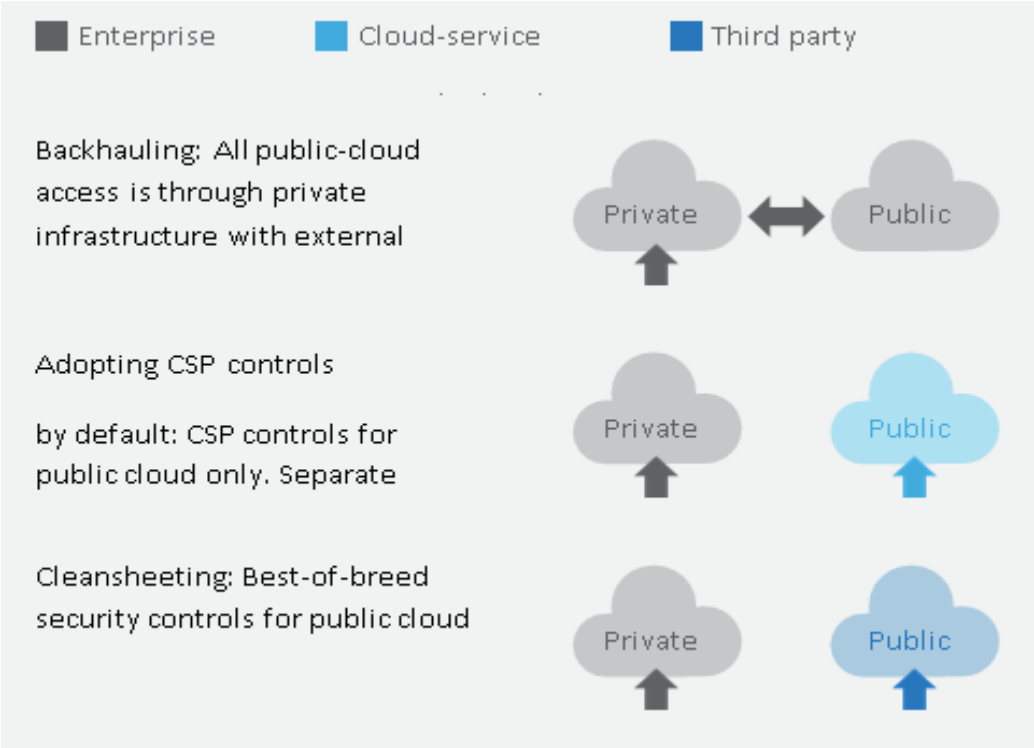


**Fig 2: Architecture of perimeter-security control**

Deciding whether to rearchitect applications for the cloud .The second choice that defines a company's cloud-cybersecurity posture is whether to rearchitect applications in the public cloud, by rewriting code or altering application architectures (or both) [8]. Just 27 percent of the executives we interviewed said their companies do this. The benefits are compatibility with all CSPs (with container architectures, for example), stronger security (with changes like tamper detection using hash, memory deallocation, and encrypting data flows between calls), superior performance (for example, by allowing horizontal scaling in the public cloud), and lower operating costs (because app-level security protections reduce the need for a company to choose best-of-breed security solutions). However, rearchitecting applications for the cloud can slow a company's migration rate. Because of this, a large

majority of enterprises in our survey, 78 percent, migrate applications without rearchitecting them for the public cloud [12].

The choice of perimeter-security design, along with the choice about whether to adapt applications to the public cloud, create six archetypes for cloud cybersecurity. In our experience, five primary criteria inform enterprises' decisions about their overall cloud-cybersecurity model: public-cloud security effectiveness, their desired cloud-migration rate, their willingness to pay additional security costs, their expertise implementing new security programs, and the flexibility they desire from their security architectures.

Rearchitecting applications for the public cloud improves security effectiveness but can slow down migration [13]. Backhauling extends existing controls that companies are already familiar with to public-cloud implementations. Using default CSP controls is the simplest and most cost- effective approach. Cleansheeting controls calls for substantial security expertise but provides flexibility and support for multiple clouds. Organizations can use these criteria to choose the best methods. That said, companies need not apply the same archetype to their entire public- cloud profile. It's possible, even advantageous, to use different archetypes for applications

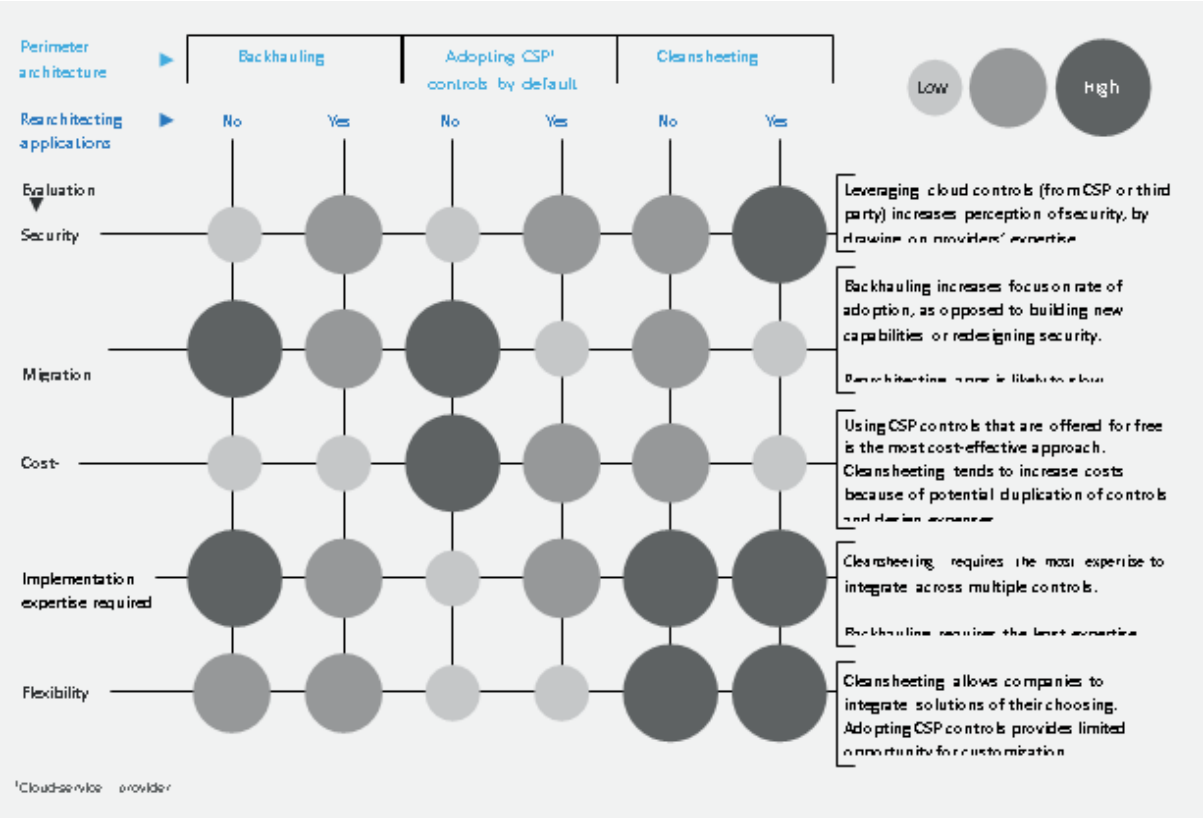

**Fig 3: Assessing Architecture for Cloud Security Model**

## IV.CONCLUSION

Redesigning a full set of cybersecurity controls for the public cloud once enterprises have decided on a security archetype (or a mix of archetypes, with each archetype matched to a group of workloads with similar security requirements), they can design and implement cybersecurity controls. Understandably, companies are experimenting with a variety of designs for controls, and, given the pace of progress, cybersecurity executives anticipate considerable change to these controls over the next three years. Cybersecurity controls can be categorized into eight areas, which organizations need to think about in combination. The eight control areas are listed below, along with observations from our research.

## REFERENCES

[1] Dave Lee, "Warning over 'panic' hacks on cities," BBC, August 9, 2018, bbc.com.
[2] "Ukraine power cut 'was cyber-attack'," BBC, January 11, 2017, bbc.com.
[3] Gartner says 8.4 billion connected "things" will be use in 2017, up 31 percent from 2016, Gartner, 2017.
[4] 2018 vulnerability statistics report, edgescan, 2018.
[5] Michael Kan, "Researcher develops ransomware attack that targets water supply," CSO, February 14, 2017, csoonline.com.
[6] Megumi Lim, "Seven years after tsunami, Japanese live uneasily with seawalls," Reuters, March 8, 2018, reuters.com.
[7] Steven Morgan, "Global ransomware damage costs predicted to hit $11.5 billion by 2019," Cybersecurity Ventures, November 14, 2017, cybersecurityventures.com.
[8] Charlie Osborne, "NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs," ZDNet, January 26, 2018, zdnet.com.
[9] Brian Krebs, "Target hackers broke in via HVAC company," Krebs on Security, February 5, 2014, krebsonsecurity.com.
[10] A Strategic Compass for Security and Defence, EEAS, March 2022.
[11] Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, EDA, February 2022.
[12] Attribution to Russia of malicious cyber activity against Ukraine, Australian government, February 2022.
[13] Brumfield, C., Russia-linked cyber-attacks on Ukraine: A timeline, CSO, April 2022.