Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.758 – 764

REVIEW ARTICLE

Firewall Security of Cloud Server

Vivek Kumar, Nishika

Abstract

Hybrid computers have the features of both analog and digital computers. The digital component behaves like the controller, providing logical operations. The analog behaves like the 'solver,' computing differential equations. Easy2Source Electronics says, "Hybrid computers have been necessary for successful system development and are generally used in scientific applications or in controlling industrial processes."

Advantages

Speed

Hybrid computers have tremendous computing speed enabled by the all-parallel configuration provided by the analog subsystem. This is particularly useful when numerical solutions for differential equations are required, such as in the case of flight simulation. Analog systems have been used for these purposes and are faster than digital computers; they provide the solutions in a shorter time. However, the precision and accuracy of these results are questionable. A hybrid computer on the other hand, provides quick, precise results and is particularly useful when big equations need to be managed in real time and the results are required almost immediately.

Precision

The results provided by hybrid computers are precise, accurate, more detailed and much more useful when compared to their earlier counterparts. This is enabled by the digital component of the hybrid computer. With the hybrid computer, "seed" values are generated quickly, but are mathematically precise as this is achieved from the analog computer front-end. These results are then fed into the digital computer which uses an iterative process and gets the precise and accurate (accurate up to 3 to 4 digits) numerical seed. The total computation time taken to achieve this precise seed value is less than a simple analog or digital computer alone. The combination of speed and precision is extremely important for real time applications like weather system computation or high frequency phased-array radar.

On-Line Data Processing

Professionals in the field of medicine have been using digital computers for various purposes. Considering the speed with which hybrid computers are able to process data, on-line data processing is now being explored. In fact a hybrid computer has been installed at the Bio-Medical Engineering Center at the Ohio State University wherein the cardiac catheterization data from different hospitals is transmitted to the hybrid computer through infrared optics. This data is analyzed in real time and the results made available to the physician immediately.

Thus, the waiting period between the catheterization procedure and the result generation is considerably reduced.

Introduction to Hybrid Computing

A hybrid computing platform lets customers connect the packaged small business software applications that they run on their own internal desktops or servers to applications that run in the cloud.

Software vendors are deciding to develop and deliver new applications as cloud-based, software-as-a-service (SaaS) solutions. This model helps them reach a broader market and serve customers more efficiently and cost-effectively. And, because cloud computing can often provide significant cost, time and ease-of-use benefits, more companies are choosing to buy and deploy cloud computing solutions instead of conventional on-premise software as new solutions needs arise.

However, most companies will continue to use a combination of both traditional on-premise software and cloud-based SaaS solutions. Think about it: You are unlikely to get rid of an application you're running in-house just to swap in a SaaS solution. But if you need a new solution, you're likely to look a range of options, including SaaS applications, to fit the bill.

Importance

Many software vendors with a strong presence and customer base in the traditional packaged or "on-premise" software world are developing platforms that provide new SaaS solutions that extend and integrate with their traditional on-premise applications. Some vendors provide app stores or marketplaces to make it easier for you to find solutions that will work well with those you already have.

For instance, Intuit has developed a platform and Intuit's Workplace App Center so that customers can find and try applications that work with QuickBooks and with each other. Microsoft's Software + Service strategy is designed to connect a myriad of Microsoft's traditional software applications to Web-based SaaS solutions.

Recently, Sage launched its Connected Services offerings, designed to connect users of its traditional packaged software offerings with online SaaS services. The Sage e-Marketing application, for example, connects ACT and SalesLogix users with online email marketing services, while many of Sage's accounting solutions connect with its new Sage Exchange online payment processing.

These vendors realize that most companies will use a mix of on-premise and SaaS solutions for a very long time. While companies can get some value from using some point solutions in a standalone fashion, in many cases, you'll need to integrate the new SaaS solution with an existing on-premise application -- such as integrating payroll to accounting and HR, or social media management to contact or customer management application -- to get the value and efficiencies you need.

From the standpoint of their own corporate interests, vendors can increase revenues and profitability by selling existing customers new SaaS services (either their own or those of their partners) to connect to and extend on-premise solutions they're already using. Having a strong SaaS play that is integrated with their on-premise solutions also helps them protect against competitive SaaS-only vendors that could steadily encroach on their turf.

More altruistically, these vendors want to offer their customers the means to bridge between the on-premise and SaaS solution worlds more easily. After all, it can be very confusing to even sort through and differentiate between all the solutions in a given category, and expensive and time-consuming to integrate them so they work well and easily with what you're already using.

Hybrid Cloud

A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data.

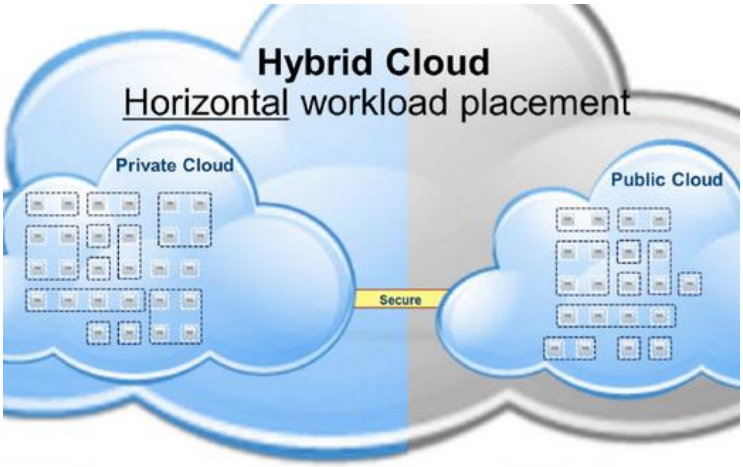
The hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid cloud is also referred to as hybrid IT.

To be effective, a management strategy for hybrid cloud deployment should address configuration management, change control, security, fault management and budgeting. Because a hybrid cloud combines public cloud and private data center principles, it's possible to plan a hybrid cloud deployment from either of these starting points. Picking the better starting point, however, will make it easier to address business goals.

A primary goal of a hybrid cloud deployment should always be to minimize change. No matter how similarly a public and private clouds are matched, design differences will inevitably exist. The greater the differences between the cloud environments, the more difficult it will be to manage multiple clouds as a single entity.

A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization. All cloud computing services should offer certain efficiencies to differing degrees but public cloud services are likely to be more cost efficient and scalable than private clouds. Therefore, an organization can maximize their efficiencies by employing public cloud services for all non-sensitive operations, only relying on a private cloud where they require it and ensuring that all of their platforms are seamlessly integrated.
Hybrid cloud models can be implemented in a number of ways:

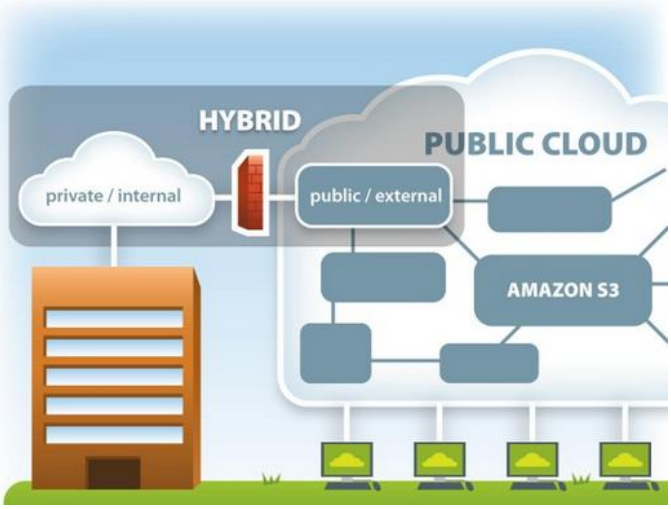
- Separate cloud providers team up to provide both private and public services as an integrated service
- Individual cloud providers offer a complete hybrid package
- Organizations who manage their private clouds themselves sign up to a public cloud service which they then integrate into their infrastructure



In practice, an enterprise could implement hybrid cloud hosting to host their e-commerce website within a private cloud, where it is secure and scalable, but their brochure site in a public cloud, where it is more cost effective (and security is less of a concern). Alternatively, an Infrastructure as a Service (IaaS) offering, for example, could follow the hybrid cloud model and provide a financial business with storage for client data within a private cloud, but then allow collaboration on project planning documents in the public cloud - where they can be accessed by multiple users from any convenient location.

A hybrid cloud configuration, such as hybrid hosting, can offer its users the following features:

- Scalability; whilst private clouds do offer a certain level of scalability depending on their configurations (whether they are hosted internally or externally for example), public cloud services will offer scalability with fewer boundaries because resource is pulled from the larger cloud infrastructure. By moving as many non-sensitive functions as possible to the public cloud it allows an organisation to benefit from public cloud scalability whilst reducing the demands on a private cloud.
- Cost efficiencies; again public clouds are likely to offer more significant economies of scale (such as centralized management), and so greater cost efficiencies, than private clouds. Hybrid clouds therefore allow organizations to access these savings for as many business functions as possible whilst still keeping sensitive operations secure.
- Security; the private cloud element of the hybrid cloud model not only provides the security where it is needed for sensitive operations but can also satisfy regulatory requirements for data handling and storage where it is applicable
- Flexibility; the availability of both secure resource and scalable cost effective public resource can provide organizations with more opportunities to explore different operational avenues



What to Consider

Most small businesses run at least a couple of on-premise software applications that are critical to their business. For instance, it's a good bet that accounting and financials are on this list. Other applications will vary depending on the business you're in, but could include things such as solutions to manage contacts and customers, projects, human resources, logistics or a function specific to your industry.

As you identify and prioritize new requirements to streamline and automate additional tasks, think about the overlaps they'll require with workflows in the core on-premise solutions and processes that you're using. For instance, if you decide you want to streamline payments processing, does your accounting software vendor provide a payments processing service that can easily snap into the accounting application?

By taking advantage of the SaaS offerings available from a vendor's hybrid computing platform, your new solution will generally be up, running and integrated with the core application much more quickly. However, keep in mind that as you snap more services into that core on-premise application, your reliance on that anchor application will grow -- arguably making it harder to switch should your needs change.

Security Threats to Hybrid Computing

A **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.

The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community.

While other uses of the word *hacker* exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the longstanding hacker definition controversy about the term's true meaning.

In this controversy, the term *hacker* is reclaimed by computer programmers who argue that someone who breaks into computers, whether computer criminal (black hats) or computer security expert (white hats), is more appropriately called a **cracker** instead.

Some white hat hackers claim that they also deserve the title *hacker*, and that only black hats should be called *crackers*.

Security exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking.

Techniques

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Firewalls defend computers from intruders by limiting access to ports and machines, but they can still be circumvented.)

Password cracking

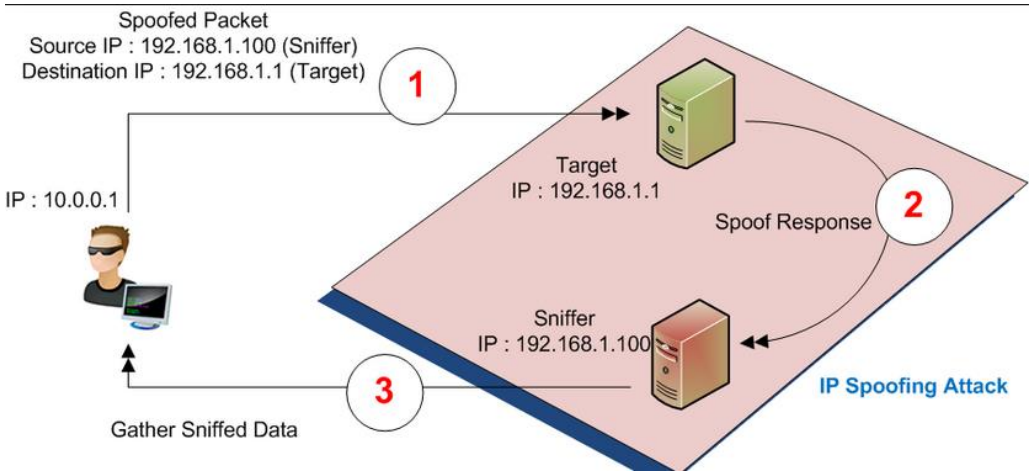
Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (Phishing)

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data and is thereby treated as a trusted system by a user or another program—usually to fool programs, systems or users into revealing confidential information, such as user names and passwords.



Rootkit

A rootkit is a program that uses low-level, hard-to-detect methods to subvert control of an operating system from its legitimate operators. Rootkits usually obscure their installation and attempt to prevent their removal through a subversion of standard system security. They may include replacements for system binaries, making it virtually impossible for them to be detected by checking process tables.

BruteForce implementation in java

```
import java.io.BufferedWriter;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.OutputStreamWriter;
public class BruteForce {
static public void run(char min, char max, int k) throws IOException
{

   BufferedWriter out = new BufferedWriter(new OutputStreamWriter

(new FileOutputStream(java.io.FileDescriptor.out), "ASCII"), 4096);

   int n = max - min + 1;
   char[] chars = new char[n + 1];
   byte[] m = new byte[k];
   int index = 1;
   char[] res = new char[k];
   for (char c = min; c <= max; c++) chars[index++] = c;
   for (int i = 0; i < k; ) {

      for (i = 0; i < k; i++) res[i] = chars[m[i] + 1];

      out.write(res);
      out.write('\n');

      for (i = 0; i < k; ++i)
         if (++m[i] == n)
            m[i] = 0;
         else
            break;
   }
```



```
    out.flush();
}

public static void main(String[] args) throws IOException {
    run('a', 'z', 4);
}}
```

References

- Logik Bomb: Hacker's Encyclopedia (1997)
- Hafner, Katie; Markoff, John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster. ISBN 0-671-68322-5.
- Sterling, Bruce (1992). *The Hacker Crackdown*. Bantam. ISBN 0-553-08058-X.
- Slatalla, Michelle; Joshua Quittner (1995). *Masters of Deception: The Gang That Ruled Cyberspace*. HarperCollins. ISBN 0-06-017030-1.
- Dreyfus, Suelette (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Mandarin. ISBN 1-86330-595-5.
- Verton, Dan (2002). *The Hacker Diaries : Confessions of Teenage Hackers*. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.
- Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. ISBN 0-8166-3345-2.
- Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime*. Routledge. ISBN 978-0-415-18072-6.
- Levy, Steven (2002). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin. ISBN 0-14-024432-8.
- Ventre, Daniel (2009). *Information Warfare*. Wiley - ISTE. ISBN 978-1-84821-094-3.

