

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.775 – 781

RESEARCH ARTICLE



Hacking in Hybrid Computing

Pardeep Balda, Matish Garg

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.

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.

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.

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.

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.

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.

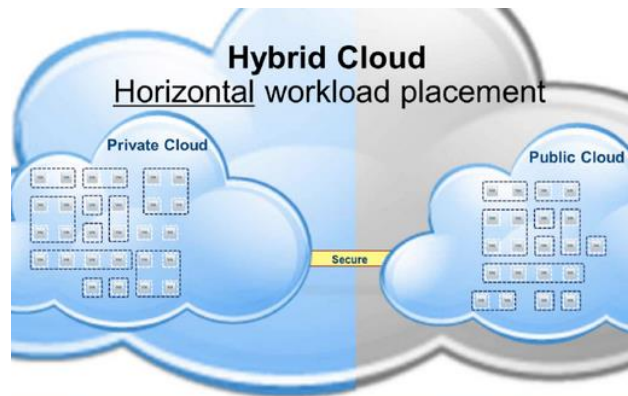
To be effective, a management strategy for hybrid cloud deployment should address configuration management, change control, security, fault management and budgeting. Because a hybrid cloud combines public cloud and private data center principles, it's possible to plan a hybrid cloud deployment from either 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:

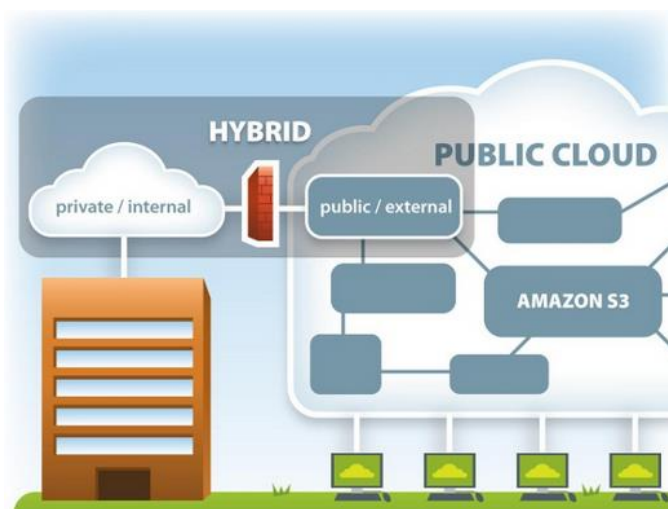
- Separate cloud providers team up to provide both private and public services as an integrated service
- Individual cloud providers offer a complete hybrid package
- Organizations who manage their private clouds themselves sign up to a public cloud service which they then integrate into their infrastructure



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.

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.

White hat

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council, also known as the International Council of Electronic Commerce Consultants, is one of those organizations that have developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.

Black hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. Black hat hackers also are referred to as the "crackers" within the security industry and by modern programmers. Crackers keep the awareness of the vulnerabilities to themselves and do not notify the general public or manufacturer for patches to be applied. Individual freedom and accessibility is promoted over privacy and security. Once they have gained control over a system, they may apply patches or fixes to the system only to keep their reigning control. Richard Stallman invented the definition to express the maliciousness of a criminal hacker versus a white hat hacker who performs hacking duties to identify places to repair.

Grey hat

A grey hat hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.

Elite hacker

A social status among hackers, *elite* is used to describe the most skilled. Newly discovered exploits circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

Script kiddie

A script kiddie (also known as a *skid* or *skiddie*) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature).

Neophyte

A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Blue hat

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term BlueHat to represent a series of security briefing events.

Attack on Hybrid Computing

A typical approach in an attack on Internet-connected system is:

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

Implementation of Phishing Scanner in java

```
import java.io.File;
import java.util.Scanner;

public class PhishingScanner {

    // list of phishing words
    private static final String[] phishingWords = { "DHL", "official",
        "bank", "security", "urgent", "alert", "important", "delivery",
        "ebay", "taxes", "credit", "verify", "confirm", "account",
```

```

"bill", "immediately", "address", "telephone", "ssn", "charity",
"check", "personal", "confidential", "atm", "warning",
"fraud", "won", "irs", "owe", "pay" };

// parallel array of point values
private static final int phishingPoints[] = { 2, 2, 1, 1, 1, 1, 1, 2, 3, 3,
3, 1, 1, 1, 1, 1, 2, 2, 3, 2, 1, 1, 1, 1, 2, 2, 2, 2, 2, 1 };

public static void main(String[] args) throws Exception {
    String fileName = args[0].toString();
    Scanner file = new Scanner(new File(fileName));

    int size = phishingWords.length;
    int wordsCount[] = new int[size];

    for (int i = 0; i < size; i++)
        wordsCount[i] = 0;

    while (file.hasNext()) {
        String word = file.next();

        for (int i = 0; i < size; i++)
            if (word.equalsIgnoreCase(phishingWords[i]))
                wordsCount[i]++;
    }

    System.out.println("\nWord\t\tCount\tPoints\n");
    int totalPoints = 0;
    for (int i = 0; i < size; i++) {
        if (wordsCount[i] > 0) {
            System.out.printf("%-15s %8d %8d\n", phishingWords[i],
                wordsCount[i], phishingPoints[i]);
            totalPoints += phishingPoints[i] * wordsCount[i];
        }
    }
    System.out.println("\nTotal points: " + totalPoints);
    file.close();
}
}

```

References

- Network Security (William Stalling)
- Computer Network(TanenBaum)
- Data Communication (Forouzan)
- Networking Complete Reference(TMh)
- Java Network programming(ORELLAY)
- JAVA BLACK BOOK(DREAM TECH)
- JAVA COMPLETE REFERENCE(TMh)

- FIREWALL 24/7(BPB)
- □ 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.