Data Protection for Cloud Using Homomorphic Mechanism

T.Shashi Kumar[1], J.Deepthi[2], V.Hariprasad[3],

Summary
Cloud computing combination of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high- end networks of server computers. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams..As cloud computing slowly moves into the mainstream, more and more personal data is being moved out of companies' own data centers and into the cloud, which means the data could potentially reside on servers anywhere on the planet. We are providing the Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones

Key words:
Data Protection, Cloud, Homomorphic

Introduction

Also referred to as a network cloud. In telecommunications, a cloud refers to a public Or semi-public space on transmission lines (such as T1 or T3) that exists between the end points of a transmission. Data that is transmitted across a WAN enters the network from one end point using a standard protocol suite such as Frame Relay and then enters the network cloud where it shares space with other data transmissions. The data emerges from the cloud -- where it may be encapsulated, translated and transported in myriad ways -- in the same format as when it entered the cloud. A network cloud exists because when data is transmitted across a packet- switched network in a packet, no two packets will necessarily follow the same physical path. The unpredictable area that the data enters before it is received is the cloud. A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.
A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.
Infrastructure-as-a-Service like Amazon Web Services provides virtual server instance API to start, stop, and access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what- you-use model resembles the way electricity, fuel and water are consumed; it's sometimes referred to as utility computing.
Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure.
Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and Google Apps are examples of PaaS. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud. Some providers will not allow software created by their customers to be moved off the provider's platform.
In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based email to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere.

Paas:

Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to

Manuscript received August 5, 2014
Manuscript revised August 20, 2014

customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

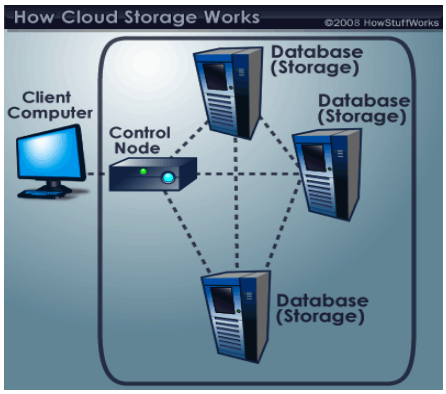


Fig: Working Model of a Cloud Storage

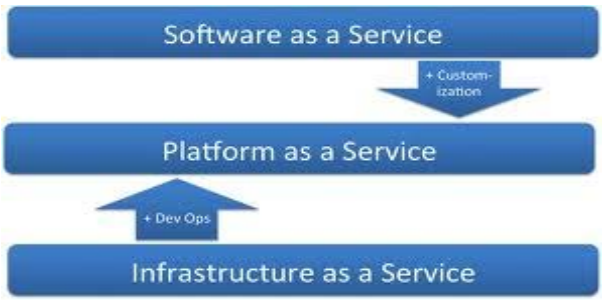


Fig: Cloud Services

How to Safely Store your Data in the Cloud:

What exactly is the cloud? It is basically the collection of computers on the internet that companies are using to offer their services. One cloud service that is being offered is a revolutionary storage method for your data. From music files to pictures to sensitive documents, the cloud invisibly backs up your files and folders and alleviates the potentially endless and costly search for extra storage space. An alternative to buying an external hard drive or deleting old files to make room for new ones, cloud storage is convenient and cost-effective. It works by storing your files on a server out in the internet somewhere rather than on your local hard drive. (For a more technical discussion of cloud computing basics, read more here.) This allows you to back up, sync, and access your data across multiple devices as long as they have internet capability

Encryption:

Trusted Platform Module:

The Trusted Platform Module (TPM) Work Group has been chartered to create the TPM specification. The definition of the TPM architecture comes from the Technical Committee and the TPM Work Group defines the implementation of that architecture. A working knowledge of security in relation to the design and usage of cryptographic modules as well as cryptographic techniques including public-key cryptography, cryptographic algorithms and protocols is recommended.

A new research report on "Trusted Computing" published by Aberdeen Group, a Harte-Hanks Company (NYSE:HHS), reveals that organizations that have deployed applications based on trusted computing infrastructure exhibit superior capabilities in security governance, risk management and compliance compared to other respondents. The term "trusted computing" refers to applications that leverage hardware-based "roots of trust" at the edge of the network and at the endpoints - sometimes referred to as "hardware anchors in a sea of untrusted software" - for higher assurance.

What is full-disk encryption (FDE)

Full-disk encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion. Without the proper authentication key, even if the hard drive is removed and placed in another machine, the data remains inaccessible. FDE can be installed on a computing device at the time of manufacturing or it can be added later on by installing a special software driver.

How to Store:

Comedian George Carlin has a routine in which he talks about how humans seem to spend their lives accumulating "stuff." Once they've gathered enough stuff, they have to find places to store all of it. If Carlin were to update that routine today, he could make the same observation about computer information. It seems that everyone with a computer spends a lot of time acquiring data and then trying to find a way to store it.

For some computer owners, finding enough storage space to hold all the data they've acquired is a real challenge. Some people invest in larger hard drives. Others prefer external storage devices like thumb drives or compact discs. Desperate computer owners might delete entire folders worth of old files in order to make space for new information. But some are choosing to rely on a growing trend: cloud storage.

While cloud storage sounds like it has something to do with weather fronts and storm systems, it really refers to saving data to an off-site storage system maintained by a third party. Instead of storing information to your computer's hard drive or other local storage device, you save it to a remote database. The Internet provides the connection between your computer and the database. On the surface, cloud storage has several advantages over traditional data storage. For example, if you store your data on a cloud storage system, you'll be able to get to that data from any location that has Internet access. You wouldn't need to carry around a physical storage device or use the same computer to save and retrieve your information. With the right storage system, you could even allow other people to access the data, turning a personal project into a collaborative effort. So cloud storage is convenient and offers more flexibility.

Cloud storage basics:

There are hundreds of different cloud storage systems. Some have a very specific focus, such as storing Web e-mail messages or digital pictures. Others are available to store all forms of digital data. Some cloud storage systems are small operations, while others are so large that the physical equipment can fill up an entire warehouse. The facilities that house cloud storage systems are called data centers.

At its most basic level, a cloud storage system needs just one data server connected to the Internet. A client (e.g., a computer user subscribing to a cloud storage service) sends copies of files over the Internet to the data server, which then records the information. When the client wishes to retrieve the information, he or she accesses the data server through a Web-based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files on the server itself.

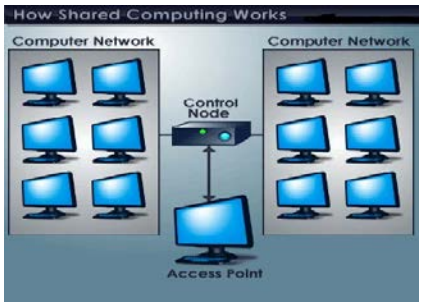
Security and Encryption:

Encryption, which means they use a complex algorithm to encode information. To decode the encrypted files, a user needs the encryption key. While it's possible to crack encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.

Authentication processes, which require creating a user name and password. Authorization practices the client lists the people who are authorized to access information stored on the cloud system. Many corporations have multiple levels of authorization. For example, a front-line employee might have very limited access to data stored on a cloud system, while the head of human resources might have extensive access to files.

Even with these protective measures in place, many people worry that data saved on a remote storage system is vulnerable. There's always the possibility that a hacker will find an electronic back door and access data. Hackers could also attempt to steal the physical machines on which data are stored. A disgruntled employee could alter or destroy data using his or her authenticated user name and password. Cloud storage companies invest a lot of money in security measures in order to limit the possibility of data theft or corruption.

The other big concern, reliability, is just as important as security. An unstable cloud storage system is a liability. No one wants to save data to a failure-prone system, nor do they want to trust a company that isn't financially stable. While most cloud storage systems try to address this concern through redundancy techniques, there's still the possibility that an entire system could crash and leave clients with no way to access their saved data.



Sharing:

Imagine that you've been assigned the task of pushing a very heavy car up a hill. You're allowed to recruit people

who aren't doing anything else to help you move the car. You've got two choices: You can look around for one person big and strong enough to do it all by him or herself, or you could grab several average people to push together. While you might eventually find someone large enough to push the car alone, most of the time it will be easier to just gather a group of average-sized people. It might sound strange, but shared computer systems use the same principle. When a computational problem is really complex, it can take a single computer a long time to process it -- millions of days, in some cases. Even supercomputers have processing limitations.

They're also rare and expensive. Many research facilities require a lot of computational power, but don't have access to a supercomputer. For these organizations, shared computing is often an attractive alternative to supercomputers. Shared computing is a kind of high-performance computing.

A shared computing system is a network of computers that work together to accomplish a specific task. Each computer donates part of its processing power and sometimes other resources -- to help achieve a goal. By networking thousands of computers together, a shared computing system can equal or even surpass the processing power of a supercomputer. Most of the time, your computer isn't using all of its computational resources. There are other times when you might have your computer on, but aren't actually using it. A shared computing system takes advantage of these resources that otherwise would remain unused.

Future Work:

Directions for possible further application of these ideas include interactions between different kinds of secret, replacing the dynamic parts of the current technique to produce a completely static analysis, and supporting interpreted languages without trusting the interpreter

Related code:

```
if (passPwd.equals("") || passPwd1.equals("")) { Integer register Error =
    Integer.valueOf(1);
    session.setAttribute ("registers Error", register Error);
    out.println ("Please enter a valid password.");
    }
    else if (! passPwd.equals(passPwd1)) { Integer register Error =
    Integer.valueOf(2);
    session.setAttribute ("registers Error", register Error);
    out.println ("Your password and confirm password does not match.");
    }
    else {
    String query2 = "INSERT INTO User Login (UserName, PassWord, StockAmt, Technology Stock, Utility Stock) VALUES (?,?,?,?,?)";
    PreparedStatement stmt =
    Con nection.prepareStatement(query2);
stmt.setString(1, passUsername); stmt.setString(2, passPwd); stmt.setInt(3, 0);
    stmt.setInt(4, 0); stmt.setInt(5, 0);
stmt.executeQuery();
    session.setAttribute("sessionUsername", passUsername);
    String sessionID = UUID.randomUUID().toString();
```

Conclusion:

We have presented a new approach for determining how much in-formation a program reveals, based on the insight that maximum flow is a more precise graph model of information propagation than reachability (as implemented by tainting) is. Using a practi-cal quantitative dentition of leakage, the technique can measure the information revealed by complex calculations involving implicit flows. By applying that dentition with an instruction-level bit tracking analysis and optimized graph operations, it is applicable to real programs written in languages such as java. In a series of case studies, our implementation checked a wide variety of confidentiality properties in real programs, including one that was violated by a previously unknown bug. We believe this tech-nique points out a promising new direction for bringing the power of language-based information-flow security to bear on the problems faced by existing applications

References:

[1] C. Dwork, “The Differential Privacy Frontier Extended Abstract,” Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.

[2] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” Proc. 41st Ann. ACM Symp. Theory Computing (STOC 09), ACM, 2009, pp. 169-178.

[3] E. Naone, “The Slow-Motion Internet,” Technology Rev., Mar./Apr. 2011; www.technologyreview.com/files/54902/GoogleSpeed_charts.pdf.

[4] A. Greenberg, “IBM’s Blindfolded Calculator,” Forbes,13 Ju ly 20 09; w w w.forbes.com /forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html.

[5] P. Maniatis et al., “Do You Know Where Your Data Are?

Secure Data Capsules for Deployable Data Protection," Proc. 13th Usenix Conf. Hot Topics in Operating Systems (HotOS 11), Usenix, 2011; www.usenix.org/events/hotos11/tech/final_files/ManiatisAkhawe.pdf.

[6] S. McCamant and M.D. Ernst, "Quantitative Information Flow as Network Flow Capacity," Proc. 2008 ACM SIGPLAN Conf. Programming Language Design and Implementation (PLDI 08), ACM, 2008, pp. 193-205.

[7] M.S. Miller, "Robust Composition: Towards a Unified Approach to Access Control and Concurrency Control," PhD

T.Shashi Kumar is pursuing M.Tech (CSE) in Sphoorthy Engineering College, JNTU Hyderabad. He has completed his B.Tech (CSE). His area of interests includes cloud computing and network security.

J. Deepthi working as an Associate Professor in Sphoorthy Engineering College, Hyderabad. She has completed M.S in Texas A&M University (TX, USA) and has completed her B.Tech (CSE) from KITS Warangal. Her interests are cloud computing and database systems.

V.Hariprasad working as Head Of The Department (CSE & IT) in Sphoorthy Engineering College, Hyderabad. He is pusuing Ph.D in JNTU Kakinada and has completed his M.Tech(CSE) from JNTU Hyderabad and B.Tech(CSE) from JNTU Anantapur . His interests are Bio Infomatics, Temporal Databases and Mining Techniques.