PUNE RESEARCH TIMES
AN INTERNATIONAL JOURNAL OF CONTEMPORARY STUDIES
ISSN 2456-0960
VOL 2, ISSUE 1

REFUGE IN CLOUD COMPUTING

S. V. BARGE
Assistant Professor
SGM College Karad
Shivaji University **(MS) INDIA**

PRAVIN THORAT
Assistant Professor
Dr. D. Y. Patil University
Pune **(MS) INDIA**

ABSTRACT

Cloud Computing, also known as 'on-demand computing', is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud Computing security and privacy are some of the biggest cloud computing issues. Secure your data and ensure your cloud compliance strategy with this primer. As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model. This paper is an attempt to discuss and underline major security threats in Cloud Computing based system simply Refuge in Cloud Computing.

Keywords: *Cloud Computing, Potential Issues, Types of Cloud Computing, Implementing of Could Management Risk.*

INTRODUCTION

The cloud is an enduring new computing paradigm driven by greater specialization and industrialization in the space. Cloud Computing adoption rates have risen rapidly on the back of the tremendous economies of scale that service outsourcing unleashes for users and providers. This helps to cut costs, boost availability and enhance quality and security. And these economies of scale increase dramatically with greater industrialization.

Cloud Computing is defined as a flexible delivery model for services that uses powerful systems and networks with high transfer rates. It typically leverages distributed hardware and software resources and shared, redundant, multitenant platforms that deliver a high degree of scalability.

Public cloud.

Services in the public cloud are highly standardized, provided like a product and generally charged per use. Examples include e-mail, productivity applications or storage. They are freely and publicly available and used over the Internet.

The degree of virtualization can vary – even including dedicated systems. Public clouds are, however, mass-market offerings. They generally fall short of the standards of business users and are not suited for critical data whatsoever. The security characteristics vary between cloud models. The hybrid model combines the best of both worlds.

Private cloud.

Private clouds can involve pooling computing resources within the enterprise and allocating them dynamically to internal users. Normally, though, dedicated private clouds are provisioned and managed by an outside service provider. These clouds are designed to satisfy the specific needs of corporate customers and to provide services on the fly.

Specialized providers with network capabilities can supply private clouds as one-stop, end-to-end solutions. They cover the full range of services and systems, from mobile and stationary devices to connectivity and bandwidth to the integration of in the customer's business processes. They also guarantee service levels through binding SLAs, giving customers maximum peace of mind.

Hybrid cloud.

It appears likely that the hybrid cloud – a combination of public and private clouds – will dominate cloud computing in the enterprise space. Providers are already mixing and matching private clouds and public services to create end-to-end offerings. They integrate public clouds mainly to capture certain functions or capitalize on economies of scale. The combination can even enhance security. A public directory service, for instance, lets users easily use and send encrypted or signed e-mails between secured private domains. Essentially, public cloud services connect private clouds and utilize the integrated security technology.

Observations:

Once organizations decide to move services to the cloud, they should start classifying their data. Critical data needs to stay in the enterprise or a private cloud. Refuge impacts of different models. Maintaining uninterrupted operations and protecting the data and applications are top priorities in any environment. However, cloud computing security profile differs from that of traditional environments. With its elasticity, it avoids failures due to overloading or availability issues. It is less exposed to threats such as the loss or theft of

(laptop) computers since data is stored centrally in the cloud. Instead, more attention must be paid to matters such as reliably segregating data and applications for different organizations or tracking where data is processed in the cloud.

Implementing cloud computing.

Once an organization has decided to embrace the cloud, it should move to the next step: execution. This begins with an analysis of the provider and its services, technical expertise and trustworthiness. Preferably, it should follow a road map: first, define the organization's unique security requirements; next, select the best-fit provider; finally, migrate all or part of the environment to the cloud.

Steps for implementing cloud computing in the enterprise.

1 Define requirements.

In cloud computing, users hand off their data and applications to providers. In so doing, they also delegate their responsibility for security. But an organization can only determine whether the cloud offers adequate security if it has clearly laid out its own security requirements. They generally flow directly from its strategy, business activities and the role played by and certain applications and data in business processes. After defining the requirements, the organization can evaluate service offerings against them. Refuge does not live in a technological vacuum, though. That is why its specialists should be familiar with the latest technology and best practices so the organization can work with its future provider on an equal footing.

Since the user is always outside the cloud, data should be protected not just within the cloud, but also when it is transferred between the user and the provider. This can be done with access and collaboration models and role, permission and digital identity management (organizational, technological and procedural identity and access management).

2 Selecting the right provider.

Clearly defined requirements give organizations a useful list of criteria for evaluating and selecting a provider. The final choice depends on the provider's capabilities, reliability, trustworthiness and ability to satisfy the security requirements. The first dimension addresses the provider's capabilities and process maturity. They can be evaluated based on its service portfolio, its proficiency in certain technologies and the opinions of market observers and analysts. The provider's track record is another dimension. It can be checked by looking up references or talking to other customers. Information on the provider's reputation, by contrast, can be obtained from user associations, business magazines or trade journals.

3 Migrations.

Selecting a cloud provider can have a large strategic impact that goes beyond simply picking a security system. The organization has to spot optimization opportunities and hive off processes for outsourcing. It then awards the contract and begins with migration. Refuge has to be planned from a 'big picture' perspective. Migrations tend to comprise five phases that should be tightly linked with risk management. The five phases of migration.

1. Strategy development
2. Requirements
3. Definition
4. Market analysis
5. Negotiations and contract Operation

Issues in Cloud Computing

Since providers centrally pool services such as e-mail, database applications or security solutions for a large number of users, they tap into vast economies of scale and can pass these savings on to customers. Users appreciate the simplicity and efficiency of cloud computing. They merely plug right into a sophisticated system – there is no need for capital investment on their part. Not that cloud computing is entirely effort-free: organizations still need to define the specifications for their business and lay them out in a contract with the provider. Overall, the cloud offers compelling business benefits, provided rigorous security is in place.

Vulnerability management.

The first step in evaluating IT or business risks are to identify threats in terms of opportunities and impacts. What specifically or generally could happen in a cloud context? Next, the organization should probe for vulnerabilities, such as inadequate data backups or weak authentication before accessing data and resources. The service provider should then integrate security processes. Vulnerabilities cannot be identified without analyzing the infrastructure and how it is used, while security risks can only be evaluated if users quantify the potential financial damage and business impact. Refuge varies depending on the requirements.

Failure due to overloading.

In a traditional server environment, unexpected demand peaks can throttle performance or even cause system failures. Cloud computing, by contrast, allocates resources flexibly and dynamically as demand changes, heading off any chance of overloading.

Privacy problems.

Organizations enforce data privacy themselves if they run proprietary systems in in-house data centers. Providers then have no way of accessing the data. In a cloud, providers could theoretically access the data, but data encryption can effectively prevent them from doing so.

Hardware loss or theft.

Most people would cite unauthorized data access as a key threat. Conventional environments, however, have another, very real loss path for intellectual property: employees carrying mobile devices or USB flash drives with confidential or critical data. If they are
Lost or stolen and land in the wrong hands, the damage can be severe. After all, how many users have really encrypted and backed up the data on their systems? Cloud Computing eliminates the risk of data loss through central data storage and the use of thin clients.

Availability problems due to server failure.

In a traditional IT environment, hardware breakdowns can inflict enormous damage if there is no failover capability. And few organizations have the funds in their budgets to build redundancy into every system. Cloud computing, by contrast, keeps availability high with various methods that stay affordable through economies of scale. Failures are kept under control.

Compliance problems due to distributed data storage.

Unlike in conventional IT environments, users do not always know where in the cloud their data and applications may be. Some providers also use subcontractors. These issues can pose legal problems, particularly in processing personal data (see sec. 5 “Legal requirements and other compliance issues”). There are, however, providers who can restrict data storage to, say, Germany or the European Union and confirm this commitment in a contract.

Out-of-date software.

Organizations that host their own IT environments will also maintain their software themselves. Maintenance is essential: every type of software has bugs and vulnerabilities that, once identified, can be fixed with patches. However, it is also complicated, potentially disruptive and can produce new errors. In cloud computing, this work is done by the provider, who applies patches centrally in order to preserve system stability and failure safety.

Liability issues.

Disagreements over liability occur in all delivery models, including the cloud. In one example, a service level agreement is breached due to technical problems. There are two possible culprits: the network or the hosted IT systems. However, it is impossible to identify which one caused the problem. This does not happen with cloud providers with network capabilities who can supply and manage an end-to-end solution.

Virus threats.

Antivirus programs are commonly used in traditional IT environments. Some new malware can still slip under the radar, however, due to sluggish processors and infrequently updated antivirus software. In the cloud, this task can be centralized, enhancing its effectiveness and update frequency. All of the provider's customers automatically enjoy the same level of protection.

Hackers.

Hackers could theoretically attack any system, data or application in any environment whatsoever. In conventional IT environments, the user is directly responsible for security and has to plan, implement, monitor and update security precautions such as firewalls, intrusion detection, virus scanners or server isolation from the public Internet. In the cloud, these activities fall to the provider.

Changing providers.

Switching to the cloud or changing providers means moving the entire application environment. Vast volumes of data and entire work environments will have to be ported. Business continuity can be assured, however, by migrating the data correctly and allowing employees to use the old and new environments simultaneously for a certain period of time. Experience is needed to maintain availability and avoid data loss during the transition.

Potential problems.

Legal issues figure prominently in the current debate about cloud computing pros and cons. Many organizations need to know the location of the server hosting their data and applications. If they do not, they may run afoul of regulatory requirements such as the German Federal Data Protection Act. Especially financial service providers, life, health and casualty insurers – even institutions and government agencies that use personal data for social security programs – are best served by a provider who can contractually guarantee strong security and fulfillment of disclosure obligations (also see sec. 5 "Legal requirements and other compliance issues").

Data segregation and data protection.

Corporate clients in other industries also believe cloud computing holds legal, technical and organizational risks of varying severity. These companies or government agencies place a premium on keeping data and transactions strictly segregated and thus protected from unauthorized access or manipulation. They are concerned, among other things, about ceding control of their corporate data, insecure or incomplete deletion of data residing on servers, vulnerabilities in tenant segmentation and open user interfaces. Legal certainty may be added to the list if the data is stored outside the European Union's reach and jurisdiction.

Identity management.

Permission management is one of cloud computing main challenges. Managing users and permissions for applications installed "out there" in the cloud requires a different solution from traditional IT systems. Professional providers have the expertise and ability to implement large-scale security systems without weakening cloud computing cost argument.
To improve security, organizations can replace their static passwords with hardware tokens such as standard smart cards or USB flash drives. Whatever their form factor, these tokens come with microprocessors that support powerful encryption keys, stopping many exploits in their tracks. Users enjoy secure access to data and applications, and can even add another layer of protection with an optional PIN.

Conclusion.

Cloud Computing is no less secure than traditional IT service models. However, its risk profile is different, since it faces threats of a different source, type and form. To account for these risks, organizational and technical security measures are updated continually. These updates should always reflect the user's security needs as based on his business model. Refuge problems only arise if providers cannot satisfy these needs. Every new IT trend forces users to weigh the risks and opportunities and learn to trust the new technology. In the case of cloud computing, trust is absolutely pivotal. The cloud is an abstract structure; how it is accessed, and who can access it, will determine how much users trust it.

BIBLIOGRAPHY

1. "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.
2. "Refuge Guidance for Critical Areas of Focus in Cloud Computing". Cloud Computing Refuge Alliance. 2011. Retrieved 2011-05-04.

3. "Cloud Computing Refuge Front and Center". Forrester Research. 2009-11-18. "Cloud Computing Access Refuge Brokers (CASBs) - Gartner IT Glossary". Retrieved 2015-10-01.
4. "Identity Management in the Cloud Computing". Information Week. 2013-10-25. Retrieved 2013-06-05.
5. SU, Jin-Shu; CAO, Dan; WANG, Xiao-Feng; SUN, Yi-Pin; HU, Xiao-Lin. "Attribute-Based Encryption Schemes". Journal of Software 22 (6): 1299–1315. doi:10.3724/sp.j.1001.2011.03993.
6. Attrapadung, Nuttapong; Herranz, Javier; Laguillaumie, Fabien; Libert, Benoît; de Panafieu, Elie; Ràfols, Carla (2012-03-09). "Attribute-based encryption schemes with constant-size ciphertexts".Theoretical Computer Science 422: 15–38. Doi:10.1016/j.tcs.2011.12.004.
7. S.Hemalatha, Raguram (2014). "Performance of Ring Based Fully Homomorphic Encryption for securing data in Cloud Computing Computing" (PDF). International Journal of Advanced Research in Computer and Communication Engineering.
8. Cloud Computing und Services - Status quo und Trends in Deutschland 2009; Cloud Computing and services: the current picture and trends in Germany in 2009; Kraus, M.; Benner, J.; 2009 (German only)