International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Public Cloud Security Challenges & Solution

Surabhi Shukla

Maharana Pratap College of Technology, Gwalior (M.P),
Rajiv Gandhi Proudyogiki Vishwavidyalay, Bhopal (M.P.), India

Abstract: ***Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.***

Keywords: CSP, TPA, VPN, data traffic, SaaS, PaaS, IaaS

1. Introduction

Cloud computing has risen as a new computing paradigm that brings unparalleled flexibility and access to shared and scalable computing resources. The increasing demand for data processing and storage in this digital world is leading a significant growth of data centers. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities [1]. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing.

2. Cloud Computing Paradigm

Cloud-computing data centers offer information technology resources as services. The hardware systems and software systems represent the resources the data center provides as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), respectively. Applications, such as web search, social networking, computation, etc., offered by cloud-computing data centers are hosted as Software as a Service (SaaS). These applications run on virtualized IT resources, namely, virtual machines, provided by IaaS and PaaS. Based on the request, the cloud service providers provision resources such as different types of VMs to the requests.

In cloud computing, the available service models are:

- **Infrastructure as a Service (IaaS)** - Provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components [3].
- **Platform as a Service (PaaS)** - Provides the consumer with the capability to deploy onto the cloud infrastructure, consumer created or acquired applications, produced using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **Software as a Service (SaaS)** - Provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings[2,6].

Four deployment models have been identified for cloud architecture solutions, described below:

- **Private cloud** - The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third-party, and may exist on premise or off premise.
- **Community cloud** - The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.

- **Public cloud** - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud** - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds) [2,6].

Cloud computing is viewed as one of the most promising technologies in computing today, inherently able to address a number of issues. A number of key characteristics of cloud computing have been identified [3]:

- On-demand self-service: A consumer is able to provision resources as needed without the need for human interaction.
- Broad access: Capabilities of a Cloud are accessed through standardized mechanisms and protocols.
- Resource Pooling: The Cloud provider's resources are pooled into a shared resource which is allocated to consumers on demand.
- Rapid elasticity: Resources can be quickly provisioned and released to allow consumers to scale out and in as required.
- Measured service: Cloud systems automatically measure a consumer's use of resources allowing usage to be monitored controlled and reported [2, 6].

3. Public Cloud Role in Cloud Computing

When used to extend existing data center footprints, public cloud can deliver big benefits for data backup and scalability. With companies such as Amazon Web Services, Google, Microsoft and Rackspace offering the ability to create virtual machines in the cloud to support and replace physical servers, cloud virtualization services are being integrated into data center infrastructures. But knowing which features to consider and which vendors to compare can be a daunting task. In most cases, established organizations with IT resources on-premises should not dispose of existing servers and move everything to the cloud. It would be a waste of money, unless the local resources were scheduled to be retired. Even then, there may be some workloads, such as latency-sensitive ones, that should run locally. Similarly, you might not want to put all of your domain controllers on a public cloud. Of course, this does not mean companies with established IT infrastructures cannot benefit from the cloud. The best approach is often to treat the cloud as an extension to the organization's existing IT footprint. In this feature, we look at the benefits of using public cloud versus an on-premises data center.

- **Workload scaling** - There are multiple ways a data center benefits from being extended to the cloud, and one involves workload scaling. There may be times your organization needs to ramp up a production workload beyond what the local data center can comfortably handle. For example, consider the way insurance companies operate. For most of the year, insurance companies typically consume a predictable level of IT resources. However, there may be open enrollment periods that occurs throughout the year. These enrollment periods are especially busy for insurance companies. As a result, existing servers may not be able to handle open enrollment workloads. Rather than buy new servers to accommodate temporary spikes in demand, the companies could use public cloud. If the company's enrollment applications are Web-based, it would be relatively easy for cloud-based Web servers to accommodate the seasonal demand. Once open enrollment is over, the cloud-based Web servers can be decommissioned.
- **Business continuity**- Another advantage of cloud-based VMs is protecting businesses in case of equipment failures or physical disasters. To protect against data center failures, some organizations build geographic clusters that span multiple data centers. Then, if a natural disaster destroys an organization's primary data centers, mission-critical workloads fail over to secondary data centers. Building geo-clusters, however, is expensive and complicated. Another way to use public cloud for business continuity is through VM replication. Not every provider or server virtualization platform supports replication, but some cloud and hypervisor combinations allow duplicate VMs to be created in the cloud and kept in sync with on-premises VMs.

  Public cloud boasts a number of enterprise benefits, but it isn't perfect. Enterprises should be aware of unpredictable cost structures and other drawbacks. Public cloud services offer enterprises several advantages. They allow for flexible and affordable virtual machine deployments and can boost an organization's data backup and workload-scaling capabilities. However, public cloud isn't without its drawbacks.
- **Multi-tenant environment**-One of public cloud's biggest disadvantages is its multi-tenant environment. The host server running your virtual machine (VM) likely is hosting other companies' VMs. Because of this, public cloud providers don't give you access to the hypervisor, so you can't install host-level utilities, such as antivirus software or backup agents. This also means you can't join a hypervisor to an existing domain or cluster. There are also security implications, as well as potential downtime from cloud or WAN failure. In addition, public cloud providers own the hardware and control the underlying software, so they can make low-level changes at will.
- **Unpredictable costs**-Another disadvantage of running VMs in the cloud is that costs can be wildly unpredictable. Public cloud providers are not known for using simple billing models. Typically, you are billed based on the resources you consume. This includes storage resources, but also CPUs, memory and storage I/O. Resource consumption may be billed differently at different times of the day, and not all activity is treated equally. There are cloud providers that differentiate between various types of CPU functions, billing those functions at different rates. Because public cloud providers use complicated billing formulas, it can be difficult to estimate the cost of running cloud workloads. They can vary each month based on how heavily the workloads are used [5].
- **Backups become complicated**-Another disadvantage is how public clouds can complicate your backup processes. If you have mission-critical VMs running in the cloud, you need a way to back them up. While most cloud service providers perform their own backups, they don't necessarily offer restoration services for customers. This can be complex because most of the off-the-shelf backup

products support data backup to the cloud, but not from the cloud. A cloud data backup increases the consumption of storage I/O, network I/O and WAN bandwidth, which may also increase costs [5].

4. Cloud Security Problem

IT departments are struggling with inadequate tools for protecting data traveling both inside and outside their enterprises. They lack strong network segmentation controls, one of the main security shortcomings that played a role in many recent breaches. a.) The old tools used for data traffic security are clearly inadequate and are now routinely defeated or by-passed by hackers. b.)Several glaring deficiencies in how networks applications are protected today are now increasingly apparent. c.) The continued in flux of mobile devices and personal devices is creating more security challenges. d.) Extension of sensitive applications to points outside the enterprise perimeter, including across the Internet, is creating new challenges.

- **Fractured Security of Data Traffic**-Protection of data traffic from end-to-end was one of the biggest security challenges. Fragmentation of controls over data traffic security that includes a mishmash of VPNs, application-layer and network-layer encryption in use by typical enterprises. IT managers reported that they need to use two or more forms of encryption to secure data traffic in their enterprises. More than a third must contend with three or more forms of encryption for securing their data in motion.

- **Network Segmentation Shortcomings**-Digging deeper, IT professionals, want to use data traffic encryption to provide stronger network segmentation for sensitive applications. But they report being unable to deploy encryption for this purpose because of encryption management issues and device performance issues, among others. We're all familiar with the classic security architecture designed to comply with basic data protection and compliance requirements: "crunchy" on the outside, with a strong, firewalled perimeter, but "soft" on the inside, with internal networks largely trusted. But an emerging best practice for data protection is to encrypt a sensitive application's data traffic regardless of where it is. This is driven by the practical realities of modern security gaps and exploits. It is no longer a safe assumption that the firewall perimeter will always keep the bad guys out. In fact, many security consultants and pen-testers advise IT managers to assume that a breach has already occurred and malware is already present in the formerly trusted zone of the enterprise network.

Similarly, it's no longer safe to assume that a sensitive application will not be shared outside the enterprise perimeter. Enterprise applications of all sorts are now routinely extended to external parties, such as partners or suppliers or employees on the move or in home offices. While it has been a longstanding practice to encrypt traffic when it traverses an external, untrusted network, it is not always easy to police this requirement in the era of BYOD and widespread remote access. Even when an application itself may not contain overly sensitive data, a compromised application of any sort can create an opening for attackers to gain a foothold in the enterprise's more sensitive areas. An increasingly common solution, especially among compliance-oriented IT shops, is to use strong encryption on all sensitive data in motion, even on internal networks.

Almost half of those who want to encrypt but can't say it is because management of the various forms of encryption is too difficult. A little more than a third of the respondents cited the reduced performance of firewalls and network devices when they are used to encrypt traffic. The third main reason cited by those who want to encrypt but can't is the complexity of encrypting at a consistent level across a multi-vendor network environment. Different vendors implement encryption at varying levels, via different standards, or even at varying network or application layers, further contributing to the management fragmentation issues discussed earlier.

IT professionals asked how encryption keys are managed in their environments. Despite widespread availability of advanced key management systems, respondents said that they continue to manage keys manually at each network hop, firewall or VPN node. These management and device performance challenges are forcing enterprises into a dangerous trade-off.

- **Muddled Mobility**-The survey findings about management fragmentation and fractured security controls carry over into the enterprise mobile device management area. The survey found that two thirds of companies are now permitting employees to use their own devices to access corporate applications and enterprise data. But how that traffic to and from the mobile devices is protected varies widely.

  The enterprises allowing BYOD indicated that they do not require data traffic to be encrypted to the personal devices, regardless of which networks the traffic will traverse. Of those that do require encryption, the most common modes of data traffic protection were application-embedded HTTPS, enterprise-controlled VPNs and security supplementing a Mobile Device Management System. But none of these was used exclusively by an overwhelming majority of managers, further underscoring the fragmented nature of security controls.
  These findings also indicate a shift in how VPNs are viewed and deployed. Traditionally, a VPN served the purpose of connecting a trusted device to a trusted network. Now, as networks are increasingly untrusted, devices are BYOD, and network security controls are increasingly fragmented and soloed, VPNs and data encryption policies focus on connecting users to applications regardless of which device or network is being used.

- **Application Conundrum**-Similarly, a majority of enterprises permits employees to access corporate applications across untrusted networks such as the Internet. Of those permitting this access, a majority reported using encryption embedded in the applications themselves and separate VPN and encryption technologies controlled directly by the enterprise, with at least a third utilizing both. This is a stark illustration of the fragmented nature of data traffic protection. Because they have no single point of control and encryption policy management, enterprises are very often forced to rely on the embedded encryption supplied by an application developer. How strong is that

encryption? Is it consistent with the encryption policies used by the enterprise for other applications elsewhere? What open source components did the application developer use for that function and are the patches up to date? Are key management controls consistent with the enterprise's policies?

- **Identity and access management**-In case of public cloud, the more companies depend on their I-A-M policy which comes under the SLA between the two parties and share Q-o-S among them.

- Authorization- It gives the policy to manage the security concern of an individual user. Permission to the given or privileged user to access the system application; what resources should be given to the user for an individual task?
- Identity provisioning- Identity of user is the information which it provides at the time of registration. The same information will be seen every time till the account of user is generated. At the time of registration, user has to fulfill some standards which are necessary for the account generation and will further help in improvement of data security. Security concerns are so high that different level of identity checking is required. In the absence of this security checking who will take the responsibility of data.
- Management of personal data-The data which is related to user is the personal data. Data can be of any type either it can be official document or some personal stuff; but all the data which user think is important for it, is its personal data. Hardware requirement depends upon the quantity of data which is to be accessed or how the accessibility of data can be increased, so that user don't feel any inconvenience. Variety of cloud provider is there to access the data stored within the cloud data storage.
- Key management- policy deals with the keys used for encrypting or decrypting the document. Till date the organizations are confused what to do with the keys. The keys should be traverse manually or it should follow some sensitive way to reach the desired goal.
- Encryption-data in transit/rest/memory all can be encrypted but what will be the well-defined policy for this.

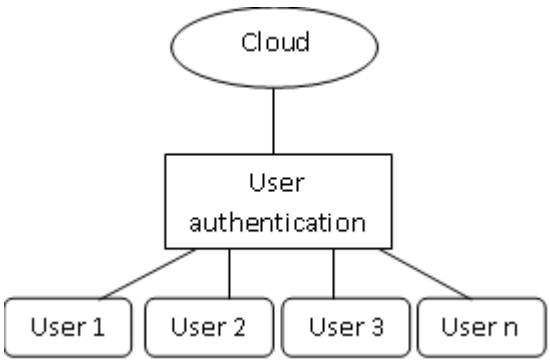


Figure (a)

- Authentication-high assurance security operation should be used. This may include login management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc. can two factor authentication be helpful to manage critical components.

5. Strategy

Security remains a major concern for moving data to the cloud. Although data encryption provides protection, decisions need to be made regarding when, where and how to encrypt data heading to cloud. The proliferation of cloud technology certainly hasn't hurt the security industry. As more people climb aboard the cloud bandwagon, data security ranks at the top of every adopter's list, regardless of the platform. However, many IT pros place less of a burden on security because of increased throughput and **stronger encryption standards**.

While advances in security and cloud technology are robust, security pros should be careful when moving data to the cloud and pay attention to when, where and how cloud-bound data is encrypted. There are a few ways to encrypt cloud-bound data, depending on your cloud stage: before, during or after the move to cloud.

- **Data encryption before taking the cloud plunge**-It seems obvious to encrypt data before moving it to the cloud. But the data that must be encrypted before a move to the cloud is data at rest. The encryption of data in transit -- while extremely important -- may not suffice in every circumstance. For example, the HeartBleed vulnerability took many security pros by surprise because HTTPS/SSL was previously considered rock solid. Admittedly, HeartBleed was more of Apache Web server vulnerability than HTTPS, but many cloud providers' management interfaces reside on similar servers. However, data encrypted before it reaches the Internet is in a better position to defend against HeartBleed. The HeartBleed vulnerability focused on stealing login credentials rather than data is actual data, but access to unencrypttrivial once login information has been compromised. Accessing data that was encrypted prior to an HTTPS login is a different matter entirely.

- **Encrypting data during a move to the cloud**-Encrypting data in transit to the cloud is vital for security and its importance cannot be overstated. Furthermore, encrypting in-transit communications is becoming so popular that a reversal of the current trend seems highly unlikely. Many times -- though not always -- cloud data encryption in transit requires trust in the vendor destination or third-party technology. The cloud vendor or third party must be equally dedicated to security; solely relying on the encryption in-transit is risky business [4].

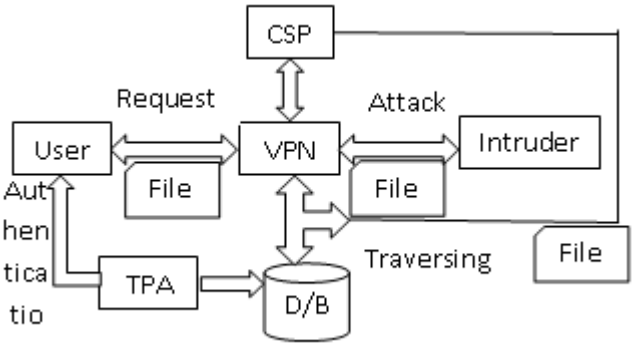


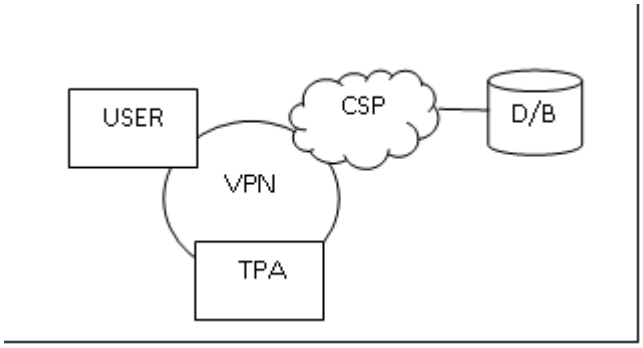
Figure (b)

- **Data encryption comes full circle after the cloud**-Data encryption following a move to the cloud brings the issue of data at rest full circle. At this point, the cloud provider is responsible for data encryption. However, several issues arise when enterprises rely on the cloud provider for data security -- including the ownership. Several cloud providers, such as Amazon Web Services and Google Cloud, have solid security mechanisms replete with encrypted files, SSL login for management and disaster recovery. But, if the data resides on AWS servers Google cloud, who owns the data and encryption keys? It only takes one lawsuit against a cloud provider to expose proprietary data -- encrypted or otherwise -- during legal proceedings. Admins need to have alternatives to relying on cloud providers for security in the event of data compromise. Whatever method is chosen, power brokers within each organization should make tolerable levels of risk clear.

We have kept all these above mentioned three major points in our mind. Data to be encrypted is a necessary task which has to be performed and we will do the same. But meanwhile we have to focus on that only encryption isn't the solution. We have to match this encryption with some more features to make the document more reliable.

Security concern should be start with the initial stage of authentication. Whatever data-file user want to access from the database server which is a cloud based server, the user has to confirm that it's a legal entity or not. With some security features we will check that the user is loyal, if user found loyal then the file can be easily accessed but if it found that the user isn't loyal then it can never view the file[4].

There are three entities user, CSP, TPA together they all generate a VPN among them. We have to focus on how the data travels among all these. If user desire for a particular file it will ask CSP for the individual file, because CSP is the mediator between the original database server. The request when reaches to the CSP,it will immediately forward this to TPA so that TPA can verify the actual user and then further process can be done. This is the core task of TPA to verify the user. After the verification the task of TPA will be finished. We can't blame TPA for any data breach because this isn't the TPA's task. It's only there for user verification.



Figure(c)

After the user verification the further process is then transferred to CSP, then CSP will check how and what files to be delivered to user. CSP will take the individual file and give it back to user.VPN will be the network in which the transfer of files takes place.

Implementing data encryption controls in a cloud environment can be quite challenging for organizations using those services. Ed Moyle discusses the first two steps to implementing data security in the cloud.

When it comes to data security in the cloud, two things are true: First, more and more sensitive information is going there, and second, traditional data protection controls like encryption of data at rest are unlikely to be applied once it's there. As a proof point of that statement, consider the recent *2013 Global Trends in Cloud Encryption* research published in April 2014. According to the survey, 53% of organizations have transferred sensitive or confidential data to the cloud. Yet only 39% of data in software (SaaS) applications is encrypted, and that number lowers to 26% when it comes to platform (PaaS) and infrastructure as a service (IaaS) deployments.

It probably goes without saying that there are some good reasons why this is the case. First of all, data protection controls in a cloud context can be challenging to implement architecturally. Recall that in the cloud, the underlying portions of the stack below that which the customer uses are deliberately opaque; the customer (by design) cedes direct control over these layers to the cloud service provider (CSP) from a management standpoint. So, unless the CSP specifically provides data protection features (note that some do), a customer's ability to implement technical data protection controls without additional engineering might be constrained.

Secondly, from a process standpoint, these controls can be challenging to pull off. There might be legitimate reasons why a CSP requires access to enterprise data -- for example, to debug application functionality or in the case that they provide monitoring services to your company. This means that the logistics of who will hold the encryption keys, as well as whether, how and even if the CSP can get access to them for legitimate business purposes requires discussion, planning and well-thought-out procedures established in advance.

Not everyone will be in a position to implement cloud data encryption controls right away, but even so, taking a few steps now let's organizations analyze both the security benefits they'd get and where those benefits are most needed. It will also help companies understand the level of difficulty if and when they do implement, and, if done strategically, can actually make the implementation process that much easier when a business does decide to pull the trigger.

- **Laying the groundwork**-The first of these steps is data classification and service inventorying. This sounds like "eat your vegetables" advice at some level, but the reason why it's important is the sheer volume of cloud services that even a modest-sized organization will have in play. Most organizations have dozens of cloud services in active use; in fact, if you include SaaS applications -- both sanctioned ones and consumer-oriented services employees may use with or without your say-so -- cloud services might number into the hundreds or even thousands.

Not all of those applications will process sensitive or confidential information, so not everyone will require

encryption of data. Distinguishing which applications are appropriate to apply encryption to from those where it is not is the crux of this first step. Essentially, the goal is to identify and record -- in as granular detail as possible -- where data an enterprise might want to encrypt resides in the cloud. For some situations (i.e., SaaS), "as granular as it gets" might be that the data is held at a certain CSP. For others (i.e., IaaS), it could be that you get down to the level of a certain virtual device or storage container. The point is, your organization should know which applications and environments process the data you care about, versus those which do not, and you should be able to construct a rough idea of where you'd need to apply controls.

If this sounds like a tall order, it can be. Start with a manageable subset and build on it. There are tools that assist in this regard. In a private cloud context or one where your business has a fairly extensive relationship with an IaaS provider, virtualization-aware tools can assist in the inventorying of specific hypervisors to help determine what's running where. SaaS discovery tools exist as well, but in a pinch some service-level information can be gleaned from examining user traffic .To automate the task of keeping track of specific systems and applications, can provide an assist as well to record services and usage as they're identified. The point is, organizations need to establish which data is in which environments so that they can prioritize their efforts.

- **Evaluating specific usage**-After data classification and service inventorying, the next step is where the "rubber meets the road." It's here where your organization must evaluate the specific usage, make the determination about whether it will encrypt, and decide how it will implement encryption. Note that depending on the cloud computing model or service your organization is using, it may need to select different tools to affect this. For example, if you have a high-sensitivity SaaS application and you want to encrypt data within it, affecting this is very different from encrypting a database within a PaaS or encrypting volume storage in an IaaS.

With an IaaS use case, for example, since you have access to the underlying OS on virtual images within that environment, you might choose to implement a tool that operates at the file-system level. In fact, Microsoft and most Linux distributions natively support encrypted file systems that may be viable options. There are dozens of commercial products that support this as well. For a PaaS, your choices might be more limited; you may need support from the developers actively working in the PaaS to author code that leverages CSP APIs or that leverage specific APIs in the application environment they're working in. And, of course, in a SaaS context, since the entirety of the application stack is managed by the CSP, you may find yourself looking to reverse-proxying tools or a specific SaaS-integrated product to accomplish that.

The point is the tools vary and these differences should be noted and planned around; if your organization needs to purchase multiple tools to do this, it will need to plan its budget accordingly. Using the inventory and data classification evaluation that you've already done can help prioritize which approach is most valuable and/or urgent.

6. Conclusion

In light of these data traffic security problems, it's no wonder that network security improvements rank among the enterprises' IT project priorities for 2015, according to the survey findings. More than half indicated that network security improvements are planned for 2015 and nearly a quarter named network security as a top IT priority for the enterprise in the coming year. In total, two-thirds of enterprises report that they are budgeting such projects. If enterprises are studying and learning from the recent parade of data breaches, then we can safely predict that several initiatives will be included in these network security projects:

1. Proactive security: More enterprises will establish proactive security and stronger network segmentation by encrypting sensitive data traffic over all networks.
2. Encryption consolidation: Reducing the number of forms of encryption and consolidating encryption control will make protecting traffic simpler and reduce the possibilities of gaps in the end-to-end data path.
3. Simpler policy management: Because all networks are essentially untrusted today, it makes less and less sense to focus solely on network-based VPNs that connect a device to a network. Instead, encryption policies are now focusing on connecting an authorized user to the applications they want to access and then applying the required encryption profile. The policy should be applied regardless of which devices or networks are involved, which in turn enables more consistent, enforceable and auditable encryption policies.

In the end, the IT security community already has benefited greatly from the lessons learned by the surge in hack attacks. IT security now has the attention of senior management and budget decision-makers. In the long run, this heightened prioritization and investment can only improve the overall effectiveness of security controls and allow them to evolve to meet the changing needs of users and applications in the modern enterprise.

References

[1] **"Cloud Computing Security Issues and Challenges";** International Journal of Computer Networks (IJCN), Volume (3): Issue (5): 2011; Kuyoro S. O., Ibikunle F. & Awodele O.
[2] "**Observing the Clouds : A Survey and taxonomy of Cloud Monitoring**"; Ward and Barker *Journal of Cloud Computing: Advances, Systems and Applications* (2014) 3:24
[3] "**Addressing cloud computing security issues**";Dimitrios Zissis ∗, Dimitrios Lekkas; Future Generation Computer Systems 28 (2012) 583–592
[4] www.techgig.com
[5] www.techtarget.com
[6] "**Exploring Cloud Computing for Naïve**";Reema Ajmera & Rudra Gautam; IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.12, December 2014 62
[7] NIST cloud definition, version 15 http://csrc.nist.gov/groups/SNS/cloudcomputing/.

Author Profile

Surabhi Shukla holds a B.E. in Computer Science, from RGPV and is currently pursuing M.E. in Computer Science at the same university RGPV. She has been involved with Infosysworld, as a business analyst for 1 year. Her interest area is Cloud Computing and database security. She is trying harder to secure database in cloud.