International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.4., 2016
(July-August)

RESEARCH ARTICLE

ISSN: 2321-7758

A STUDY IN DATA SECURITY IN CLOUD COMPUTING

NAVJEEVAN KUMAR[1], DHARAMBIR SINGH[2]
[1,2]M.Tech Research Scholar, SITM Rewari, Haryana, India

NAVJEEVAN KUMAR

ABSTRACT

The vision of 21stcentury computing is that users canaccess Internet services over lightweight portable devices rather than via variants of the traditional desktop computer. Consequently, users will have no interest in large, powerful machines. How, then, will computing power be provided? The answer to this question lies in cloud computing. Cloud computing is a recent trend in IT in which computing power and knowledge are moved away from the desktop and desktop PCs into giant datacenters. In the cloud computing paradigm, applications are delivered as services over the Internet. The key driving forces behind cloud computing are the presence of broadband and wireless networking, falling storage prices, and progressive enhancements in Internet computing software packages. Cloud service shoppers can add additional capabilities at peak demand, reduce prices, experiment with new services, and remove unessential capabilities. Service suppliers can increase utilization via multiplexing and allow for larger investments in software packages and hardware.

KEYWORD: Confidentiality, integrity, availability, transport layer security, cloud digital signature

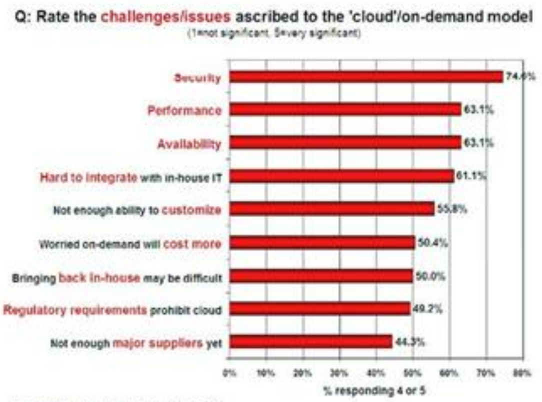
1. INTRODUCTION

Although cloud computing transfers some control over data and operations from the client to the cloud provider—in much the same way organizations commit part of their IT operations to outsourcing companies—operating a secure cloud-based IT environment remains a shared responsibility[1].However, even fundamental tasks such as applying patches and configuring network security are the responsibility of both the cloud service provider and the consumer. This paper analyses examples involving both public and private cloud services [2]. In the Infrastructure as a Service(IaaS) model, the cloud provider offers a number of preconfigured virtual machines (VMs) and is responsible for keeping them constantly updated with the latest security system patches. Then, when clients provision VMs, they trust the Cloud provider to deliver secure systems [3]. The clients do not have access to the hypervisor layer, the underlying controlling scheme that manages one or more VMs that run on a physical machine. The hypervisor layer typically precludes the apportioning of the virtual network segments with any of the other hosted VMs to avert network-based intrusions. Furthermore, the cloud supplier may offer facultative virtual private network (VPN) potentiality so that the customer can check a protected network that is not directly visible to Internet-based attackers. Maintaining the patch level for all provisioned VMs after the initial deployment, as well as a properly configured VPN, is the client's responsibility. Such measures shield their valuable data and infrastructure. However, if a client chooses to refrain from purchasing a VPN option or does not patch any of their web-facing VMs, the machines can become vulnerable [4].If an establishment decides to follow up these mechanisms in a private cloud through their internal IT department, they can trust their business policies to monitor aspects such as data confidentiality as well as application and system access control. Employees would be entrusted to handle the IT infrastructure because they are reacquainted with business policies on a regular basis. In this environment, organizations must handle the risk of unauthorized privileged user access, data loss prevention, malicious intrusions, and unintentional user errors. In addition, employees must observe and comply with internal or regulatory guidelines. If the organization decides to implement these mechanisms in a public cloud using the cloud provider discussed in the previous example, they will have to rely on written business arrangements to govern the aspects stated above. Furthermore, the organization has to manage these risks and comply with the same internal or regulatory guidelines [5].In the cloud, locating where data is physically stored is often difficult. Certificate processes that were visible in the past are now hidden behind layers of abstraction [6]This lack of visibility can result in a number of certificate and submission issues. It may also prevent certain IT use cases from being conducted in a strictly public cloud environment. Therefore, clients must ensure that they can select a physical location for even a public cloud deployment and that abbreviates are in place that ensure focalized data storage [7].

SURVEY OF SECURITY IN CLOUD COMPUTING

A. Confidentiality

For both enterprises using cloud environments and cloud service providers, encryption is a critical requirement for securing data. Vormetric encryption provides an uncomplicated means of protection comprising key management, fine-grained access controls, and advanced security intelligence data to protect sensitive data-at-rest within public, private, and hybrid cloud environments [8]. Through cloud encryption for cloud implementations, one can meet compliance requirements for encryption, separation of duties, and access controls for protected data, including PCI- DSS and Data across Borders [9]. In addition, cloud encryption can help protect against data breach incidents through the use of secure encryption, key management, and policy-based access controls on protected data in cloud environments as show in Fig1.MThe risks also include those posed by the exposure of customer data to cloud providers and of data exposure because of the shared, comingled data storage used to support cloud environments. Furthermore, cloud computing encryption(s) provides raw security intelligence on data access to encryption-protect information; such intelligence enables a Security.



Source: IDC Enterprise Panel, August 2008 n=244

Fig. 1. Ratings given to the various challenges/issues ascribed to the "cloud"/on-demand model.

Encryption provides a single, scalable solution that can easily encrypt any file, database, or application wherever they reside on supported operating and file systems, without sacrificing application performance and while avoiding key management complexity. Furthermore, cloud encryption Includes seamless key management within the solution and is fully transparent to applications and users, thereby allowing existing processes and usage to continue with no changes [11].This design efficiently protects any data within cloud environments. Similarly, the design of the cloud solution supports detailed, policy-based separation of duties to offer a higher degree of security. Unauthorized programmatic access by cloud administrators, root, and network system administrators to restricted data is prevented while allowing appropriate user and application usage.Vision and Malthus, a secure data cloud provider, eliminates the risk of exposing private information and data storage in a single joint. They also design solutions that record data in clouds for easy integration with SIEM solutions and to provide detailed information on use and access. Access attempts using SIEM solutions allow calculations to determine risks to applications, and even administrators. In terms of encryption for cloud environments, Malthus allows organizations to monitor how well their data are protected from the public; it possesses special applications and is a hybrid cloud; traditional datacenter resources are also present on premise [12].A single, centrally managed infrastructure across all environments facilitates the management of cloud data security as well as data security for physical and virtual datacenter resources. However, providers of cloud services create high value services with enhanced data security services in private clouds: Software as a Service (SaaS), Platform as a Service (PaaS), IaaS, SaaS hosting, and others. In this regard, modern cloud encryption is an ideal solution because it is multi-tenant ready and scalable, is carried out safely, and includes APIs and interfaces that are required in order to operate in synergy with existing infrastructure. Through new cloud computing encryption methodologies, new opportunities are presented to address the concerns of enterprise customers directly regarding the use of cloud services that will expose them to financial costs in the event of loss of data protected by law, and intellectual property theft, or non-compliance regulations [13]. Services provided by encryption clouds improve with higher levels of data protection that meet regulatory standards and results in unique cloud solutions. When Edward Snowden revealed to reporters the first details of the surveillance practices of the NSA in June 2013, industry analysts expected his revelation to adversely affect cloud deployment plans. For example, the Information Technology and Innovation Foundation said in August 2013 that leaks could cause cloud providers in the United States to lose 10% to 20% of the market to foreign competitors abroad, or up to 35 billion dollars in potential sales in 2016. The Cloud Security Alliance (CSA) received a similar reaction from European companies regarding fears that the U.S. government will have access to their data. However, after six months, the effect seems to be less severe than had been expected. Despite reports of sluggish sales of cloud services by United States vendors to overseas companies, and experts now expect that the leaks reported by Snowden will have little effect on long-term sales. The business benefits of employing cloud-based services continue to override fears of government control as shown in Fig 2 and 3

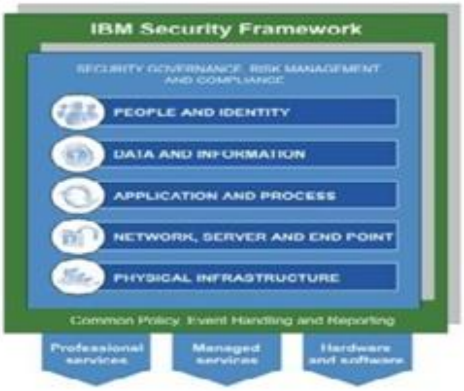


Fig. 2. IBM's cloud security framework.

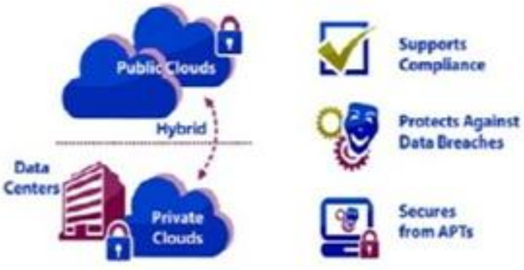


Fig. 3. Cloud security compliance elements.

However, the NSA leak prompted increased focus on data security and cloud protection. Such focus is expected to increase in 2014. According to IT-Harvest, the leaks showed how little control companies exercise over data stored in clouds: "There is a fundamental shift to a model zero confidence in the cloud." In institutions, "there cannot be any gap in the chain of trust from the internal resources to the cloud and back." Analysts report that IT security officials are considering several key areas, such as data encryption, key management and data ownership, regionalization, and the need for increased government transparency, to enhance cloud security.

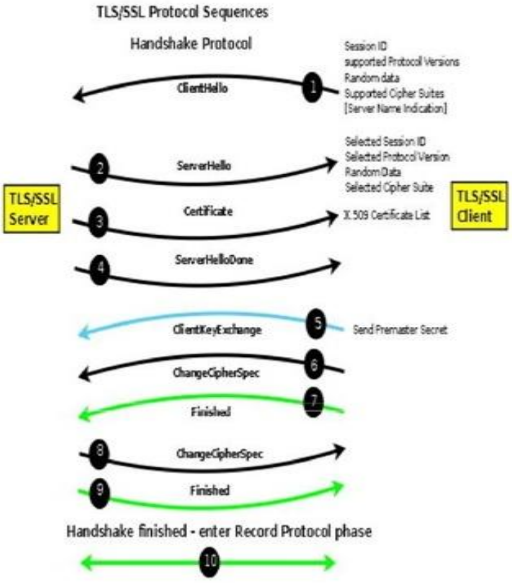


Fig. 4. TLS/SSL protocol sequence.

1) Data encryption: The leaks by Snowden attracted much attention in the field of encryption. Consequently, major service providers, such as Microsoft, Yahoo, and Google, have since added encryption to end-to-end data hosting and management for customers. For example, Google Cloud Storage now automatically encrypts all new data written to disk. Server-side encryption will also soon be available for old data stored in Google clouds. Since the leaks, Microsoft announced its intention to increase support for encoding various services such as Outlook.com, Office 365, Sky Drive, and Windows Azure. By 2014, Microsoft expects to complete the development of measures for encoding information being transferred between client sites and datacenters and data in transit between its own datacenters. Similar to Google, Microsoft plans to maintain knowledge in various cloud service providers' clouds. Drop-down, Sonic.net, and Spider Oak have announced support for similar programs, encryption, options, future proof encrypted knowledge, and 2048-bit keys for the "perfect forward secrecy" methodology. According to consultants, these measures are very important for protecting the movement of knowledge between the client companies and the suppliers of cloud services. Classified documents from the NSA show that they are trying to weaken encryption algorithms used by the public. The faucet fiber links that connect datacenters and service suppliers provide the impetus for these efforts.

2) Key management and data ownership: According to the US government, during its dispute with Lavabit, a secure email services provider, cloud service firms must hand over their encryption keys when asked. Such statements have focused considerable attention on key management and data ownership. Eric Chiu, the president of HyTrust, a cloud infrastructure management company, confirmed that although encryption efforts by service providers play a vital part in improving cloud security, their effectiveness is limited.

B. Integrity

The sequences used in the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocol are illustrated in Fig. 4. While the TLS/SSL segments of our proposed framework were being processed, we observed underutilized computation and network resources on both the server and client sides that result from the sporadic computation and communication bottlenecks that occur when the network and computation workloads are varied. When the given network and computation resources are under-utilized, the TLS/SSL throughput can be improved by maximizing the utilization of the given resources. Applying a specific compression method to a TLS/SSL connection may not be optimal if the connection and computation workload are different and dynamic. If excessive data are loaded for a low-bandwidth TLS/SSL connection, a compression mechanism reflecting environment heterogeneity. (Such as the device, network, and cloud) should be applied. However, considering that conventional TLS/SSL mechanisms provide a static compression mode, a renegotiation request by an application must alter the compression algorithm to be applied. Therefore, a mechanism that enables TLS/SSL to identify the best compression technique for TLS/SSL connections in a timely and transparent manner must be applied while considering the aspects specified.First, we introduce tightly coupled, threaded TLS/SSL coding, with the objective of maximizing computation and communication utilization when TLS/SSL data segments are sent and received. In conventional TLS/SSL, computation routines, such as compression and encryption operations as well as the TLS/SSL network routines are executed in a loosely coupled manner. This type of execution triggers frequent blocking and wake-up operations in the TLS/SSL process.

C. Availability

Business organizations must have IT solutions that are "always on" because interruptions in computing services result in increased costs and can sometimes contribute to a loss of consumer confidence. Cloud computing fundamentally relies on the Internet. Thus, companies interested in beginning or expanding their use of cloud-based services must work closely with an IT consulting firm that can show them how to organize bandwidth levels and meet their IT needs.

1)Examples of Cloud Failures: The importance of theavailability of cloud resources has been demonstrated by the recent outages of several high-profile cloud providers, with Amazon and Google being among the most notable.

a)Amazon cloud failure: The EC2 infrastructure outage of Amazon was caused by human error involving a configuration mistake in a scheduled network update. Amazon datacenters are split into availability zones, areas inside buildings that are intended to be isolated from each other. The main network serving one of four zones in the North Virginia Amazon datacenter required a larger capacity. Consequently, an Amazon employee mistakenly moved the traffic off a primary network onto a secondary network that had a lower bandwidth and was predominantly used as a backup network. The misconfiguration overloaded the backup network because of the excessive traffic.

b) Google cloud failure: A recent Gmail outage took place when Google took a small number of Gmail servers offline for maintenance [14]. Google underestimated the change in traffic load that would be placed on request routers, which send web queries to the appropriate Gmail servers. The routers became overloaded with traffic, and the capacity was unable to manage the increase in traffic. As a result of the error, Google brought in additional request routers online to add more capacity [15]. In addition, Google has taken steps to isolate Failures in datacenters so that traffic overload in one area would not create problems elsewhere. Similar to the Amazon outage, the Gmail outage demonstrates how a cloud failure can easily occur. In the case of Google, the level of traffic placed on request routers was underestimated when servers were taken offline. This simple human error created a significant disruption in Gmail services. Millions of users rely on Gmail to send and receive emails; thus, when the Gmail outage occurred, millions of users were affected and thousands of dollars of revenue were lost. Google is taking steps in the right direction by adding more request routers and attempting to isolate failures in the future. However, more changes have to be made to prevent outages such as this one from occurring in the future. One method that will improve availability is to clean up the datacenters that host cloud environments. Numerous datacenters used by cloud providers contain large amounts of useless and redundant data that have accumulated over time as users moved from one IT paradigm to the next. Cloud service providers do not spend money to address the issue of data accumulation because they do not see any business benefits in resolving this issue. However, cloud computing would be more efficient if datacenters did not retain useless data. Present cloud computing services should be complemented with local data storage and local applications. Moreover, users of cloud services should have procedures in place in case of a disaster. The procedures should provide instructions on how to recover any lost data as well as alternative applications to use. Continuity planning can also reduce any disruptions that result from an interruption of availability over the cloud. An alternative to a disaster recovery plan is to utilize the services of multiple cloud providers. A user can have contracts with two or more cloud providers. The other cloud providers can be used as backup if the primary cloud provider encounters an availability disruption. Moreover, cloud providers should be located in multiple locations to reduce the threat of an availability disruption in a specific location.The lack of a standardized cloud model makes moving applications from one cloud provider to another difficult and complicated. Depending on the specific cloud providers, moving applications between cloud providers may be impossible. Hence, even though a user could enter into contracts with multiple cloud providers to improve the availability of cloud services, they have to be aware that this option has many disadvantages.

2) High availability: However, increasing cloud computing data storage and assuring data service reliability in terms of data correctness and availability are very important. While redundancy can be added to data for reliability, the problem becomes challenging in the "pay-as-you-use" cloud paradigm, where users always want to efficiently resolve corruption detection and data repair. Prior distributed storage systems based on erasure codes or network coding techniques have either high decoding computational cost for data users or too great a burden for data owners in terms of data repair and being online. The secure cloud storage service presented in this paper addresses the reliability issue with near-optimal overall performance.

CONCLUSION

The information rupture at Target, bringing about the loss of individual and MasterCard data of up to 110 million people, was one of an arrangement of startling robberies that occurred amid the ordinary repairing and stockpiling of Information. "Distributed computing presents noteworthy new roads of assault," said the CSA report creators. Unquestionably the security of hypervisor operation and virtual machine operations is still to be demonstrated.

REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2]. S. Goyal, "Public vs Private vs Hybrid vs Community-Cloud Computing: A critical review," International Journal of Computer Network & Information Security, vol. 6, issue 3, pp. 20, 2014.

[3]. R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: A systematic literature review," Future Information Technology, pp. 285-295: Springer, 2014.

[4]. J. Hwang, "Improving and repurposing data center resource usage with virtualization," PhD Thesis, George Washington University, 2014.

[5]. J. Mun, Y. Jung, J. Kim, Y. Lee, K. Park, and D. Won, "Security controls based on K-ISMS in cloud computing service," Advances in Computer Science and its Applications, pp. 391-404: Springer, 2014.

[6]. S. M. Moorthy, and M. R. Masillamani, "Intrusion detection in cloud computing implementation of (SAAS & IAAS) using grid environment," Proceedings of the International Conference on Internet Computing and Information Communications, Springer India, pp. 53-64, 2014.

[7]. G. Laatikainen, O. Mazhelis, and P. Tyrväinen, "Role of acquisition intervals in private and public cloud storage costs," Decision Support Systems, vol. 57, pp. 320-330, 2014.

[8]. P. Ayers, "Securing and controlling data in the cloud," Computer Fraud.