EPiC Series in Computing

Volume 58, 2019, Pages 356–367

Proceedings of 34th International Conference on Computers and Their Applications

Secured Cloud for Enterprise Computing

Salman M. Faizi[1] and Shawon S. M. Rahman[2]

[1] Ph.D. Candidate, Information Technology, Capella University, 225 South 6th St, Minneapolis, MN 55402, USA. salfaizi@outlook.com

[2]Associate Professor, Department of Computer Science and Engineering, University of Hawaii-Hilo, Hilo, HI 96720 sRahman@Hawaii.edu
and
Part-time Faculty, Capella University, 225 South 6th St, Minneapolis, MN 55402, USA

Abstract

Cloud computing is a transformative technology that organizations cannot ignore. Before adopting cloud computing, an organization must determine its needs and risks and encapsulate them into cloud service provider selection criteria. Due to being sharable and the openly accessible nature of cloud computing, the criteria must highlight data security and protection against malware. Only after developing the criteria, should the organizations select a cloud service provider. Choosing the right provider is essential.

Keywords: Cloud Computing, Cloud Security, Cloud Service Provider Selection, Data Encryption, Data Security, Malware Detection, Trusted Cloud

1 Introduction

Cloud computing (CC) is an attractive option for organizations allowing them to offer innovative IT services anytime, anywhere while saving money. However, CC's attraction can diminish rather quickly unless organizations address many of its inherent problems [3, 4]. These problems include the security of customer data, malicious attacks on applications, mismatched expectations of operations, adoption of strategies, etc. [6]. CC is defined as an IT service model for delivering computing services to customers on demand over a network [3]; it is cost-effective and scalable in providing IT services [7]. When realized in a trusted cloud, CC will uphold user privacy, data security, and protect against attacks [8]. Similar to other trusted systems, the trusted cloud has the same goal—improve business and remain competitive by exploiting a new technology; however, any new technology takes time to build a reputation for good performance, security, and user trust [4]. Here we use trusted cloud computing as defined by Manuel [9] who describes cloud computing trust as having four essential parameters: availability, reliability, turnaround efficiency, and data integrity.

Additionally, since CC is outsourced to a Cloud Service Provider (CSP), it provides benefits in cost. It relieves the organizations from expenses for equipment and employees that would have been required to provide the equivalent services [3]. The characteristics of CC are available anywhere, sharing of servers, pooling of computing resources and sharing with multiple users, ability to quickly grow or shrink, pay-per-use services, and on-demand self-service; if not adequately addressed these characteristics will risk organizations losing their autonomy [10]. Selecting the right CSP is essential because customers rely on a CSP to achieve operational efficiency and autonomy [11]. Therefore, organizations should use a trusted cloud and select the right CSP because the trusted cloud is the only way to address data security, prevent application attacks, and only the right CSP will help them meet their operational and strategic needs.

2 Security Threats

As digital society grows in sophistication and footprint, cybercrime grows with it. Huang, et al. [12] report alarming statistics on cybercrime. In 2015, the cost of cybercrime was estimated to be $3 trillion, and this number is expected to grow to $6 trillion by the year 2021. Cybercrime affects about a third of companies, and 61% of CEOs reported concerns with their companies' cybersecurity readiness. Cybercrime has evolved from an iniquitous hobby in the 1970s to a booming business where cybercriminals use cybercrime to make a living. As cloud computing increases its offering of "as-a-service" delivery model, the cybercriminals match it with a nefarious "as-a-service" model of cyberattacks allowing an attacker, with no knowledge or expertise in cybercrime, to purchase their services. The business-like nature of cybercrime attracts more able hackers to make money in the cybercrime business with a goal of maximizing profit and minimizing arrest. As the efforts of law enforcement to curtail cybercrime increase, the cybercriminals only get better at evading arrest and increasing sophistication [13]. Several recent high-profile cybersecurity incidents highlight the sophistication and reach of cybercriminals.

Cloud computing is not beyond the reach of cybercriminals – attacks from cybercriminals buffet a growth in cloud adoption. McAfee [14] reported that from 2017 to 2018, the use of cloud computing, whether public, private, or a combination of both, among surveyed organizations went up from 93% to 97%; however, during the same timeframe, the organizations reporting with cloud-first strategy went from 82% to 65%. The decrease is in part due to concerns over security. Of the surveyed organizations, 25% reported data theft from the public cloud, and 20% experienced advanced attacks on their public cloud infrastructure. McAfee [14] found popular services for each of the three cloud service delivery models. In software-as-a-service (SaaS), Salesforce, Box, and Office 365 were popular options; for Infrastructure-as-a-Service (IaaS), Amazon Web Services (AWS) and Microsoft Azure were popular; and for Platform-as-a-Service (PaaS), popular examples include Google App Engine, Red Hat OpenShift, Force.com, AWS PaaS, and Azure PaaS. Interestingly, organizations surveyed reported that from 2015 to 2017 the use of private cloud went down from 51% to 23% respectively. This fact points to the popularity of the public cloud, and it also highlights the need for a trusted cloud where organizations can place their information data without worrying about its theft or loss.

3 Trusted Cloud

If the organizations cannot trust their confidential data to cloud computing without fear of theft, they will not adopt it. It is for this reason that enterprise readiness for cloud computing requires a trusted cloud [15, 16] that ensures data are kept secure. Customers lose trust in CC due to missing transparency, lack of control over data, and security concerns [4]. Loss of data due to lacking security of confidential

data result in financial loss and reputational damage. Keeping confidential data secure can also be a requirement by authorities. In the US, for example, various statutory acts and governmental regulations mandate safekeeping of medical, financial, and personal data [16, 17]. Examples of such acts and regulations include HIPAA and SEC safeguard rules. A trusted cloud provides a secure setting for organizations to transfer, store, process, and retrieve confidential data without reasonable concern for theft of data [16]. Adequate usage of the cloud may be achieved by ensuring that the cloud can counter deterioration in performance, reliability, and security. To achieve a trusted cloud that will keep confidential data secure, we must first understand and address vulnerabilities present in cloud computing in the areas of security.

There are four broad categories of security threats in cloud computing: virtualization level, application level, network level, and data level security threats. These attacks can cause serious damage, and the cloud computing user must take steps to safeguard against them. Some attacks are on resources that are under the control of the cloud provider, and the user has no access to them. The cloud computing user must prevent such attacks through selecting the right cloud provider with acceptable service level agreements. Next, each category of security threats in cloud computing is described.

3.1 Virtualization Level Attacks

These attacks target virtual machines (VMs) and hypervisors. As shown in Figure 1, a single physical server hosts multiple virtual machines through hypervisors; virtualization level attacks exploit this design [5]. The executable code of the VM is transferred as an image or a virtual hard drive to a newly provisioned VM. An attacker can modify the executable code of a VM before it is copied to another VM, and the attacker can insert and replicate viruses across all the VMs who get the modified executable code.

Cross VM side channel attack can steal sensitive data, such as encryption key, from another VM. The cross-channel attack exploits the communication between VMs through the physical hardware of the server. The attacker is able to extract resource usage details, encryption keys, even user credentials [16]. One of the benefits offered by VMs is the ability to migrate them to different servers or rollback a VM to a different configuration. VM migration and rollback attacks occur during migration of a VM from one physical server to another, can access the execution state log of the VM to get access to it. The log files contain sensitive information about the use of the VM allowing a hacker to gain control of the targeted VM.VM scheduler-based attacks get a VM to execute for free by modifying scheduling characteristics. The physical servers that host the VMs and hypervisors are under direct control of the cloud service provider. The cloud customer does not get to control the physical server which is the source of many VM and hypervisor-based attacks.

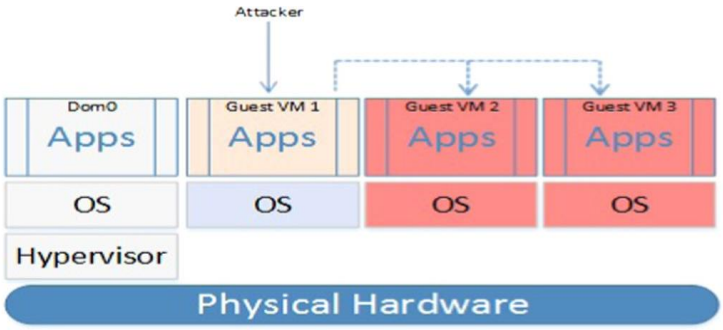

Figure 1: VM-to-VM or Guest-to-guest attacks [5]

3.2 Application Level Attacks

Applications are prone to attacks due to vulnerabilities in them leading to unique challenges and threats. In 2009, a study found that attacks on web applications made up more than 60% of the total attacks on the internet [18]. However, things have only gotten worse in this area. Cisco Systems [19] reported that in 2017, 64% of all denial of service attacks targeted applications. The attackers specifically target the applications because the network layer has increased protection leaving less room for exploitation. The increased attacks on the application need the increased protection of the application by removing security flaws in them.

The top ten security attacks experienced by applications include Injection, broken authentication, sensitive data exposure, XML external entities (XXE), broken access control, security misconfiguration, cross-site scripting (XSS), insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring [20]. No stage of software development is immune from exposure to security flaws. The OWASP Foundation [18] states that security flaws can be injected into the software during any stage of the software development lifecycle. Security flaws can result during security requirements definition, conceptual design creation, following poor coding practices, improperly deploying software, or introducing a security flaw during maintenance or updating. Thus, it follows that policies, processes, and procedures must cover all phases of software development for including security.

These application attacks target the weakness in applications; some specific application attacks are described next. A malware injection and steganography attack allows an attacker to insert malicious code in an application through the insecure application interface [16]. The security monitoring services ignore these changes since they occur under the control of an application. Some examples of malware are Viruses, Worms, Trojan Horses, Rootkits, Ransomware, Keyloggers, and Grayware [21]. An attacker can trace the activities of an application that uses shared architecture to learn the user's activities and steal the account.

Web services communicate via protocols. The Simple Object Access Protocol (SOAP) is used between the client and the server to exchange XML-based messages, which are transmitted over the network using http or https protocols. Even when protected via a digital signature, the content of a SOAP message can be modified without invalidating the signature [22]. XML has many security vulnerabilities leading to Denial of Service attacks or XML injections attacks.

On a system running an application based on shared architectures, an attacker can trace the execution path of a user's application. The attacker can detect the user's account credentials and steal the account [23]. The cache of a CPU leaks significant information according to research. The microarchitectural design of the CPU cache minimizes the memory access time of data that were recently used, and the cache is shared across cores of modern multi-core processors; hackers have used cache attacks to steal cryptographic information or to bypass the kernel address space layout randomization (ASLR) [24]. ASLR is a memory protection method designed to prevent an attacker from exploiting memory. In summary, several application-based attacks detract trust from cloud computing.

3.3 Network Level Attacks

This type of attack can cause delays or make it inaccessible. Botnets have infiltrated networks to cause harm to the cloud computing platform. For example, hackers have been able to run a botnet such as Zeus in public clouds such as Amazon EC2 or Google AppEngine to operate as a command and control servers to steal passwords. The Zeus botnet was used to steal passwords, and other botnets have performed illegal bank transactions [16]. Recently, a botnet called Loapi showcased the skills of hackers to write extensible code; similarly, the botnet Terdot amplified the importance of social media credentials [1]. Botnets get access to the cloud computing platform by breaching the network.

A man-in-the-middle attack is another sophisticated attack. During the holiday season of 2017, Web Proxy Auto-Discovery (WPAD) attack caused serious interruptions. WPAD is a protocol that lets computers discover the web proxy for use. A JavaScript file called proxy auto-config (PAC) defines web proxy, and hackers can locate the PAC script on target computers and replace it with an alternate PAC file allowing the hackers to intercept its traffic [1]. PAC files allow hackers to mount a man-in-the-middle attack. The figure below shows a sample PAC file.

```
function FindProxyForURL(url, host) {

// If the hostname matches, send direct.
     if (dnsDomainIs(host, "intranet.domain.com") ||
     shExpMatch(host, "(*.abcdomain.com|abcdomain.com)"))
     return "DIRECT";

// If the protocol or URL matches, send direct.
     if "url.substring(0, 4)=="ftp:" ||
     shExpMatch(url, http://abcdomain.com/folder/*))
     return "DIRECT";

// If the requested website is hosted within the internal network, send direct
     if (isPlainHostName(host) ||
     shExpMatch(host, "*.local") ||
     isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
     isInNet(dnsResolve(host), "172.16.0.0", "255.240.0.0") ||
     isInNet(dnsResolve(host), "192.168.0.0", "255.255.0.0") ||
     isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
     return "DIRECT";

// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
     if (isInNet(myIpAddress(), "10.10.5.0", "255.255.225.0"))
     return "PROXY 1.2.3.4:8080";

// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
     return "PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080";
}
```

Figure 2: A sample PAC file [1]

Other popular network attacks include distributed denial of service attacks, which are launched from many different servers with different IP addresses and use various methods to render a server unresponsive to valid requests. For example, the TCP protocol sets aside memory blocks while waiting for a response from the server requesting a connection for the duration of the wait timer, and too many such requests will leave the server with no memory to service valid requests. An intrusion detection system cannot easily detect DDoS attacks. Microsoft Azure [25] uses a novel approach of trapping DDoS attacks at the edge of its network and leaving the mission-critical machines deep inside the network available to service valid requests. An ARP spoofing attack lets an attacker transmit packets from an impersonated MAC address to gain access to a valid ethernet packet from a target VM.

3.4 Storage Level Attacks

This type of attack can lead to loss of data or unauthorized manipulation. A goal of cloud computing is to provide an always-available experience for the customers. This always-available design of cloud computing also leads to enhanced exposure of data for theft or manipulation. The high availability design of cloud computing means building redundancy into the system. Some cloud vendors may store three to six replicas of data. Thus, if one data storage device fails, other devices remain available, and the failed storage device is replaced with another device to maintain the expected replicas of data. These availability design mechanisms can also increase the attack surface of data. Furthermore, application programming interfaces (API) for accessing cloud data provide easy access; however, hackers can

exploit the APIs to steal or manipulate data [5]. Thus, data theft or manipulation is a concern for cloud computing.

Next, we provide some examples of data theft. An attacker can steal sensitive data or get access to private data. A data scavenging attack targets the erased data in the file system since the file system only marks the data for deletion without deleting them [16]. An attacker can recover the deleted data. A deduplication attack can reveal the content of files while data are being deduplicated to preserve storage space. Physical disks that host data are under the control of the cloud provider and the customer does not get to control low-level operations such as deletion and deduplication.

Data can be encrypted using a key to which only the data owner has access. The key may be stored in a key vault. For example, Microsoft Azure cloud provides a key vault for storing customer owned encryption keys [26]. Without the data encryption key in the key vault, the encrypted data cannot be read, and without authenticating using multiple factors, the key cannot be accessed. For even more sensitive data, a cloud customer may choose to encrypt data on the client side and storing the encrypted data in the cloud data storage service. This way the cloud vendor cannot see the data and this method can provide the cloud customer extra piece of mind.

Security Issues	**Attack vectors**	**Attack Types**	**Impacts**
Virtualization level Security Issues	• Social engineering • Storage vulnerabilities • Datacenter vulnerabilities and Network • VM vulnerabilities, etc.	• DoS and DDoS • VM Escape • Hypervisor Rootkit	• Software interruption and modification (deletion) • Programming flaws
Application level Security Issues	• Session management and broken authentication • Security misconfiguration, etc.	• SQL injection attacks • Cross Site scripting and • Other application-based attacks.	• Modification of data at rest and in transit • Confidentiality • Session hijacking
Network level Security Issues	• Firewall misconfiguration, etc.	• DNS attacks • Sniffer attacks • Issues of reused IP address • Network Sniffing, VoIP related attacks (e.g. VoIP phishing).	• Traffic flow analysis • Exposure in network
Storage level Security Issues	• Loss of privacy or secrecy of data	• Data scavenging • Data deduplication	• Data compromise • Personally identifiable information theft

Table 1: Taxonomy of Cloud Computing Attacks

The table above provides additional information on the four categories of security threats in cloud computing. For each category, attack vectors, attack types, and impacts are provided. Some of the data in the table are derived from Iqbal, et al. [5].

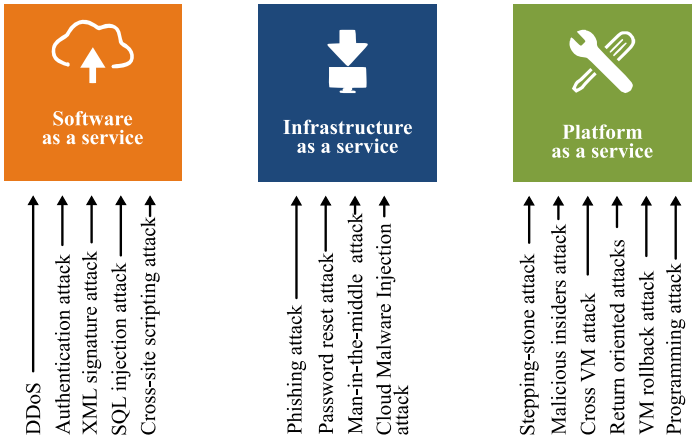

Figure 3: Cloud Computing Attacks by Service Delivery Model

Furthermore, the three cloud service delivery models (infrastructure as a service, platform as a service, and software as a service) present different security vulnerabilities. The diagram above contains attacks for each service model. The diagram below shows what additional precautions cloud computing customers must take to protect their data and to develop a trusted cloud since each delivery model of cloud computing service allows a different level of control for the customer. The strategy to build a cloud computing solution that qualifies as a trusted cloud requires customers to protect the part under their control and select a cloud computing vendor to manage the part under its control. We highlighted above the four broad categories of security threats in cloud computing: virtualization level, application level, network level, and data level security threats.

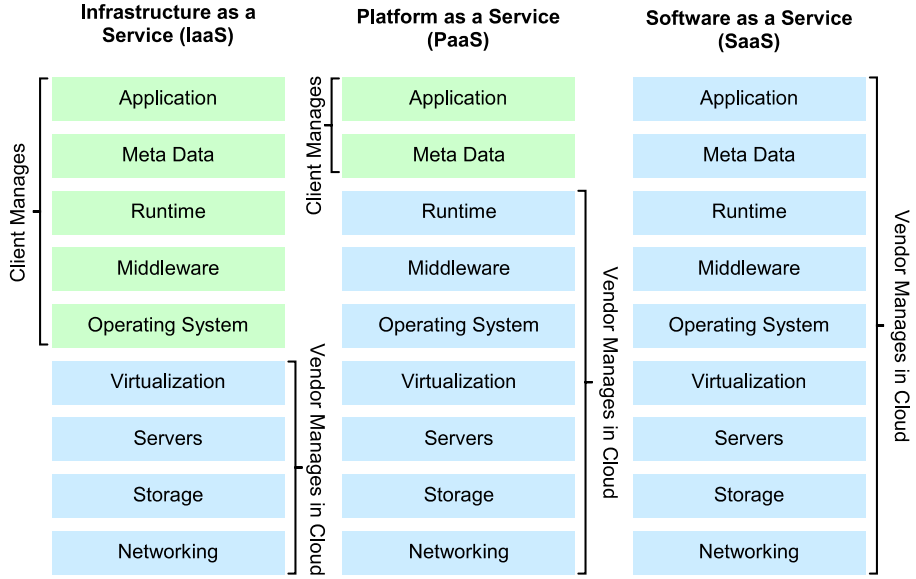

Figure 4: Cloud Service Delivery Models

It is essential that IT organizations guard against all four types; the cloud vendor can protect against some attack types with little user involvement. Therefore, the cloud customer must focus on storage and application attacks. Storage attacks are prevented using data encryption which makes data unreadable without the encryption key [4].

IT Organizations must ensure cloud security by encrypting data and by preventing application attacks from malicious software such as computer viruses. Thus, the two essential elements of cloud computing security, prevention strategies for storage attacks and application attacks, are discussed below. Data encryption is standard practice to safeguard data against storage attacks. Encryption is the computerized encoding and decoding of information, and encrypted data are decrypted with the same encryption key that was used to encrypt the data [27]. An encryption key is a sequence of numbers used to encrypt or decrypt. Unfortunately, the heavy computational workload of encryption has become a challenge [28]. Since each computer has limited computational capacity, the challenge is to allocate capacity to encryption while still having the capacity to run application software.

One technique for addressing this challenge is to offload encryption to some other processor leaving the central processor for running application software. One such processor that is capable of taking on this load is the graphical processor unit (GPU) which can be used for performing encryption [28]. A GPU today contains massive computational capacity for displaying complex graphics. Data encryption can use the same computational capacity; however, there is an associated risk that must be mitigated. A hacker could break into the graphical processor to steal the encryption key and read the encrypted data. Encryption key attacks are often left unguarded [29]. One way to address this risk is to use a technique called On-demand Bootstrapping Mechanism for Isolated cryptographic operations (OBMI) on commodity accelerators [28]. OBMI safeguards the key and has been shown to be an effective mechanism to prevent stealing of the key [28]. Hence, to guard against storage attacks, organizations considering CC must encrypt their sensitive data and insist on safeguarding their encryption key using OBMI or equivalent.

The second type of attack to protect against is Application attacks. Application, in this case, is a software program that performs one or more functions of benefit to an end user. Examples include online shopping, accounting, video editing, and word processing. Malware, a nefarious type of application, attacks other applications, and it can provide a backdoor method of stealing sensitive data [16]. Malware is a combination of the words “malicious” and “software,” and it refers to any code added, changed, or removed from a software system to intentionally cause harm or subvert the system’s intended function [2]. Malware can significantly subvert CC security by providing backdoor access to confidential data.

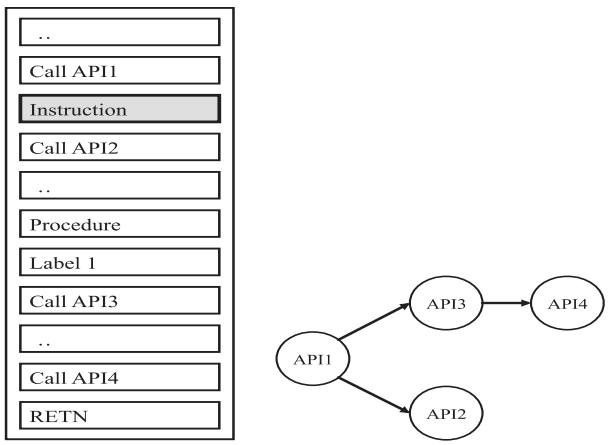

Figure 5: An example of mapping code into a call graph [2]

Traditionally, the way to deal with malware is using user-installed anti-malware software. Such software works by determining patterns for each running application, and if the pattern matches its database of malicious patterns, a malware instance is identified [2]. The diagram above shows an example of the transformation of code into call graphs.

Malware, today, is increasingly sophisticated and avoids detection by changing its patterns each time it runs [30]. The changing of patterns makes detection nearly impossible. Even though malware can change its patterns, it cannot change its behavior. A new technique can detect malware based on its behavior [2] using an algorithm called Minimal Contrast Frequent Subgraph Miner (MCFSM). IT organizations can effectively guard against applications attacks by using malware detection with anti-malware software that uses an algorithm like MCFSM.

4 Implementation Details

From our experience in cloud computing security, implementing security (which in turn enables trust) consists of assigning accountability for some aspects of security to the CSP and others to the CC consumer. Listed below are some best practices in the implementation of security in CC.

4.1 Access Management

Access management, a critical aspect of CC security, consists of the abilities to identify and authenticate users. Organizations should use multifactor authentication to lower the risk of unauthorized access that can result from compromised credentials. A hacker with access to stolen credentials must now also authenticate via an alternate means which the hacker is unlikely to have, and that reduces the risk of unauthorized access. For example, a scheme based on two-factor authentication may consist of authenticating a user via a password and via a secret code, which is only valid for a short duration of time, sent to the registered mobile phone of the user.

Additionally, organizations must assign user access rights based on the user role. A system user need not have the same access rights as a system administrator. Many CSPs provide the ability to assign role-based access control. CC has evolved to offer multiple storage services: blob storage, file storage, virtual hard disks, and content delivery. Given the differences in how each of the storage services stores data, organizations must understand and configure access policies that are tailored to each type of storage.

4.2 Data Protection

Data present three challenges: preventing unauthorized access; continuity of access to important data in the event of failure, errors, or disasters; and prevention of accidental access to deleted data. Each of the three challenges requires a specific security implementation. Next, we describe our strategies for dealing with these challenges.

First, preventing unauthorized access to data requires encryption. Organizations must ensure they configure encryption of data at rest and data in motion whether within the cloud computing network or outside of it. Organizations should only select CSPs that provide options to enable encryption for both data at rest and data in motion. For data at rest, ideally, organizations must use two keys: a data encryption key to encrypt data, and a key encryption key to encrypt the data encryption key. Using two keys makes it easier to rotate keys in case of a key compromise. The key must be stored in a secure key vault such as a hardware security module (HSM). Losing an encryption key can lead to loss of data. The key used must be of sufficient complexity such as a 256-bit key. Similarly, for data in motion, an organization should use encrypted connections such as HTTPS, SSL, TLS, and FTPS. Data, when in motion, even within the CSP's network, is susceptible to being intercepted.

Second, continuity of access to important data in the event of failure, errors, or disasters requires the CSP to keep multiple replicas of data for recovery from a failed device and periodic backup for recovery from point in time failures caused by user mistakes. Organizations must ensure that the data backup procedure of the CSP and the associated service level agreements are acceptable to meet their needs. Often, the users of the CC can configure these options that may be available at additional cost.

Third, prevention of accidental access to deleted data requires an understanding of where the data are stored and how they are replicated across the CSPs' infrastructure. CSPs keep multiple replicas of data, if a device storing one of the replicas fails, the CSPs must physically shred the device to prevent unauthorized access to the data on the failed device. Data may end up in the logging and monitoring service of the CSP. Thus, organizations must fully understand how data are moved within a CSP's network. For ultrasensitive data, one option is to encrypt and decrypt the data on the client side. This way any replication or dissemination of data within the CSP's network will be of the encrypted data.

4.3 Monitor and Defend in Real Time

The CSP can only monitor certain parts of the CC, and a CSP typically does not monitor user-created applications. The CSPs monitor their infrastructure and alert their users via a monitoring service. Organizations must act on the monitoring provided by the CSP, and they must ensure that the CSP provides an adequate level of monitoring of the infrastructure beyond their reach. Organizations must understand the level of monitoring available from the CSP, design of the monitoring service, and the meaning of different alerts they will receive from the CSP's monitoring service. For user-controlled environments such as IaaS, the organizations must build their monitoring capabilities that will monitor beyond what their CSP can. For PaaS and SaaS-based applications, the organizations must coordinate with the CSPs for a comprehensive monitoring strategy.

5 Conclusions

Cloud is an attractive option for a modern IT organization for delivering computation services to its users anywhere, anytime. For cloud computing to work for IT organizations, the risks associated with it must be mitigated. Mitigating the risks means developing comprehensive criteria encapsulating all the needs of the organization. The criteria, at a minimum, must include operational matters, strategic issues, trusted cloud, data security, and preventing malware application attacks. Once an organization develops satisfactory criteria, it must use a scientific method to compare all the cloud computing vendors available in the market to select the one just right for them. Cloud computing, when done right, will help IT organizations meet future growth, offer innovative solutions, and implement data security that is greater than or on par with what they had before adopting cloud computing.

References

[1] Akamai, "State of the Internet / Security : Carrier Insights, Spring 2018 report focuses," 2018, Available: https://www.akamai.com/es/es/multimedia/documents/case-study/spring-2018-state-of-the-internet-security-report.pdf.

[2] A. Hellal and L. Ben Romdhane, "Minimal contrast frequent pattern mining for malware detection," *Computers and Security*, vol. 62, pp. 19-32, 2016.

[3] A. Dutta, G. Peng, and A. Choudhary, "Risks in Enterprise Cloud Computing: The Perspective of it Experts," *Journal of Computer Information Systems*, vol. 53, pp. 39-48, 2013.

[4] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88-115, 2017.
[5] S. Iqbal *et al.*, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *Journal of Network and Computer Applications*, vol. 74, pp. 98-120, 2016.
[6] S. Liu, F. T. S. S. Chan, and W. Ran, "Decision making for the selection of cloud vendor: An improved approach under group decision-making with integrated weights and objective/subjective attributes," *Expert Systems with Applications*, vol. 55, pp. 37-47, 2016.
[7] M. W. S. Chun, C. Griffy-Brown, and H. Koeppel, "The new normal: Fundamental shifts for 21st century organizations and for the CIOs who lead them," *Journal of Applied Business and Economics*, vol. 16, pp. 27-50, 2014.
[8] S. Siadat, A. Rahmani, and H. Navid, "Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model," *Journal of Supercomputing*, Article vol. 73, no. 6, pp. 2682-2704, 2017.
[9] P. Manuel, "A trust model of cloud computing based on Quality of Service," (in English), *Annals of Operations Research*, vol. 233, no. 1, pp. 281-292, Oct 2015.
[10] N. Patrignani and I. Kavathatzopoulos, "Cloud Computing: the Ultimate Step Towards the Virtual Enterprise?," *ACM SIGCAS Computers and Society*, vol. 45, pp. 68-72, 2016.
[11] J. Modic, R. Trapero, A. Taha, J. Luna, M. Stopar, and N. Suri, "Novel efficient techniques for real-time cloud security assessment," *Computers and Security*, vol. 62, pp. 1-18, 2016.
[12] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Computing Surveys*, Article vol. 51, no. 4, pp. 1-36, 2018.
[13] L. Ablon and M. Libicki, "Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data," *Defense Counsel Journal*, vol. 82, pp. 143-152, 2015.
[14] McAfee, LLC,, "Navigating a cloudy sky - practical guidance and the state of cloud security," 2018, Available: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf, Accessed on: 10/31/2018.
[15] N. Khan and A. Al-Yasiri, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," *Procedia Computer Science*, vol. 94, pp. 485-490, 2016.
[16] M. A. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11-29, 2016.
[17] J. D. Dodd, "Data Security Law—State Statutory Requirements for Protecting Personal Data," *American Journal of Trial Advocacy*, vol. 38, pp. 623-629, 1999.
[18] The OWASP Foundation, "OWASP Secure Coding Practices Quick Reference Guide," 2010.
[19] Cisco Systems, "Cisco Annual Cybersecurity Report," Available: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2
[20] The OWASP Foundation, "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks," 2017, Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.
[21] S. Abraham. (2017, 10/31/2018). *List of types of malware*. Available: https://www.malwarefox.com/malware-types/#tab-con-7
[22] A. Nasridinov, Y.-S. Jeong, J.-Y. Byun, and Y.-H. Park, "A histogram-based method for efficient detection of rewriting attacks in simple object access protocol messages," *Security & Communication Networks*, Article vol. 9, no. 6, pp. 492-499, 04// 2016.
[23] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-tenant side-channel attacks in PaaS clouds," presented at the Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, Arizona, USA, 2014.

[24] D. Gruss, C. Maurice, K. Wagner, and S. Mangard, "Flush+ Flush: A fast and stealthy cache attack," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2016, pp. 279-299: Springer.

[25] Microsoft Azure. (2018, 10/6/2018). *Azure DDoS Protection*. Available: https://azure.microsoft.com/en-us/services/ddos-protection/

[26] D. Plastina. (2015). *Azure Key Vault—Making the Cloud Safer*. Available: http://blogs.technet.com/b/kv/archive/2015/01/08/azure-key-vault-making-the-cloud-safer.aspx.

[27] H. L. Xu and Y. Lu, "Hierarchical Certificate-Based Encryption: Definition and an Efficient Construction," *Applied Mechanics and Materials*, vol. 513-517, pp. 1971-1974, 2014.

[28] Y. Kim *et al.*, "On-demand bootstrapping mechanism for isolated cryptographic operations on commodity accelerators," *Computers and Security*, vol. 62, pp. 33-48, 2016.

[29] L. Jiguo, Y. Hong, and Z. Yichen, "Cryptanalysis and improvement for certificateless aggregate signature," *Fundamenta Informaticae*, Article vol. 157, no. 1/2, pp. 111-123, 2018.

[30] L. Gheorghe *et al.*, "Smart malware detection on Android," *International Journal of Applied Engineering Research*, vol. 9, pp. 5968-5974, 2014.