1. Introduction to cloud computing and security issues

Joe Kong, Xiaoxi Fan and K.P. Chow

I. INTRODUCTION

The evolution of the Internet and the widespread adoption of virtualization technology have brought cloud computing to the forefront of innovation in the early 21st century, a circumstance in which computation has become per-use service-based. Cloud users can now process data and utilize storage platforms through high bandwidth networks at low cost and high efficiency. At its most basic and general level, cloud computing technology refers to the delivery of information technology resources as a service to multiple customers through the Internet: a process whereby software, shared resources and information are held on remote servers designed and established by the respective network or infrastructure operator. Consequently, the handling of this data is under the control of service providers, and this is known as 'the cloud'. In other words, cloud computing enables information to be accessible anywhere to anyone with an Internet connection.

The centralization of computing infrastructure and the change in the global computing landscape have allowed individual users and business enterprises to perform their activities round-the-clock with the advantage

---


2 Virtualization is a technology that combines computing resources to present one or many operating environments using methodologies like hardware and software partitioning, partial or complete machine simulation, and others. Susanta Nanda Tzi-cker Chiueh and Stony Brook, ‘A Survey on Virtualization Technologies’ (RPE Report, 2005) 1–42.

of device and location independence. Many of us who are using webmail, social networking services, web conferencing and online music services may already be in the cloud. At the same time, the use of cloud computing in the business community has begun to expand because cloud computing supports scalable and virtualized computer-related resources using the Internet. Such a model does not require its users to have the necessary expertise in or control over the cloud infrastructure, and this technology can be implemented using different deployment approaches or architectures. Businesses utilizing cloud services can save huge costs such as being able to use central processing unit cycles without having to buy their own mainframe computers, storing data and documents without having their own storage networks, and using expensive software and being able to provide it to their clients without having to buy the software themselves. Functioning through a 3G/4G network, the portability of computation has come to a stage where cloud users can share their data resources freely at any time, at any location, from any device or with any person. The prominent cloud service providers (CSPs) offering a variety of services include VMware, Sun Microsystems, Rackspace US, IBM, Amazon, Google, BMC, Microsoft, Ubuntu and Yahoo. Most of them rely on the use of virtual machines (VMs), which are software implementations of computers used to execute programmes.

As we can imagine, the benefits of cloud computing are enormous. Through this model, individuals, businesses and governments can rent services and store data at a much cheaper price than buying new equipment and software themselves. Cloud computing can also reduce the waste of information systems resources, increase the efficiency of data centres, save significant energy and lower operating costs. It is also a further developed technical model of the previously applied point-to-point business outsourcing processes.


On account of its significance, cloud technology was recognized as one of the top ten information technologies in 2012 and the personal cloud as one of the top ten strategic technologies in 2013. It was predicted by Gartner that by 2016, more than 50 percent of Fortune/Global 1000 companies will have stored customer-sensitive data in a public cloud, which means that the cloud revolution will have significant implications not only for technology development but also for new business model design and the economy at large. It is estimated that by 2014, the public cloud services market in the European Union (EU) alone will reach €11 billion in revenue, amounting for 3.6 percent of the total IT market. Globally, the total revenue from public IT cloud services exceeded €17 billion (US$21.5 billion) in 2010 and the forecast is that it will reach €58 billion (US$72.9 billion) in 2015. In 2011, Neelie Kroes, Vice-President of the European Commission for Digital Agenda, urged Europe to move from being ‘cloud-friendly’ to ‘cloud-active’. In 2012, the European Commission announced the adoption of the Cloud Computing Strategy for the European Union and the establishment of a European Cloud Partnership that has included private industry and public sector users.

---

Yet, the vast potential of cloud computing also brings with it unprecedented challenges. Among various concerns, the most pressing ones are personal data protection and information security. OWASP (Open Web Application Security Project), a commonly referenced worldwide organization focused on improving the security of application software, named personal data protection as one of the top ten issues for the cloud computing environment. The majority of the survey results have confirmed that the information security issue is the critical hurdle for users when considering switching to the cloud computing environment. It is also known that the US government does not store classified data in the public cloud for national security reasons. The above concern is certainly understandable since, by putting our personal data and information on remote servers, we may easily lose control over our data. Moreover, in most cases, we do not know how, where, by whom our personal data is being processed.

To understand and tackle security concerns in the cloud, we will start off in Section II by explaining the meaning of cloud computing and its various deployment models which entail different personal data concerns. Then in Section III we will explore how new security issues arise in the cloud computing environment. Although some may argue that the nature of cloud computing does not differ much from current Internet and web technology, a closer look at the nature of the non-standardization of different models, resource sharing and outsourcing will reveal different

---


15 Kroes (n 11).


sets of challenges to security. Critical and unique issues highlighted in this chapter with respect to the cloud environment are the sharing of roles and responsibilities between cloud service providers and data users, with illustrations of the problems of security. Finally, in Section IV, we offer solutions that can enhance security in the cloud environment. Although the industry model is still in its infancy, it may be an answer in view of the gap between legal regulation and innovation.

In this chapter, users of cloud services in a non-private capacity (whether corporate or public administration, business enterprises, or individuals) are referred to as ‘users’ or ‘customers’, whereas individuals using such services in a private capacity are referred to as ‘consumers’.18

II. WHAT IS CLOUD COMPUTING?

A. Definition and Features

As mentioned briefly at the start of this chapter, cloud computing is a service whereby information, software, and shared resources are provided as a utility to electronic devices such as computers over the Internet. Although there is no single definition of cloud computing, the formulation by the United States National Institute of Standards and Technology (NIST) has gained wide recognition and has provided an authoritative guideline.19 It defines cloud computing as ‘a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction’.20 Embedded in this definition are five essential characteristics of cloud computing: (1) on-demand self-service; (2) broad network access; (3) resource pooling and location independence; (4) rapid elasticity; and (5) measured services.21


19 European Commission (n 6).


21 Ibid 2.
First, through on-demand self-service features, end-users are empowered to directly control and manage IT resource provisioning, meaning that they have unilateral access to different cloud services whenever required. Second, for most cloud environments, IT resources can be managed and controlled through broad network access or a web browser, regardless of the physical location of one’s devices (for example, laptops, smartphones or personal computers). Hence, the service is location independent and enables us to work ‘through the cloud’. Third, due to the software running on the servers that provide cloud resources, it enables resource pooling and location independence, which is one of the most important aspects of the nature of cloud computing, by enabling the effective use of resource sharing between various users and consumers around the world in different data centres. Resource pooling is also known as multi-tenancy in the cloud as a large number of users and consumers can share costs and resources on single systems, which makes cloud systems more efficient and cost-effective. Fourth, as IT resources are expected to be shared and provisioned when needed in real time, availability of resources appears to be virtually ‘unlimited’. In fact, the system has been made to be more elastic, scalable, and customized to meet needs and demands. In the cloud environment, choices and options for users and consumers can be built into the software platform, whereas the cloud service providers (suppliers) can profit from the economies of scale. Finally, any piece of IT equipment, storage, or computation power can be converted into a measurable charging scheme. Cloud service providers then have controls over both the storage and infrastructure, or either one, depending on the delivery model and the service level agreement between the users and the consumers. The latter two groups will have to pay for the services based on the agreed service charge.

B. Service Models

Cloud computing is not entirely new to the market and can be viewed as a collective repackaging of IT services. An analogy can be drawn between cloud computing and serviced apartments in real estate. When one owns a house, one can modify and configure anything within that house, but the house owner also has to replace or to fix any malfunctioning facilities within the house. Whereas for serviced apartments, one can just focus on managing one’s living space and enjoying the services.

---

22 Sluijs and others (n 13) 14.
23 Ibid.
while all other activities such as maintaining the building and the services, such as electricity and plumbing, within the house will be handled by the service provider. The tenant’s requirements are stated in their service level agreement with the landlord.

Likewise, in the cloud environment, the services to be provided by the cloud service providers should be defined (in a service catalogue) and available for users to choose from. In other words, a cloud service is like a tenancy arrangement for computing facilities. A landlord with a large house can establish a flexible multi-tenancy arrangement with more than one tenant for an undetermined timeframe. Anyone can join as a tenant to use the computing facilities, or leave the cloud architecture when they need to, but the choice of service is pre-defined in the contract. In other words, no matter which type of service model (infrastructure, platform or software) is used, the clients (users or customers) rely on the cloud service provider to manage and maintain the shared servers, data storage and systems.

In the first model, that of Infrastructure-as-a-Service (IaaS), the cloud service providers offer basic computing infrastructure such as processing power and/or storage (for example, virtual remote servers, CPU power, network bandwidth and storage capacity) to customers and consumers who are responsible for installing their own operating systems and applications. These providers are often specialized market players that can rely on a physical, complex infrastructure that spans several geographic areas.24 However, security and privacy provisions beyond the basic infrastructure have to be managed by the users. Examples are Rackspace and Amazon EC2 and S3.

In the second model, that of a Platform-as-a-Service (PaaS), the cloud service providers provide a platform and tools (for example, operating system, database management, security and workflow management, and web servers) to customers and consumers so that they can construct, install and develop their own applications. These services are targeted mainly at market players that use a PaaS to develop and host proprietary application-based solutions to meet in-house requirements or to provide services to third parties.25 Security and privacy provisions are split between the cloud providers and the cloud users. Examples are Google’s App Engine and Microsoft’s Windows Azure.

25 Ibid.
In contrast to the above models, there is a third model, that of Software-as-a-Service (SaaS). In this model, in addition to providing basic computing infrastructure and platforms, the cloud service providers will also provide application software. In other words, various application services are delivered and made available to end-users. Well-known examples are Facebook, Google Maps and YouTube. In the cases of web hosting and email management, a company can set up its own web server and email server by purchasing, installing and configuring the servers. With the SaaS model, the company management team can also decide not to own the server but to simply pay for the already installed and configured server together with software. The IT team just needs to load the web server content or email addresses. Consequently, these services often replace conventional applications being installed on the local systems of the users, resulting inevitably in the outsourcing of the storage and processing of data to cloud service providers. Security and privacy provisions are carried out mainly by the cloud service provider. Users do not have control over the cloud infrastructure or applications, except for some administrative or preferential settings.

The above three service models are not mutually exclusive. Instead, they often run as an integrated or multi-layered service. For instance, a cloud service may involve layers of different providers. In the case of Dropbox, data users consider it to be a SaaS, while Dropbox itself uses Amazon’s IaaS infrastructure.

C. Deployment Models

Besides service models, there are also four major deployment models for cloud computing environments – public, private, community and hybrid clouds – in which a deployment model refers to the scheme of resource sharing. With respect to security and privacy for different cloud service deployment models, the level of protection would depend on the effectiveness of the relevant policies, the robustness of the security and privacy controls, and the extent of the transparency of the performance and management details of the cloud environment. Besides the above, the choice of service model is also an important indicator of the scope of the control that a cloud user has over the cloud environment.

---

26 Ibid.

In public clouds, resources are provisioned dynamically for public users and accessed through the Internet from a third-party provider in a self-service manner. In contrast, private clouds are used exclusively by a single organization. They can be managed by a third party or used as an internal resource, and can be hosted off-site or on the company’s premises. Likewise, in a community cloud, organizations or companies within a specific community share infrastructure that can be managed by either a third party or the community itself, and can be hosted off-site or within the community’s premises. Lastly, a hybrid cloud is a combination of two or more clouds where the individual cloud entities have maintained their uniqueness even though they are bound into one cloud.

Among the four deployment models, the private cloud gives the consumers the highest degree of control while the public cloud gives the lowest. In between is the hybrid cloud, constituting a combination of different deployment models. Coupled with the various service models, the provision of cloud services can involve complicated legal issues depending on the flow of personal data through the chain of cloud services, the roles and responsibilities of the cloud service providers and their sub-providers, and the location of the cloud service providers. For instance, public clouds are commonly located in different jurisdictions, entailing issues of trans-border data transfer which will be discussed further in Chapter 5 and Chapter 6.

III. SECURITY CHALLENGES IN THE CLOUD ENVIRONMENT

Regardless of which service model or deployment model of cloud computing is involved, security remains a core concern.

A. General Security Concerns

In the old days, if the computer of one’s neighbour was being hacked, one might dismiss it by saying ‘It’s not my business’, but in the present era of shared infrastructure in the cloud, everyone is at risk. Even though cloud computing has been deployed and used in production environments since the 1990s, security has continued to be a pressing concern. In 2010, a survey conducted by Harris Interactive for Novell revealed that
90 percent of more than 200 IT leaders at large enterprise organizations were concerned about cloud security and 50 percent of them viewed security concerns as the primary barrier to adopting the cloud. In 2011, a survey conducted by International Data Corporation (IDC) showed that 47 percent of 500 IT executives were concerned about the threat to security posed by cloud computing. Cisco’s CloudWatch 2011 report for the UK revealed that 76 percent of 250 IT decision makers in large UK companies cited security and privacy as top barriers to adopting the cloud.

This general fear and concern is not without grounds. The Cloud Security Alliance in 2013 identified nine major threats to cloud computing. The first threat is related to data breaches, which refers to the intentional or unintentional release of secure information to an untrusted environment, involving financial information, personally identifiable information, personal health information, and so on. It is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. For instance, a malicious hacker behind a virtual machine (VM) could use side-channel timing information to extract private cryptographic keys being used by other VMs on the same server. The second threat involves data loss, including not only the deletion of data by malicious hackers but also by careless CSPs or natural or human-induced disasters. The third threat to cloud computing is account or service traffic hijacking. For instance, if attackers gain access to another’s credentials, they can eavesdrop on another’s activities and transactions, and then manipulate data, return falsified information and redirect another’s clients to illegal
sites. The fourth threat is the problem of insecure APIs\textsuperscript{33} which will impact the security of the implementation of system management, provisioning, orchestration and monitoring of cloud services. The fifth threat is the denial of service (DoS) when an attacker fails to knock out the cloud service entirely but manages to use up the VM’s processing time, rendering the applications unable to provide their service. The sixth threat involves malicious insiders gaining direct access or making modifications to the systems and application data. The seventh threat concerns abuse of the cloud by outsiders. For example, a hacker can make use of cloud servers to launch a DDoS attack\textsuperscript{34} or share pirated software. The eighth threat is concerned with inadequate due diligence checks carried out when an organization moves its IT operations to the cloud without having adequate resources, or is not sufficiently familiar with cloud technology, and therefore does not have adequate or proper security measures for protecting its data. Finally, there is the problem of technology vulnerabilities when cloud service providers use software that is not designed to offer strong isolation properties in a multi-tenant architecture.

1. Challenges inherent in the cloud infrastructure

One needs to bear in mind that transitioning to cloud computing involves a transfer to the cloud provider of the responsibility and control of data and systems that were previously under the organization’s direct control. The major tradeoff is that one shifts risk and loses control to gain flexibility, availability and to save costs in shared, remote resources. Yet, this increases the potential threat from hackers, cybercriminals and their malware.

As mentioned earlier in Section II.B, depending on the service model used, cloud infrastructure security is a responsibility shared between the cloud service providers (CSPs) and the users. The users are generally responsible for host based security while the CSPs are responsible for

\textsuperscript{33} Application Programming Interface (API) is a language and message format used by an application programme to communicate with the operating system or some other control programme such as a database management system or communications protocol. See ‘Definition of: API’ (PC Magazine Encyclopedia), www.pcmag.com/encyclopedia/term/37856/api, accessed 4 August 2014.

\textsuperscript{34} Distributed Denial of Service (DDoS) attack is the most advanced form of DoS attack which uses many computers to launch a coordinated DoS attack against one or more targets. See Christos Douligeris and Aikaterini Mitrokotsa, ‘DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art’ (2004) 44(5) Computer Networks 643, 645.
network based security. This split of responsibilities has another significant impact on IaaS because the CSPs supply basic resources such as machines, disks and networks, while the users are responsible for the operating system, the software environment necessary to run their applications, and the data placed into the cloud computing environment. In contrast, for a SaaS or a PaaS arrangement, the infrastructure, software and data are the primary responsibility of the CSP as the user has little control over any of these features.

The cloud is composed of four deployment models (public, private, community and hybrid) and three delivery models (IaaS, SaaS and PaaS). For a system with multiple components, security depends not only on the correct implementation of components, but also on the interactions among different components. Complex interactions among components would increase vulnerability. In the cloud environment, logical separation managed by software is used rather than a physical separation of resources. An attacker could disguise itself as a legitimate user to obtain access to the cloud service, exploit vulnerabilities from within the cloud environment and then compromise the separation mechanisms to gain unauthorized access to other tenants of the cloud server. Exposing the remote administrative interfaces of cloud computing to a user on the Internet would increase the risks of intrusion compared to the relatively secure direct connections needed for system administration in a traditional data center. In the cloud environment, some system administration functions may be supported by the CSP. The latter may perform the functions with remote administrative access. Both these activities introduce additional security risks. Hence, great damage may be caused by a malicious insider in the cloud computing environment. In particular, public cloud computing environments, most of which run on either SaaS or PaaS systems, are extremely complex because of the potential risks of trust or data breaches being involved. Sharing an infrastructure with unknown outside parties can be a major drawback for some applications, and strong security mechanisms should be used for logical separation.

In other words, the cloud environment promotes the integration of many networked computers while at the same time concealing the structure behind it. Users’ access to security audit trails in the cloud can be difficult or even impossible. This shortcoming has provided camouflage for perpetrators of malicious activity to pose as legitimate customers, making it more difficult for security practitioners to track down the perpetrator’s activities through permissible means. If data content cannot be monitored, such online storage and the anonymity of users’ identities could impose an arduous task on security practitioners when
they try to uncover or detect any unlawful activities that are associated with virtual computers in the cloud.

2. New relations between providers and users
In the cloud environment, where security issues are concerned, the emphasis is typically placed on cloud service providers while the role of users and consumers is often overlooked. For instance, web browsers are mostly used by the client-side to access cloud computing services. There may be other lightweight applications running simultaneously on the client’s desktop or mobile devices used to access the cloud services. It is not surprising that the various plug-ins and extensions for web browsers are ill-famed for their security problems since those add-ons do not provide automatic updates and thus increase the persistence of vulnerabilities. Ensuring secure access from mobile devices such as smartphones or tablets is made even more difficult by the preloaded operating systems which might become outweighed by malware over time and collapse. Besides that, their small size and portability can result in the loss of physical control while the limited built-in processing power plus the weak security mechanisms are usually inadequate and can be easily circumvented by attackers. The growing availability of mobile networks and the use of social media, personal webmail and other public cloud storage systems on mobile devices are a concern, since these software and services have been increasingly used to serve as paths for social engineering attacks and have a negative impact on the security of the underlying cloud service platform. Moreover, cloud applications are often delivered to users through custom-built native apps instead of a web browser. There is always a chance of having a backdoor Trojan keystroke logger, or other type of malware, embedded in the apps running on a mobile device.

B. Implications for IT Management
From the above perspective, cloud computing represents a significant paradigm shift away from the conventional IT security management of an organizational data centre to a de-perimeterized infrastructure that is open to use by a potential adversary. The decisions about transitioning organizational data, applications and other resources to a cloud computing environment require an organization to take a risk-based approach to analysing available security and privacy options. The information technology governance practices of the organization that pertain to the security policies, procedures, implementation, testing, use and monitoring of deployed or engaged services should be extended to include the use of
the cloud computing environment. When shifting risk from locally managed servers and services to the cloud, one should not forget the key areas of security concern, that is, confidentiality (the data should not be exposed, exploited or leaked), integrity (the data should be correct, attestable and not corrupted) and availability (access to the data is not disabled and service is not denied).

Based on the above-mentioned threats, the Cloud Security Alliance recommends a defensive, in-depth strategy that includes computer, storage, network, application and user security enforcement and monitoring.35

IV. SOLUTIONS TO SECURITY AND PRIVACY THREATS

A. General Solutions

Indisputably, as we have explained earlier, cost reduction and efficiency enhancement are the primary motivation for computer users needing major computer processing power to move towards a cloud environment. At the same time, security and privacy have become the primary interest and concern of CSPs.

To provide a ‘solution’ to the challenge to privacy inherent in cloud computing, configuration control, vulnerability testing, security audits and patching of platform components, greater consistency and system platform hardening should be offered by the CSP.36 In addition, better resilience and disaster recovery strategies need to be built into the cloud computing environment to cope with sudden bursts of service demands and distributed denial of service attacks. Furthermore, the provision of better backup and restore procedures will enable cloud services to provide a more reliable off-site repository for an organization’s data.37

It is essential for cloud users to oversee and manage how the CSPs maintain the security of the computing environment and ensure data

35 Ted Samson (n 32).
confidentiality. The default offering of CSPs generally does not reflect a specific security and privacy need. To determine a suitable service from a risk perspective requires a full understanding of the operation of the users’ business or organization, and the users’ concerns about potential threats to it. The selected cloud computing solution should be configured, deployed and managed to meet the identified security and privacy requirements.

B. Service Level Agreements

Other than simply implementing the default offering of a CSP, a negotiated service agreement can document the assurance of the CSP that it will accomplish the customer’s and consumer’s requirements to protect critical data and applications on the cloud.

Service Level Agreements (SLAs) refer to binding agreements between a service provider and its customer or consumer that have now become an important part of the cloud service delivery model. These agreements specify the conditions under which a service is to be delivered. Traditional SLAs did not cover security aspects. In 2011, Bernsmed outlined how to have a cloud SLA cover security aspects. It allows the easier selection of cloud services from different CSPs with defined security levels. In their suggested SLA lifecycle, the CSP should first publish its security services. When a potential user plans to use a cloud service, they will then negotiate a specific SLA with the CSP about the security requirements and the security services offered by the CSP. If both parties agree on the SLA, the CSP and the user will commit to the SLA and the services will be provisioned by the CSP. Following this, the user can monitor the service to ensure that the negotiated SLA is being implemented by the CSP. If the user wants to change the requirements or detects any violations of the SLA, it may result in renegotiation of the SLA. After the services are provided, the SLA will be terminated and all resources will be freed.


39 Karin Bernsmed, Martin Gilje Jaatun, Per Hakon Meland and Astrid Undheim (n 38).
C. Data Encryption

Cloud computing has additional privacy issues as it is operating as a co-tenant platform. It is important that new security design principles for privacy should be considered. For instance, a group of cloud servers might run different types of applications simultaneously for 1,000 users, and one of those applications might have no purpose other than spying on the other 999, which the CSP may be unaware of. To protect the user, data should be encrypted, and that data would only be decrypted when it is actually being processed, and the results after computations would be re-encrypted again. In addition, a new design for inside-out security should be deployed where all network-connected data must be able to defend itself from attacks at any endpoint. The system must have an awareness of timeline, identity, location and content, with well-defined user access policies. For example, when millions of users need access to cloud resources, user provisioning and de-provisioning should be simple, scalable and efficient.

In other words, if we apply ordinary encryption to cloud storage, it will prevent the cloud provider from processing the data, and will confine the cloud’s role to being just simple storage. There are two kinds of encryption which can be applied to achieve trusted data sharing over untrusted CSPs, namely incremental encryption and homomorphic encryption.

1. Incremental encryption

In cryptography, the term ‘plaintext’ refers to data in its original plain form while ‘ciphertext’ refers to data in its encrypted form. In incremental encryption, plaintext is encrypted incrementally several times using different encryption keys. Incremental encryption allows the computation of the final ciphertext based on the initial ciphertext and the change in the plaintext.\footnote{Chunming Rong, Son T. Nguyen and Martin Gilje Jaatun, ‘Beyond Lightning: A Survey on Security Challenges in Cloud Computing’ (2013) 39(1) Computers & Electrical Engineering 47.} It can encrypt data multiple times with different keys, and produce a final ciphertext which can be decrypted in a single decryption by a single key. The scheme allows changing the encryption key without decrypting the data first, thus it enables the re-encryption of data in an untrusted environment. During the sharing, the data is always in its encrypted form, though at different stages it may be encrypted with different keys. There is no single stage in which the data is decrypted into its plain form before it is delivered to the authorized users. For example,
the cloud user $U_1$ encrypts all his documents using his key $K_1$. When $U_1$ wants to share one of the documents $D_1$ with another user $U_2$, $U_1$ can incrementally encrypt the document $D_1$ with another key $K_2$. The user $U_2$ can then decrypt the incrementally encrypted document $D_1$ with another key $K_3$. In the sharing process, the document $D_1$ never appears in plain form until it is delivered to and decrypted by the authorized user $U_2$.

2. **Homomorphic encryption**

Homomorphic encryption allows the CSP storing the ciphertext to perform certain operations without decrypting the ciphertext. With homomorphic encryption, the CSP can perform operations on the data without decrypting the data, that is, the encrypted data never appears in plain form during the data processing. Unfortunately, at the moment there is no practical homomorphic encryption scheme that can be implemented in the cloud computing environment.

D. **Hardware-Anchored Security**

In 2013, Ryan proposed hardware-anchored security. Under this scheme, the CSP can decrypt the data when the CSP needs to perform processing on it. The main idea is that the decryption key is bound to the programme. The CSP can use the key to process the data using the designated programme, while no other programme is allowed to use the key. The CSP uses special hardware to store the keys which makes them accessible only to designated programmes. Hardware-anchored security in the style of Excalibur is a more versatile and applicable approach.

E. **Remove Sensitive Data**

Data encryption provides a good way for protecting data confidentiality but it often requires the sacrifice of a certain degree of efficiency and flexibility in data processing. Instead of encrypting all the data, another way to ensure data confidentiality is to remove the sensitive data and just store non-sensitive data in the cloud. For example, when handling data containing personally identifiable information, the client can remove the

---


42 Mark D. Ryan (n 41).

unique identifying information to protect user privacy. This method preserves efficiency and flexibility in data processing as the distribution and management of keys are not required.

V. CONCLUSION

Given that cloud computing has become part of our lives, data security and privacy have become an increasing area of concern for both service providers and users. No matter what line of business, branch of government or online engagement one is dealing with, once we decide to use the cloud, preventing unauthorized access to information resources will become a major consideration. This chapter has highlighted the security issues unique to the architecture of cloud computing. The solutions lie in strengthening in-built technological security capabilities and management, reaching new types of contractual arrangements between service providers and users and in adopting encryption technology.

Data must be secured while at rest, in transit and in use, and access to the data must be controlled. Standards for communications protocols and public key certificates allow data transfers to be protected using cryptography and can usually be implemented with similar effort in SaaS, PaaS and IaaS environments. Any cloud computing solution should be properly configured, deployed and managed to meet the security and privacy requirements of customers and consumers using the solution. Organizational or business data must be protected in a manner consistent with the organization’s or business’s policies, whether in the organization’s or business’s computing centre or in the cloud. In addition, security and privacy controls should be implemented correctly and operate as intended throughout the system lifecycle. Accountability for security and privacy in cloud deployments cannot be delegated entirely to cloud providers. To a certain degree, it also remains an obligation for users to fulfill.

As cloud service providers endeavour to come to grips with having to tackle security challenges in the constantly morphing clouds, users should also grapple with newly arising concerns and not be too easily dazzled by digital cloud wizardry. We all want to live in a smarter cloud at a fast rate and at low cost, but we also need to factor data security into the total equation.

Securing Cyber-Physical Critical Infrastructure (Waltham, Massachusetts, United States: Elsevier 2012) 389.