Webology (ISSN: 1735-188X)
Volume 19, Number 2, 2022

An Investigation Into Recent Security And Privacy Issues In Cloud Multi-Tenancies

Mirza Mohammed Akram Baig

Senior Member of Technical Staff, Illumio Inc.

Abstract
Cloud computing has become a popular phenomenon in the 21st century. The uniqueness and shattering growth of cloud computing makes this a sensational research area. The aim of the paper was to survey recent security and privacy issues in cloud multi-tenancies. The article put together unique works that address the risks, liabilities, and potential controls in cloud computing. Even though cloud computing emerged recently, key security and privacy issues have emerged from recounted events of initial users trialing with existing service provider platforms. Issues discussed include trust, the cloud computing structural design, management of identity, software isolation, safety of data, and availability of the cloud computing platform.

Keywords: Cloud computing; security of data; data privacy; NIST; virtual machin

Introduction

The 21st century is best characterized as an age of information and globalization. As a consequence, it is riddled with businesses that desire massive computing power to generate insights and achieve competitive advantage [1], [2]. Traditionally, enterprises process their data through in-house data centers. However, it can be complicated and costly for businesses to operate data centers and keep up with the increasing data processing requests. This is where cloud computing comes in as an alternative.

Cloud computing has in recent times surfaced as a buzzword in the distributed computing community. Many scholars and experts deem that Cloud will restructure the information technology industry as a revolution [3]. Cloud computing promises to provide on-demand computing power with certain benefits, such as quick implementation, less information technology staff, little maintenance, and lower cost [4]. As projected by Gartner [5], end-user expenditure on public cloud is likely to grow 18% in 2021. As businesses grow their investment in mobility, cooperation, as well as other isolated working tools and infrastructure, Gartner expects growth in public cloud to be continuous beyond 2024 [5]. Recent survey data also shows that close to 70%

of institutions currently employing cloud services are likely to increase their cloud spending because of the disruption caused by the coronavirus pandemic [5].

The uniqueness and exploding growth of cloud computing makes this a sensational research area. Currently, there are many cloud computing challenges that need identifying, analyzing, and addressing [3], [4], [6]. The current paper attempts to survey recent security and privacy issues in cloud multi-tenancies. The article puts together unique works that address the risks, liabilities, and potential controls in cloud computing. It also presents information on the top cloud architectures and frameworks.

The remainder of the review paper is structured in the following manner: Section 2 presents an overview of cloud computing and its architecture. The section defines cloud computing and lists associated actors, delivery models, and the basic cloud service offerings. Section 3 discusses the key securities and privacy issues affecting cloud computing. Issues discussed include trust, the structure of cloud computing, management of identity, software isolation, protection of data, and availability of the cloud computing environment. Finally, section 4 concludes the paper with potential future directions.

2. An Overview of Cloud Computing and Its Architecture

A. Definition

Many conventional definitions of cloud computing have been suggested. However, the definition provided by the U.S. National Institute of Standards and Technology (NIST) standards out and seems to have the primary elements often used in the Cloud Computing community. According to NIST "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or service provider interaction," [7]. The definition by NIST includes cloud architectures, deployment, and security strategies. Specifically, five primary cloud computing elements are evidently formulated: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

B. Primary Cloud Computing Elements

The on-demand self-service element allows an individual with an instantaneous need to automatically provide computing assets without turning to human interaction with the providers of the resources. Examples of computing resources under this element include CPU time, the use of software, and network storage among many others [8]–[10]. The second element, broad network access, involves computing resources that are provided over the network, such as the internet. Many client applications with dissimilar platforms positioned at the site of a consumer, such as laptops, mobile phones, and PDAs use these resources [3], [8]–[10]. The next element, resource pooling, requires a provider of cloud services to combine their resources and provide their services to different clients using multi-tenancy or rather virtualization prototypes. Resource pooling

presents a decent opportunity to assign and reassign different resources depending on client requirements. The motivation for resource pooling lies in two primary factors: specialization and the economies of scale. Resource pooling hides the physical computing resources from the clients, who in many instances do not have information about the location, formation, and originalities of the resources. What this means is that cloud computing clients never have even the slightest information on where their data is stored in the cloud [3], [8], [10]. Next, rapid elasticity describes computing resources and how they are immediate instead of persistent. Resource provision for most consumers seems to be infinite, and consumption can increase rapidly to meet the peak requirements at any moment. The last element, measured service, refers to the cloud infrastructure that processes the use of computing resources for every individual consumer through its metering capabilities [3], [9], [10].

C. Service Models

Apart from the five characteristics described above, cloud computing has also been categorized under various service models: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Data storage as a Service (Daa S). Under the SaaS model, companies allocate their functions to a hosting atmosphere. Users access these functions through distinct clients, for instance web browser and Personal Digital Assistant, among others. The Cloud infrastructure follows a multi-tenancy system architecture that denies consumers control. Some examples of SaaS include Google Mail, SalesForce.com, and Google Docs among others [3], [11]. PaaS is a model that bolsters the entire "Software Lifecyle" and presents clients with the chance to develop cloud functions precisely on the PaaS cloud. SaaS and PaaS are different in that SaaS is dedicated to proficient cloud functions while the PaaS model supports both complete and incomplete projects. Google App Engine is an example of PaaS [3], [12]. IaaS directly provides consumers with IT infrastructures, such as processing, networks, storage, and other key computing resources. Under the IaaS model, clients can benefit from virtualization, which combines physical resources to meet the changing demands from clients. Amazon's EC2 is an example of IaaS [3], [13]. The last model, Daa S, delivers virtualized storage on demand. This model can be considered as a special type of IaaS. With Daa S, consumers can pay for whatever they are using instead of the site license for the entire database. Google Big Table, Amazon S3, and Apache HBase are primary examples of Daa S [3].

D. Deployment Models

Four deployment models exist in the cloud community: private, community, public, and the hybrid cloud. A single organization manages the structure of a private cloud. The structure is then controlled by the organization or an external party, notwithstanding whether it is on or off the premise. A private cloud can be setup to maximize and optimize the use of current in-house resources, deal with security concerns, and to facilitate teaching and research purposes [3], [14]. The private cloud community allows institutions to advance a similar cloud structure governed with strategies, obligations, ideals, and concerns. Such a cloud structure could be hosted by an

external vendor or one institution within the community [3], [14]. The most dominant type of Cloud computing is the public cloud. The public uses this model to enjoy ownership of public cloud services. Examples of common public clouds include Google App Engine, Amazon EC2, S3, and Force.com [3], [14]. The last category, the hybrid cloud infrastructure merges more than one cloud as distinctive units. However, these clouds are supported together using a regulated set of rules or trademarked technology. Some organizations opt to use the hybrid cloud infrastructure to optimize their resources, enhance their key competencies, and control core activities [3], [14].

3. Key Security and Privacy Issues of Cloud Computing

Even though cloud computing emerged recently, it is possible to get perceptions of key security and privacy issues from testified encounters of initial uses and experiments [15]. This section addresses security and privacy-related issues that have a longstanding significance for cloud computing. In some issues, the paper presents examples of challenges initially exhibited to exemplify the issue. Since cloud computing has sprouted out of a merger of technologies, most of the security and privacy issues involved can be considered as known problems presented in a new setting.

A. Trust

Trust, as a concept, is a difficult matter with no globally approved scholarly definition. According to Pearson and Benameur [16], trust refers to a "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another." However, this definition does not adequately capture the vibrant subtleties involved. Trust is considered a measurable belief that uses experience to make responsible decisions.

Within the cloud computing environment, an institution gives up direct power over various safety matters [16]. By doing so, they bestow a high level of trust upon the service provider. Consequently, clients lose power over cloud resources and concede a poor position to safeguard their data against unsanctioned access, subordinate use, or other arrangements of misappropriation [16], [17]. Instead, customers must depend on contracts or other trust aspects to try to promote proper usage. Besides, they must also depend on compensation mechanisms in the event of a breach [3], [16]. This heightens the risk to data privacy and security.

Data that is prepared or stored externally has a high level of insider security threat attached to it. Insider threats exceed those posed by current or former employees and include those resulting from organizational affiliates, contractors, as well as entities that receive access to the networks, data, and systems belonging to an organization [15], [16]. Security incidents may arise from different forms of fraud, interference with sources of information, and theft of information. A few occurrences can happen without warning. Moving data and functions from an organization to an outward cloud computing environment raises the insider security risk for the service provider and other clients using the service [16], [17]. An example of this is when a service user creates initial accounts on Amazon Elastic Compute (EC2) and launches virtual machine instances for each as part of an internal denial of service attack [15].

Trust issues can also arise from composite services. As mentioned initially, it is possible to nest and layer one cloud service over another. To demonstrate, a SaaS provider may develop its services while relying on an IaaS or PaaS cloud [3], [15], [18]. Service providers that hire external experts for some of their functions can encounter some concerns, including the nature of control over the external party, their responsibilities, and potential fixes whenever issues arise. Trust is never transitive and can be a major issue to deal with, especially when handling composite services [15], [16]. Liability and performance guarantees can also turn out to be a major issue with composite cloud services. A fitting example is The Linkup, an online storage service that closed operations after losing their access to data belonging to over 20,000 customers. The loss came about because Nirvanix and Savvis (both external parties) hosted customer data and application and database correspondingly for The Linkup [15].

Various approaches have been developed to protect clouds against threats that can weaken trust levels. Traditional hard security measures, including encryption and authorization, provide a strong foundation [17], [19], [20]. However, these measures fail when third-party entities act malevolently because of the extent and provisional nature of collaborations. Trust is a sensitive social security phenomenon that can help restrict malevolent entities resulting from external interactions, thereby dealing with security threats. Besides, trust also develops a cloud computing environment with the highest level of trustworthiness [17], [19], [20].

It is a challenging ask to assess and control the risk involved in cloud computing services. In many instances, the degree of trust relies on the level of direct control that an institution can apply to third-party service providers [3]. There can be different phases in a trust relationship in cloud computing. It is difficult to build trust, while at the same time it is also easy to lose it. A single contravention of trust can damage years of slowly amassed credibility.

B. The Cloud Computing Architecture

Cloud services are delivered with the help of software systems. The structure of these services includes hardware and software living within the cloud. It is the responsibility of the service provider to find out the physical location of the cloud computing structure and the procedures for executing the basic support framework [3], [21]. The theoretical unit of deployment includes virtual machines (VMs) which are blended informally with the structure of the cloud storage. Cloud computing applications are developed on the programming surfaces of internet-enabled services and entail a number of cloud elements that communicate with each other [3], [15], [21]. Because of this, the architecture of cloud computing can be susceptible to attack surface, virtual network protection, ancillary data, client-side protection, and server-side protection issues.

Within the cloud environment, there is always an extra layer of software installed between an operating system and a hardware platform. The extra layer is often referred to as a virtual machine monitor or a hypervisor [3], [15], [22]. This layer facilitates the operation of multi-tenant VMs as well as applications hosted accordingly. Apart from virtualized resources, the virtual machine monitor always supports additional programming interfaces to carry out administrative operations, including launching, migrating, and ceasing VM occurrences [22]. Contrasted to a non-

virtualized implementation, including a virtual machine monitor results in an increase in the attack surface which can compromise the security within the cloud computing environment. The complexity in the virtual machine environment can also be more challenging compared to its traditional counterpart, thereby resulting in conditions that weaken security [22]. To demonstrate, activities such as paging, checkpointing, along with the migration of virtual machines can uncover delicate data. This can subvert the mechanisms of protection within a hosted operating system. There is also an increased possibility that the hypervisor could be compromised. For example, a zero-day manipulation in the Hyper VM virtualization application apparently caused an eradication of about 100,000 virtual server-based websites held at Vaserv.com [15], [23].

Most platforms used for virtualization can develop switches based on software and network designs in their simulated environment. Such tools allow simulated machines on a similar host to converse openly [3], [15]. The security protection devices available on the physical network cannot notice traffic on such networks. Such a security threat can be averted by duplicating the physical network protections on the virtual network [3], [15].

The emphasis of protection in the cloud computing environment is on application data. However, service providers also hold extensive information concerning the accounts of the users. There is a high chance that such information could be compromised and used in subsequent attacks [3], [15]. Payment information is an example of such details. Salesforce.com experienced such an attack when their database of contact information was stolen through targeted phishing and used to set up effective email attacks against the users of the service [15]. An incident like this demonstrates that cloud computing service providers must account for security violations happening in all the data they hold. Virtual machine images are another category of ancillary data that can be subjected to attacks [24], [25]. A virtual machine image is used to boot the VM into an earlier version or a version of some preliminary checkpoint. Most businesses in the cloud computing environment share VM images. However, these image repositories must be managed meticulously and regulated to avoid potential challenges [24], [25]. The image provider faces an increased risk since an image can include proprietary code and data**.** Attackers have the ability to analyze images to establish if they disclose information or provide an opportunity for data violation. Such an instance can occur, especially when working with development images that are released by mistake. Alternatively, it is also possible for an attacker to provide a VM image with malware to users in a cloud computing environment [3], [15], [24], [25].

A successful defense system in cloud computing requires a secure client, secure website infrastructure, as well as a secure server–side protection. Web browsers and the other plug-ins and extensions used in the cloud computing environment are popular for their security problems [3], [26]. It is also important to note that a majority of add-ons on browsers do not present an opportunity for automatic updates. This boosts the tenacity of security issues. The security of a browser can also be affected by the existence of social media, personal Webmail, and other platforms that are available in the public domain [3], [26]. For example, [15] noted a spyware attack that was installed in a hospital through the Yahoo Webmail account of an employee. The attack disseminated over 1,000 screen captures comprising financial and other confidential

information [15]. Any form of malware can interfere with the security of a cloud computing platform. Hence, organizations must employ measures to safeguard the client side as part of the general architecture of the cloud computing environment. Similarly, the server-side often requires protection [3], [26]. It is important to protect virtual servers in IaaS, in the same manner that non-virtualized types enjoy protection. The server-side must also be managed carefully to minimize the unplanned deployment of data comprising vulnerabilities [3].

C. Identity Management

Data sensitivity and the privacy of information increasingly concern many organizations. Aligned to the privacy of information is unauthorized access [3]. A key reason for this is that the identification and authentication structure used by most organizations may not extend into the cloud. This may need a lot of input to restructure the design of cloud services. In many cases, it is impractical to have two distinct systems, one meant for internal while the other meant for external systems. One way to manage identity is through the Security Assertion Markup Language (SAML) standard [3], [27], [28].

Most providers of cloud services support the SAML model and use it to manage and authenticate users before allowing them access to applications and data. Through SAML, providers of cloud services have time to swap information [3], [28]. Requests and response messages passing through SAML are plotted over the Simple Object Access Protocol (SOAP), which depends on XML for its format. For instance, after an individual on Amazon Web Services develops a public key certificate, it can be used to guarantee SOAP requests to the EC2 [29]. However, the security validation of SOAP messages is a complex process and must be implemented out painstakingly to prevent potential attacks, such as XML wrapping attacks. These attacks manipulate SOAP messages and have successfully been exhibited against Amazon's EC2 services [3], [28], [29].

Apart from authentication issues, the cloud computing environment also suffers from the ability to alter the privileges of users and retain control over the right to use resources. Essentially, access control is part of identity management [30], [31]. Most organizations use standards, such as eX tensible Access Control Markup Language (XACML) to manage access to cloud resources rather than depending on the proprietary interface of the service provider [32]. XACML can regulate the patented service interfaces of cloud computing providers, some of which have the standard incorporated in their operations, such as salesforce.com and Google Apps [15]. Messages communicated through XACML are vulnerable to attack by mischievous third parties. Because of this, it is important for organizations to have precautions in place to safeguard decision requests and authorization decisions from potential attacks. Appropriate precautions can help minimize unauthorized disclosure, deletion, replay, and modification attacks [3].

D. Software Isolation

A virtual machine monitor (VMM) runs various guest VMs and hosts operating systems and applications simultaneously on a single host computer. From a theoretical point of view, a VMM can be less significant and less intricate matched to an operating system [22]. The small size and

the lack of sophistication makes it easier to examine and enhance the quality of security. This gives a VMM the ability to maintain strong isolation between the guest VMs [3], [33]. In practice, however, contemporary VMMs can be large and problematic contrasted to an operating system, counteracting the stated benefits. Subsequently, functions installed on guest VMs remain exposed to attack and compromise, in the same manner as their non-virtualized counterparts. Hence, it is important for organizations to understand the concept of virtualization to comprehend the risks and security issues involved [22], [33].

In addition to VMM complexity, multi-tenancy in VM-based cloud infrastructures can cause a new set of attack vectors. The gravest threat is that a nasty code could dodge the locality of its VMM and impede the virtual machine monitor or other guest VMs [3], [22], [33]. The transition of a VM between hypervisors on various host computers, often referred to as live migration, can also increase the size of the software and complexity involved in securing the cloud computing environment. The increased size of the software possibly adds other areas to target in an attack [3]. There are various examples of attack vectors that are possible in this kind of software setup. One illustration is mapping the cloud structure, which is an involving task to accomplish. Moreover, there are some indirect attack avenues that are possible in the cloud computing environment. As an example, an attacker can get managerial control of VMware guest VMs in live migration [21]. It is possible that a man-in-the-middle attack could be used to change the code used for authentication. In the course of migration, memory modification can result in additional possibilities, such as the ability to include a VM-base rootkit layer underneath the operating system [15], [34]. Another illustration may involve inspecting the use of resources on a shared server. The aim of such an attack could be to obtain information and start a side-channel attack similar to those used in computing setups. An attacker may determine top activity times, examine the rate of traffic, and carry out keystroke timing attacks to get passwords and related data from the target [3], [34].

E. Protection of Data

Data stored in the cloud occurs in a distributed environment combined with data from other customers. Institutions transferring confidential data into the cloud must account for the control of data [3], [35], [36]. Data in a cloud-based application exists in various forms, ranging from application programs, configuration settings, scripts, and development tools. The data may also include records, account information, and other content created or used by deployed applications [35], [36]. One way to keep such data from unauthorized access is to use access controls and encryption. However, access controls are basically based on identity, making the authentication of the identity of users a key security issue in cloud computing [3], [35], [36].

Cloud computing also uses different database environments. Some databases support a multi-instance model, while others use a multi-tenant model. A multi-instance model includes a distinctive database management system running on a VM instance for each service user. This model gives the user total control over the definition of roles, authorization of users, as well as other administrative duties associated with the security of the cloud computing environment [37]. On the contrary, a multi-tenant model creates a pre-defined environment that is shared among

cloud service tenants. The model does this by tagging data with the identity of the users. Even though tagging is an unquestionable use of instance, it relies on the service provider to maintain a safe database environment. There are many multi-tenant arrangements that can be used on databases [38]. Multi-tenant arrangements pool resources different and offer varying levels of isolation and resource efficiency. Because of this, the privacy of sensitive information remains a serious concern in cloud computing [3].

Besides, data needs to be protected while at rest, in transit, and while in use. It is also important to control access to data. Data transfers using cryptography can be protected using procedural standards and public key certificates [39], [40]. However, the techniques for protecting data at rest are yet to be clearly standardized. This makes interoperability an issue because of the superiority of patented systems [3], [39], [40]. The constrained interoperability impacts the availability of data and complicates the convenience of applications and data between the cloud service providers.

Cloud computing service providers also implement data sanitization practices that have clear security consequences. Data sanitization involves removing confidential data from a storage device in various circumstances, a case in example when a storage device is eradicated from service or moved somewhere else for storage [3], [15]. The process also influences backup copies designed for recovery, repair of service, and remaining data after the closure of a service. In a cloud computing, the data obtained from one subscriber can be considerably mixed with the data collected from other subscribers. This possibility often makes matters difficult to deal with a cloud computing environment. Attackers with suitable skills and tools can effortlessly recover data from botched drives that have been disposed of poorly [3], [41].

Another cloud computing issue arising from data protection concerns the location of data. Organizations that use an in-house computing center develop better structures that allow data to be stored and safeguarded [3], [42], [43]. Then again, a characteristic of most cloud computing services is that the detailed information of the location of an institution's data is inaccessible or never presented to the service subscriber. With such a possibility, it is difficult to ascertain whether enough safeguards have been put in place and whether legitimate and supervisory conditions are being met [42], [43]. External audits and security certifications can help assuage this issue, but they are not a universal solution. Furthermore, upon passing the nationwide border it becomes difficult to provide data protection under peripheral laws and regulations [42], [43]. A solid example of this is the solid power of the USA Patriot Act that has raised apprehensions with some external governments since the provision would grant the U.S. government access to private information [3], [44]. Hence, the location of data determines the technical, physical, and administrative precautions of data stored in the cloud.

F. Cloud Computing Availability

Availability issues concern whether an organization has its complete set of computing resources accessible and functional all the time. Interferences to availability can be temporary or permanent,

and can result in the restricted or complete loss of data. The availability of data can be jeopardized by equipment outages, denial of service attacks, along with natural disasters [3], [42], [45].

Even though cloud computing services use architectures that guarantee high service availability and reliability, these platforms can and often encounter outages and slowdown in performance. As an example, Amazon's Simple Storage Service (S3) and EC2 services experienced an outage lasting three hours that, eventually, affected Twitter and similar startup companies using these services in 2008 [3], [46]. Similarly, Microsoft's Azure cloud service encountered a serious degradation in March 2009 that lasted for close to 22 hours [3], [47]. Cloud computing services have a 99.999% reliability, and this allows at least 8.76 hours of downtime each year. Consequently, the reliability of a cloud service together with its ability for backup and recovery should be considered in an organization's emergency plan [3]. A contingency plan may include an alternative cloud service provider backing up data to ensure that during an extended disruption at the primary provider, the data remains accessible for an instant recommencement of key operations [48]. Apart from temporary outages, cloud computing service providers can also experience prolonged and permanent outages. These can often arise from bankruptcy or facility loss, which affects service for longer periods of time [48]. An example of this was in 2009 when the Federal Bureau of Investigation (FBI) invaded computing centers in Texas and confiscated hundreds of servers while probing fraud allegations against some companies. The confiscation perturbed service to various businesses secluded from the investigation. Most of these businesses had their data collocated at the targeted centers [3].

Denial of service attacks can also affect the availability of data in cloud computing. A denial-of-service attack fills a target with sham invitations to prevent them from reacting to legitimate requests in a timely manner [3], [49], [50]. The attacker uses different computers or a botnet to start an incursion. The vibrant nature of a cloud connects an attacker to potential harm. Cloud resources are colossal and can be saturated with enough attacking devices [50]. A simple denial of service attack can quickly consume a lot of resources to shield against and cause an increase in charges. This type of attack can also affect private services in the cloud [3], [49], [50].

The value concentration of data in the cloud can also affect availability of cloud computing services. Essentially, data is considered the 21st century currency and the cloud-based environment is the bank vault [3]. Because of this, the cloud computing environment is an ever more preferred target for most attackers. Compromising the security of the cloud has a remarkably high payoff. Putting together data with that of an organization with an outstanding threat profile can contribute to a denial-of-service attack as an unintentional casualty [3], [49], [50]. Similarly, it is possible for there to be indirect effects from an attack directed against the physical resources of a service provider dealing with a high-profile organization. An example would be the IRS facilities that are incessantly targeted by imminent attackers [3].

4. Conclusion

This paper explored the recent security, and privacy issues surrounding the cloud computing environment. The paper also explored various cloud computing architectures, their requirements,

applications, and assorted challenges and concerns. The following groups of security and privacy issues are discussed: trust, the structure of the cloud computing environment, management of identity, software isolation, protection of data, and availability of the cloud computing platform. In the cloud computing environment, an institution gives up all the control over various aspects of security. This gives the service provider a high level of trust. Most customers lose control of the resources in the cloud and are never in a decent position to use technical mechanisms to safeguard their data against unauthorized access, subordinate usage, and other forms of misuse.

The structure of cloud computing relies on consistent computing and cryptography. It is necessary to protect data belonging to an institution that is consistent with policies, whether it is available physically or in the cloud. No regulated service exists to cover the various cloud services available together with the requirements of various organizations. The starting point to dealing with the highlighted security and privacy issues is developing a list of common outsourcing provisions, including privacy and security standards, service level requirements, regulatory and compliance issues, continuity of service provisions, change management processes, and termination rights among many others.

References

[1] V. Rajaraman, "Cloud computing," Reson, vol. 19, no. 3, pp. 242–258, Mar. 2014, doi: 10.1007/s12045-014-0030-1.

[2] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for Internet of Things sensing based applications," in 2012 Sixth International Conference on Sensing Technology (ICST), Dec. 2012, pp. 374–380, doi: 10.1109/ICSensT.2012.6461705.

[3] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Apr. 2010, pp. 27–33, doi: 10.1109/AINA.2010.187.

[4] H. Yang and M. Tate, "Where are we at with Cloud Computing?: A Descriptive Literature Review," ACIS 2009 Proceedings, vol. 26, Dec. 2009, [Online]. Available: https://aisel.aisnet.org/acis2009/26.

[5] Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021," Gartner, Nov. 17, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021 (accessed May 07, 2021).

[6] Y. Wei and M. B. Blake, "Service-Oriented Computing and Cloud Computing: Challenges and Opportunities," IEEE Internet Computing, vol. 14, no. 6, pp. 72–75, Nov. 2010, doi: 10.1109/MIC.2010.147.

[7] NIST, "Final Version of NIST Cloud Computing Definition Published," NIST, Oct. 25, 2011. https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published (accessed May 07, 2021).

[8] B. Liu et al., "Information fusion in a cloud computing era: A systems-level perspective," IEEE Aerospace and Electronic Systems Magazine, vol. 29, no. 10, pp. 16–24, Oct. 2014, doi: 10.1109/MAES.2014.130115.

[9] H. Geng, "Internet of Things and Data Analytics in the Cloud with Innovation and Sustainability," in Internet of Things and Data Analytics Handbook, John Wiley & Sons, Ltd, 2017, pp. 1–28.

[10] A. S. Sendi and M. Cheriet, "Cloud Computing: A Risk Assessment Model," in 2014 IEEE International Conference on Cloud Engineering, Mar. 2014, pp. 147–152, doi: 10.1109/IC2E.2014.17.

[11] J. Y. Lee, J. W. Lee, D. W. Cheun, and S. D. Kim, "A Quality Model for Evaluating Software-as-a-Service in Cloud Computing," in 2009 Seventh ACIS International Conference on Software Engineering Research, Management and Applications, Dec. 2009, pp. 261–266, doi: 10.1109/SERA.2009.43.

[12] W. Tian, S. Su, and G. Lu, "A Framework for Implementing and Managing Platform as a Service in a Virtual Cloud Computing Lab," in 2010 Second International Workshop on Education Technology and Computer Science, Mar. 2010, vol. 2, pp. 273–276, doi: 10.1109/ETCS.2010.126.

[13] S. S. Manvi and G. Krishna Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey," Journal of Network and Computer Applications, vol. 41, pp. 424–440, May 2014, doi: 10.1016/j.jnca.2013.10.004.

[14] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Mar. 2012, pp. 877–880, doi: 10.1109/ICCEET.2012.6203873.

[15] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in 2011 44th Hawaii International Conference on System Sciences, Jan. 2011, pp. 1–10, doi: 10.1109/HICSS.2011.103.

[16] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Nov. 2010, pp. 693–702, doi: 10.1109/CloudCom.2010.66.

[17] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," Procedia Engineering, vol. 15, pp. 2852–2856, Jan. 2011, doi: 10.1016/j.proeng.2011.08.537.

[18] R. K. Jena, "Multi Objective Task Scheduling in Cloud Environment Using Nested PSO Framework," Procedia Computer Science, vol. 57, pp. 1219–1227, Jan. 2015, doi: 10.1016/j.procs.2015.07.419.

[19] Y. S. Gunjal, M. S. Gunjal, and A. R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing," in 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), Feb. 2018, pp. 187–190, doi: 10.1109/ICACCT.2018.8529627.

[20] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," in 2011 31st International Conference on Distributed Computing Systems, Jun. 2011, pp. 383–392, doi: 10.1109/ICDCS.2011.55.

[21] M. E. Elsaid and C. Meinel, "Multiple Virtual Machines Live Migration Performance Modelling – VMware vMotion Based Study," in 2016 IEEE International Conference on Cloud Engineering (IC2E), Apr. 2016, pp. 212–213, doi: 10.1109/IC2E.2016.9.

[22] D. Ye, A. Pavuluri, C. A. Waldspurger, B. Tsang, B. Rychlik, and S. Woo, "Prototyping a hybrid main memory using a virtual machine monitor," in 2008 IEEE International Conference on Computer Design, Oct. 2008, pp. 272–279, doi: 10.1109/ICCD.2008.4751873.

[23] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, "Intrusion Detection System in Cloud Computing: Challenges and opportunities," in 2013 2nd National Conference on Information Assurance (NCIA), Dec. 2013, pp. 59–66, doi: 10.1109/NCIA.2013.6725325.

[24] M. Kazim, R. Masood, and M. A. Shibli, "Securing the virtual machine images in cloud computing," in Proceedings of the 6th International Conference on Security of Information and Networks, New York, NY, USA, Nov. 2013, pp. 425–428, doi: 10.1145/2523514.2523576.

[25] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in Proceedings of the 2009 ACM workshop on Cloud computing security, New York, NY, USA, Nov. 2009, pp. 91–96, doi: 10.1145/1655008.1655021.

[26] N. Kaaniche and M. Laurent, "A Secure Client Side Deduplication Scheme in Cloud Storage Environments," in 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), Mar. 2014, pp. 1–7, doi: 10.1109/NTMS.2014.6814002.

[27] Md. S. Ferdous and R. Poet, "Dynamic Identity Federation Using Security Assertion Markup Language (SAML)," in Policies and Research in Identity Management, Berlin, Heidelberg, 2013, pp. 131–146, doi: 10.1007/978-3-642-37282-7_13.

[28] J. Wang, D. Del Vecchio, and M. Humphrey, "Extending the security assertion markup language to support delegation for Web services and grid services," in IEEE International Conference on Web Services (ICWS'05), Jul. 2005, pp. 67–74 vol.1, doi: 10.1109/ICWS.2005.59.

[29] N. Gruschka and L. L. Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," in 2009 IEEE International Conference on Web Services, Jul. 2009, pp. 625–631, doi: 10.1109/ICWS.2009.70.

[30] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," Journal of Information Security and Applications, vol. 19, no. 1, pp. 45–60, Feb. 2014, doi: 10.1016/j.jisa.2014.04.003.

[31] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in 2010 Proceedings IEEE INFOCOM, Mar. 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5462174.

[32] I. C. Hsu, "Extensible access control markup language integrated with Semantic Web technologies," Information Sciences, vol. 238, pp. 33–51, Jul. 2013, doi: 10.1016/j.ins.2013.02.046.

[33] R. Jithin and P. Chandran, "Virtual Machine Isolation," in Recent Trends in Computer Networks and Distributed Systems Security, Berlin, Heidelberg, 2014, pp. 91–102, doi: 10.1007/978-3-642-54525-2_8.

[34] E. Brown, B. Yuan, D. Johnson, and P. Lutz, "Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks," Journal of Information Warfare, vol. 9, no. 3, pp. 26–38, 2010.

[35] F. Pfarr, T. Buckel, and A. Winkelmann, "Cloud Computing Data Protection – A Literature Review and Analysis," in 2014 47th Hawaii International Conference on System Sciences, Jan. 2014, pp. 5018–5027, doi: 10.1109/HICSS.2014.616.

[36] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in 2012 International Conference on Computer Science and Electronics Engineering, Mar. 2012, vol. 1, pp. 647–651, doi: 10.1109/ICCSEE.2012.193.

[37] M. M. O. Deye, Y. Slimani, and M. Sene, "Load Balancing Approach for QoS Management of Multi-instance Applications in Clouds," in 2013 International Conference on Cloud Computing and Big Data, Dec. 2013, pp. 119–126, doi: 10.1109/CLOUDCOM-ASIA.2013.69.

[38] E. J. Domingo, J. T. Nino, A. L. Lemos, M. L. Lemos, R. C. Palacios, and J. M. G. Berbís, "CLOUDIO: A Cloud Computing-Oriented Multi-tenant Architecture for Business Information Systems," in 2010 IEEE 3rd International Conference on Cloud Computing, Jul. 2010, pp. 532–533, doi: 10.1109/CLOUD.2010.88.

[39] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences, vol. 387, pp. 103–115, May 2017, doi: 10.1016/j.ins.2016.09.005.

[40] A. N. Jaber and M. F. B. Zolkipli, "Use of cryptography in cloud computing," in 2013 IEEE International Conference on Control System, Computing and Engineering, Nov. 2013, pp. 179–184, doi: 10.1109/ICCSCE.2013.6719955.

[41] P. Han et al., "CloudDLP: Transparent and Scalable Data Sanitization for Browser-Based Cloud Storage," IEEE Access, vol. 8, pp. 68449–68459, 2020, doi: 10.1109/ACCESS.2020.2985870.

[42] Z. Mahmood, "Data Location and Security Issues in Cloud Computing," in 2011 International Conference on Emerging Intelligent Data and Web Technologies, Sep. 2011, pp. 49–54, doi: 10.1109/EIDWT.2011.16.

[43] T. Ries, V. Fusenig, C. Vilbois, and T. Engel, "Verification of Data Location in Cloud Networking," in 2011 Fourth IEEE International Conference on Utility and Cloud Computing, Dec. 2011, pp. 439–444, doi: 10.1109/UCC.2011.72.

[44] S. C. Bennett, M. J. Daley, and N. Gerlach, “Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act,” Sedona Conf. J., vol. 13, pp. 235–252, 2012.

[45] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, “The rise of ‘big data’ on cloud computing: Review and open research issues,” Information Systems, vol. 47, pp. 98–115, Jan. 2015, doi: 10.1016/j.is.2014.07.006.

[46] W. Kim, “Cloud computing: Today and tomorrow,” Journal of Object Technology, vol. 8, no. 1, pp. 65–72, 2009.

[47] B. P. Rimal, E. Choi, and I. Lumb, “A Taxonomy and Survey of Cloud Computing Systems,” in 2009 Fifth International Joint Conference on INC, IMS and IDC, Aug. 2009, pp. 44–51, doi: 10.1109/NCM.2009.218.

[48] N. Sultan, “Cloud computing: A democratizing force?,” International Journal of Information Management, vol. 33, no. 5, pp. 810–815, Oct. 2013, doi: 10.1016/j.ijinfomgt.2013.05.010.

[49] S. Dong, K. Abbas, and R. Jain, “A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments,” IEEE Access, vol. 7, pp. 80813–80828, 2019, doi: 10.1109/ACCESS.2019.2922196.

[50] K. Bhushan and B. B. Gupta, “Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment,” J Ambient Intell Human Comput, vol. 10, no. 5, pp. 1985–1997, May 2019, doi: 10.1007/s12652-018-0800-9.