# A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions

**Yuhong Liu**\*

Department of Information Science and Technology, Penn State Altoona, PA, USA
yuhong@psu.edu

**Yan (Lindsay) Sun**

Department of Electrical, Computer and Biomedical Engineering, University of Rhode Island, Kingston, RI, USA
yansun@ele.uri.edu

**Jungwoo Ryoo and Syed Rizvi**

Department of Information Science and Technology, Penn State Altoona, PA, USA
jryoo@psu.edu, srizvi@psu.edu

**Athanasios V. Vasilakos**

Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulea, Sweden
vasilako@ath.forthnet.gr

## Abstract
While cloud computing is gaining popularity, diverse security and privacy issues are emerging that hinder the rapid adoption of this new computing paradigm. And the development of defensive solutions is lagging behind. To ensure a secure and trustworthy cloud environment it is essential to identify the limitations of existing solutions and envision directions for future research. In this paper, we have surveyed critical security and privacy challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations, and envisioned future research directions.

## I. INTRODUCTION

Cloud computing is defined as a service model that enables convenient, on-demand network access to a large shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with mini- mal management effort or service provider interaction [1]. This innovative information system architecture, which is fundamentally changing the way that computing, storage and networking resources are allocated and managed, brings numerous advantages to users, including but not limited to reduced capital costs, easy access to information, improved flexibility, automatic service integration,

and quick deployment [2].

In spite of these advantages, as an emerging technology, cloud computing also faces tremendous security and privacy challenges which hinder its rapid adoption. Security has been recognized as the top barrier for users to move to cloud computing [3]. The reason is multifaceted. First, in the cloud environment, users outsourcing their data and applications can only rely on the Cloud Service Provider (CSP) to protect their security. Many concerns are raised due to the fear of the unknown. Second, the unique characteristics of cloud computing introduce various new security challenges. Third, the immaturity of security technologies and lack of security governance in the cloud are obstacles to satisfy users' security needs. Frequent security outages in the cloud have undermined users' confidence in adopting this new technology. The development of advanced research on cloud security challenges and solutions is urgent.

On the other hand, cloud computing presents some serious challenges to privacy. This is partly due to the fact that a person may easily lose control of his or her personal information under the terms and conditions of the CSP storing the person's information. In fact, many cloud-based social media rely on their leverage on an individual's private information to make profits. Therefore, it is highly probable for these companies to have clashes with their customers regarding their privacy policies. In this paper, we do not have separate sections that address privacy concerns in cloud computing. Rather, we discuss privacy in an opportunistic manner in various sections of our paper whenever the discussion is relevant.

The goal of this paper is to propose desirable future research directions to address the remaining challenges in cloud computing security and privacy research. Specifically, our research objectives are to 1) identify all the major security and privacy challenges in cloud computing, 2) conduct a thorough survey of the existing solutions, and 3) find any deficiencies by mapping the solutions to the challenges.

## II. SECURITY AND PRIVACY CHALLENGES

In this section, we investigate the specific security and privacy challenges in cloud computing which require the development of advanced security technologies.

### A. Loss of Control

In cloud computing, loss of control refers to the situation that cloud users' control over their data is diminished when they move the data from their own local servers to remote cloud servers. A great number of concerns about data protection are raised, since giving up direct control has to be one of the hardest things enterprises have to do [4].

#### 1) Data Loss and Data Breach

Data loss and data breaches were recognized as the top threats in cloud computing environments in 2013 [5]. A recent survey shows that 63% of customers would be less likely to purchase a cloud service if the cloud vendor reported a material data breach involving the loss or theft of sensitive or confidential personal information [6]. Whether a CSP can securely maintain customers' data has become the major concern of cloud users. The frequent outages occurring on reputable CSPs [7], including Amazon, Dropbox, Microsoft, Google Drive, etc., further exacerbate such concerns.

To help customers recover in case of service failures, data proliferation is conducted in the cloud where customers' data is replicated in multiple data centers as backups [8]. However, the distributed storage for multiple data copies may increase the risks of data breaches and inconsistency. First, due to the heterogeneity of security settings for the multiple storage devices, the overall security level of the data is only determined by the weakest link in the chain. Attackers can obtain the data if any one of the storage devices is compromised. Second, the multiple data copies need to be synchronized when customers make any data updates, including insertion, modification and deletion. The failures of data synchronization will lead to data inconsistency. Last but not least, it is more challenging for Cloud Service Users (CSUs) to track the appropriateness of a CSP's data operations. For example, it is extremely difficult to ascertain whether the CSP will completely delete all the data copies when such a request is made by the CSU [8]. External auditing processes are required to supervise a CSP's data operations.

#### 2) Data Storage and Transmission under Multiple Regional Regulations

Due to the distributed infrastructure of the cloud, cloud users' data may be stored on data centers geographically located in multiple legal jurisdictions, leading to cloud users' concerns about the legal reach of local regulations on data stored out of region [9]. Furthermore, the local laws may be violated since the dynamic nature of the cloud makes it extremely difficult to designate a specific server or device to be used for transborder data transmission [8].

#### 3) Cheap Data and Data Analysis

The rapid development of cloud computing has facilitated the generation of big data, leading to cheap data collections and analysis [10]. For example, many popular online social media sites, such as Facebook, Twitter and LinkedIn, are utilizing the cloud computing technology to store and process their customers' data [11]. Cloud providers that store the data are gaining considerable business revenue by either retrieving user information through data mining and analysis by themselves or selling the data to other businesses for secondary usage [8].

One example is that Google is using its cloud infrastructure to collect and analyze users' data for its advertising network [10].

Such data usage has raised extensive privacy concerns since the sensitive information of cloud users may be easily accessed and analyzed by unauthorized parties. The Electronic Privacy Information Center (EPIC) asked to shut down Gmail, Google Docs, Google Calendar, and the company's other Web apps until government-approved "safeguards are verifiably established" [12]. Netflix had to cancel its $1 million data challenge prize due to a legal suit because it violated customers' privacy during the data sharing process [13]. While technologies such as data anonymization are under investigation [8], users' data privacy has to be fundamentally protected by standards, regulations and laws.

## B. Lack of Transparency

In the context of cloud computing security, transparency refers to the willingness of a CSP to disclose various details on its security readiness. Some of these relevant details include policies on security, privacy, service level, etc. [14]. In addition to the willingness, when measuring transparency, it is important to observe how accessible the security readiness data and information are. No matter how much security facts about an organization are available, if they are not presented in an organized and easily understandable manner for CSUs and auditors, the transparency of the organization should still be rated relatively low.

CSUs and auditors need to know the types of security controls put in place by CSPs for their cloud infrastructure, but CSPs are often not willing to share this information. This is partially due to the fact that some of this information can be considered to consist of trade secret. For example, a lot of technical knowhow is involved in effectively storing and securing customer data, and it takes significant time and resources to reach the acceptable level of technical sophistication.

Therefore, CSUs and CSPs should negotiate on the information to be shared. Depending on the negotiation results, CSUs may decide not to use the services provided by the CSP. In fact, many CSUs choose not to use CSPs because of the frustration associated with this negotiation process and the resulting lack of transparency. For cloud computing to be more widely used, this challenge of transparency is one of the biggest obstacles to be removed.

## C. Virtualization Related Issues

Virtualization refers to the logical abstraction of computing resources from physical constraints. One representative example of virtualization technology is the virtual machine (VM). Virtualization can also be performed on many other computing resources, such as operating systems, networks, memory, and storage. In a virtualized environment, computing resources can be dynamically created, expanded, shrunk or moved according to users' demand, which greatly improves agility and flexibility, reduces costs and enhances business values for cloud computing [15].

In spite of its substantial benefits, this technology also introduces security and privacy risks in the cloud computing environment.

### 1) New Access Context

Virtualization brings new challenges to user authentication, authorization and accounting in terms of properly defining roles and policies [16]. Virtualization technology enables users to access their data and applications running on a single logical location which is usually the integration of multiple physical or virtual devices. The lack of security border and isolation introduces the possibility of information leakage [17]. Furthermore, such access can be done through a single user account logged on from diverse devices located anywhere in the world. This new access context raises many challenges, such as whether a user has the same privileges to access different physical or virtual devices; whether the accounts logged on from multiple distant geographic locations belong to the same user. Granular separation of user roles is required to address these challenges [16].

### 2) Attacks against Hypervisor

The hypervisor which manages multiple VMs becomes the target of attacks [16]. Different from physical devices which are independent from one another, VMs in the cloud are usually residing in one physical device managed by the same hypervisor. The compromise of the hypervisor therefore will put multiple VMs at risk. Furthermore, the immaturity of the hypervisor technology, such as isolation, access control, security hardening, etc., provides attackers with new ways to exploit the system. Diverse attacks against virtual machines are as follows.

*VM Hijacking*: When a VM is launched, the information required to invoke the VM is created and saved on the host. In the multi-tenant scenario, this information for all the VMs located in the same server will be stored on a common storage system. The attackers gaining access to this storage space will be able to break into the VMs, which is called VM Hijacking [18].

*VM Hopping*: If an attacker gains access over the hypervisor, he/she is able to manipulate the network traffic, configuration files, and even the connection status of the VMs located on top of the hypervisor [19, 20].

*VM Escape*: Attackers gaining access to the host running multiple VMs are able to access the resources shared by the VMs, and even bring down these resources and turn off the hypervisor [20].

*VM Mobility*: A VM can be copied over the network or through a USB, and the source configuration files are rec-

reated when the VM is moved to a new location. This way, the attackers are able to modify the configuration file as well as the VM's activities [19]. Furthermore, once a VM is infected and readmitted to its original host, the infection can potentially spread out to other VMs located on the same host. Such an attack is also known as a virtual library check-out [21].

*Dormant VMs*: VMs can exist in either active or dormant states. Although the dormant VMs may still hold sensitive user data, they can easily be overlooked and not updated with latest security settings, leading to potential information leakage [16].

### D. Multi-Tenancy Related Issues

Multi-tenancy is defined as "the practice of placing multiple tenants on the same physical hardware to reduce costs to the user by leveraging economies of scale" [22]. It indicates sharing of computational resources, storage, services and applications with other tenants, hosted by the same physical or logical platform at the provider's premises [23]. While the multi-tenancy architecture allows CSPs to maximize the organizational efficiency and significantly reduce a CSU's computing expenses, it does not come without costs. Adversaries taking advantage of the co-residency opportunities may launch diverse attacks against their co-residents, resulting in a number of security/privacy challenges [24].

Specifically, in the multi-tenant environment, different tenants' security controls are heterogeneous. The tenant with less security controls or misconfigurations is easier to compromise, which may serve as a stepping stone to the more secured tenants located in the same host. This could reduce the overall security level for all the tenants to that of the least secured one [16]. Furthermore, the security policies made by different tenants may disagree or even conflict with one another. Such disagreements or conflicts could introduce threats to tenants' needs, interests or concerns [25].

Furthermore, attackers taking advantage of the multi-tenancy architecture may be able to launch diverse attacks against their co-tenants, such as inferring confidential information or degrading co-tenants' performance.

Confidential information may be inferred via side-channel attacks. A side-channel attack is any attack based on information gained from the physical implementation of a system [26]. This type of attack primarily occurs due to covert channels with flawed access control policies that allow unauthorized access [27]. Some typical side channel attacks include: 1) timing attacks based on measuring the time it takes for a unit to perform operations [28], 2) power consumption attacks where the attacker can identify system processes by analyzing the power consumed by a unit while performing different operations [28], and 3) differential fault analysis where the attacker studies the behavior of a system by injecting faults into it

[28], 4) cache usage attacks where the attacker measures the utilization of CPU caches on its physical machine to monitor the activities on co-residents' activities [29], 5) load-based co-residence detection where the attacker measures the load variation of its co-resident to verify whether it is co-located with the target victim [29], and 6) estimating the traffic rates of the co-resident [29].

A co-resident's performance may be degraded by over-consuming computing resources, such as CPU, memory, storage space, I/O resources, etc. A Swiper attack is proposed in [30], with which the attacker uses a carefully designed workload to incur significant delays on the co-resident's targeted application. In [31], the authors propose and implement an attack which modifies the work-load of a victim VM in a way that frees up resources for the attacker's VM. The reason for the success of such attacks is that an overload created by one tenant may negatively impact the performance of another tenant [32].

### E. Managerial Issues

Most cloud-specific security and privacy challenges have their own managerial aspect. For example, the malicious insider challenge involves the problem of effectively managing employees to detect early warning signs and responding to policy violations in a timely manner once malicious insider incidents occur. These managerial challenges are non-technical in nature but also closely related to the technical solutions that could help cope with the corresponding technical challenges. Note that one of the biggest managerial challenges in cloud computing security is that all these technical solutions have to be managed eventually. Implementing a technical solution and not managing it properly are bound to introduce vulnerabilities. For example, security management for virtualization, which is dramatically unlike that of traditional networks, requires knowledge and skill sets beyond the capabilities of the general network administrator, leading to increased management complexity and risks [17]. Inappropriate VM management policies may cause the number of VMs to continuously grow while most of them are in the middle or sleep mode (i.e., VM sprawling), leading to the host machine's resource exhaustion [33]. We discuss the relationship between technical solutions and their managerial counterparts in Section IV.

Loss of control is another example of a managerial challenge dominating its associated technical challenges. The main source of the problem results from the fact that in-house managerial controls are not able to reach the computing and data resources managed by a CSP. The managerial challenge in this case is to develop a comprehensive and effective service level agreement (SLA) to extend the reach of the in-house security and privacy controls into the CSP organization. Often this effort leads to power struggles between CSUs and CSPs and becomes highly political, which require both technical and mana-

gerial expertise in order to arrive at a mutually beneficial solution for both CSUs and CSPs.

Finally, the lack of transparency challenge has its own strong managerial components. CSUs and CSPs must go through elaborate negotiations to acquire and provide essential information to ensure the security and privacy of the cloud services. An SLA also plays an important role in this challenge since it helps articulate and specify what information has to be available to satisfy the security and privacy needs of the CSU and the requirements imposed by laws and regulations.

The fact that managerial challenges are overarching and add to the other challenges is what makes it one of the toughest challenges to deal with. CSPs have to make a decision on the scope of their managerial effort in order not to exhaust their resources before all their most critical security and privacy goals and objectives are met.

## III. TAXONOMY OF EXISTING SOLUTIONS

Diverse defense studies have been launched to secure the cloud computing environment. In this section, we mainly focus on the state-of-the-art research that aims to address the security and privacy issues in cloud computing.

### A. Encryption Algorithms

At the current stage, encryption is still the major solution for addressing data confidentiality issues in cloud computing [34, 35]. Through encryption algorithms, sensitive information is encrypted and can only be accessed by users possessing the encryption keys. There are many encryption schemes available, including symmetric and asymmetric encryption methods [36–38]. El-etriby et al. [39] compared eight modern encryption methods in the context of cloud computing. When combined with compression, the encryption process can be more efficient as discussed in [40].

In encryption-based schemes, one critical question is which party should encrypt the data and manage the encryption keys.

CSUs can entirely rely on the CSP for their encryption needs. For example, Amazon Simple Storage Service (S3) encrypts a CSU's data by default. In this case, the problem is that CSUs lose the control over ensuring the confidentiality of their data. That is, a CSP now has full access to CSUs' data. Even if the CSP as a whole does not intend to do any harm to CSUs' data, there is also a risk associated with malicious insiders. A rogue employee of the CSP can always breach the confidentiality, integrity, and privacy of the CSUs' data.

CSUs can also encrypt their data by choosing any arbitrary encryption methods and manage the encryption keys by themselves. Many CSUs are using this approach today to protect their data. Homomorphic encryption [41]

is useful in this scenario because it allows CSPs to manage CSUs' data by providing services such as searches, correctness verification, and error localization [42], without having to decrypt it. Although promising, homomorphic encryption has its own disadvantages such as extra computational and bandwidth costs. Another weakness is exposed when attackers can detect certain patterns in the communications associated with operations using the homomorphic encryption [43].

Newly emerging cloud encryption methods take a step further in terms of key management. They do not allow any one party to take a full ownership of an encryption key. Instead, they divide the key into pieces, each of which is kept by CSU, CSP, and a third party data encryption service independently [44].

### B. Access Control

Access control, consisting of authentication, authorization, and accounting, is a way of ensuring that the access is provided only to the authorized users, hence the data is stored in a secure manner [45].

A number of research projects have been conducted to develop advanced access control techniques in terms of properly defining roles and policies [17, 21]. For example, a Role-Based Multi-Tenancy Access Control (RB-MTAC) model, which applies identity management to determine the user's identity and applicable roles, is designed to efficiently manage a user's access privilege to achieve application independence and data isolation [46]. In [47], the authors define and enforce access policies based on data attributes and allow the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. Furthermore, physical measures are also proposed to ensure the access control to the hypervisor or VMs. An example is a hardware token possessed by the administrator in order to launch the hypervisor [48].

### C. Third Party Auditing

Information system (IS) auditing refers to the activity of examining the checks, balances, and controls within an organization [49]. In this section we focus on the third-party audits (TPA), where CSUs and CSPs are not involved in the auditing process except for providing data and information for the independent auditors.

TPA can be used to relieve the concerns on data integrity, confidentiality, availability, and privacy. TPA can examine at least two aspects of data integrity: while data is in transit and while it is stationary. Regarding data confidentiality, how data is encrypted is the primary focus of TPA. In addition, TPA checks whether the CSP conforms to the SLAs, which can then be used to ensure data availability and privacy. TPA should also assess and evaluate

the overall security management practices of a CSP according to their impact on a specific audit focus, such as data integrity, confidentiality, availability, and privacy.

The Message Authentication Codes (MAC), when combined with encryption done by either CSP, CSU, or a third party, can provide a variable options for TPA to check the authenticity and integrity of files stored in the cloud against the source files [50, 51]. Although offering a reasonable auditing choice, the use of MAC by TPA introduces significant overhead. The main source of the overhead is the exchange of data between CSPs and TPA to validate MAC values. Ways to mitigate this overhead have been developed. One example approach is to simply exchange MAC values between TPA and CSPs rather than the file data itself. However, this method still requires intermittent file data transmissions.

TPA can also use other forms of authentication, such as Public Key Infrastructure (PKI), Kerberos, and Secure European System for Applications in a Multi-vendor Environment (SESAME) [52], but these authentication schemes by themselves do not provide integrity checks, unlike the approaches using MAC. In particular, Kerberos is designed to provide a single sign-on capability, which allows users to authenticate once and to be authenticated for a certain period of time without having to re-authenticate. SESAME is similar to Kerberos.

Due to the dynamic nature of data files, solutions are required to check the integrity of the data stored in the cloud. CSUs can download each data file segment, calculate MAC, and share the MAC with TPA, but this is not feasible mainly due to the processing burden imposed on the CSUs. The use of homomorphic verifiable tags (HVT) [53] can reduce this burden, but the weakness of this approach is that it only provides a partial coverage for data integrity checks. That is, it is still possible that data integrity is violated, and the integrity checks cannot detect it. A more complete solution to the dynamic data integrity check problem is available in the form of dynamic provable data possession (DPDP) protocols [54, 55]. DPDP-based approaches are more comprehensive because they cope with not only update data operations but also other data operations, such as insert and delete operations. The DPDP research leads to the rise of mechanisms using the Merkle hash tree (MHT) [56].

## D. Isolation

Due to the sharing of resources among disparate users in the multi-tenant cloud, attackers are able to launch diverse attacks against their co-tenants. There should be a certain level of isolation among tenants' data, computing and application processes. Specifically, such isolation should consider 1) segregation of VMs' storage, processing, memory and access path networks in IaaS, 2) segregation of running services and API calls as well as operating system level processes in PaaS, and 3) segrega-

tion of transactions carried out on the same instance by different tenants and tenants' data or information [15, 23]. With perfect performance isolation, the execution of one user's service should not interfere with the performance of another user.

Current studies handle isolation from several aspects. 1) Hypervisors or virtual machine monitor (VMM), a piece of computer software, firmware or hardware that creates and runs virtual machines, can be utilized to facilitate isolation. For example, the original development of the Xen hypervisor aimed to realize isolation [57]. 2) Some software-level resource management mechanisms are proposed to perform isolation for cache [58], disk [59], memory bandwidth [60], and network [61]. 3) Hardware-level solutions are proposed to allocate memory bandwidth [62] and processor caches [63] in a better way. 4) Strict mechanisms to separate customer data are required by cloud users [6]. 5) Security models are established to ensure isolation. In [64], the concept of tenant-ID is introduced on the data-link layer to securely segment, isolate and identify tenants and their assets in the cloud. The authors in [65] propose a security model and a set of principles to secure logical isolation between tenant resources in a cloud storage system.

## E. Soft Trust Solutions

Trust has been identified as one promising approach to address security and privacy issues in cloud computing [66]. However, due to the complex relationships among diverse parties involved in the cloud environment, establishing trust in cloud is not an easy task [67]. Specifically, 'soft' trust is defined as the relationship between two parties for a specific action or property. That is, one party believes that the other party will perform an action or possess a property. Current trust studies in cloud computing focus on several aspects.

Diverse trust models have been proposed to evaluate the trustworthiness of a CSP. For example, a dynamic trust evaluation approach based on multi-level Dirichlet distribution is proposed in [68]. The authors in [69] propose a formal trust management model which evaluates the trustworthiness of SaaS in a cloud computing environment by integrating various trust properties, such as direct trust, recommended trust, reputation factor, etc. A trust management model based on the fuzzy set theory is proposed in [70] to help cloud users select trustworthy CSPs. In [71], an extensible trust evaluation model is proposed to compute the trust of CSPs by integrating a time-variant comprehensive evaluation method for expressing direct trust and a space-variant evaluation method for calculating recommendation trust. A multi-tenancy trusted computing environment model (i.e., MTCEM) has been designed as a two-level hierarchy transitive trust chain model to assure a trusted cloud infrastructure to customers [72].

In addition, a number of studies also integrate trust mechanisms with existing technologies to address specific security and privacy challenges in cloud computing. In [73], a collaborative trust model of firewall-through is proposed to ensure the security of the cloud by combining the strength of a domain-based trust model and the feature of a firewall. In [74], a watermark-aware trusted running environment is proposed to ensure software running in the cloud.

## F. Hard Trust Solutions

In the cloud computing model, customer views are limited to a virtual infrastructure typically built on top of non-trusted physical hardware or operating environments. Hardware-based security solutions are envisioned as a natural trend that a CSP will be likely to follow in coming years to resolve different data privacy and integrity issues [75].

Specifically, the Trusted Computing Group (TCG) [76] proposed a set of hardware and software technologies to enable the construction of trusted platforms. Trusted computing is the industry's response to growing security problems in the enterprise and is based on hardware root trust. The TCG proposed a standard for the design of the trusted platform module (TPM) chip that is now bundled with commodity hardware. Currently, the TPM is the only standardized physical device to measure trust indicators in open platforms [77]. In general, TPM consists of three basic components, the root of trust for measurement, the root of trust for reporting, and the root of trust for storage [78]. In particular, TPM is designed for secure key generation, cryptographic operations, user authentication, and remote attestations. The TPM has been widely adopted to address security issues in the cloud. A trusted computing based Federated Identity Management (FIM) framework is proposed in [78] to solve the issue of identity theft in a cloud computing environment. In particular, the proposed method highlights the use of the TPM, virtual TPM (VTPM), OpenID protocols, and single sign-on (SSO) to support the tasks of authentication, authorization and identity federation in a trusted computing framework.

## G. Governance

Governance refers to a comprehensive set of activities associated with planning and implementing controls. In the context of cloud security, it is still too early to expect a mature governance framework to appear, but there are some initial signs of a cloud-specific security governance framework emerging. In particular, there are efforts being made to extend the existing security standards, such as Purchasing Card Industry-Data Security Standards (PCI-DSS) series by creating cloud security guidelines.

Another example is ISO/IEC 27000 series which provide an overall Information Technology (IT) security governance framework mainly specifying general IT security standards as well as how to certify organizations for being compliant with them. As of this writing, ISO/IEC is developing a new standard specifically addressing cloud-specific information security controls, which supplements the existing ISO/IEC 27000 series. This new standard will still be part of ISO/IEC 27000 series and be called ISO/IEC 27017. Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T) is collaborating with ISO/IEC to develop ISO/IEC 27017.

There are also special interest groups that are developing their own standards for cloud security governance. Cloud Security Alliance (CSA) is one of such organizations. The goal of CSA is slightly different from that of ISO/IEC 27017 in a sense that they are pursuing automated audit, assertion, and assurance. To accomplish this overarching goal, they plan to provide a "common interface and namespace that allows enterprises who are interested in streamlining their audit processes" [79].

Although the new standards are emerging, in terms of what practitioners can adopt and use, there is not much available today. It is largely up to individual cloud security professionals to acquire knowledge in cloud computing and cloud security and to apply that knowledge to govern various aspects of their cloud security. This is far from being ideal, but it is part of the growing pain the cloud industry has to go through to get to the next level of adoption.

## H. Summary

Based on the above discussions, we can classify the existing solutions according to three criteria: 1) solution adopter, which party can use the solution to address security/privacy issues, 2) reaction, whether the solution is used to prevent/predict the occurrence of attacks, or to respond to attacks after the occurrence, and 3) hardware or software, the solution addresses security/privacy challenges from hardware or software perspective. The detailed classification is summarized in Table 1.

## IV. SOLUTION COMPARISON AND OPEN RESEARCH ISSUES

In this section, we compare the existing solutions in terms of what challenges they can address and their limitations.

**Encryption:** Encryption can partially address the challenges associated with malicious insiders by preventing them from obtaining sensitive data and information in their readable format. However, encryption cannot be an ultimate solution to insider attacks since the insider may turn out to be a person who could legitimately decrypt the

**Table 1.** Classification of existing solutions

| | Solution adopter | | | Reaction | | Hardware/Software | |
|---|---|---|---|---|---|---|---|
| | **CSP** | **CSU** | **Third party** | **Proactive** | **Reactive** | **Hardware** | **Software** |
| Encryption | √ | √ | √ | √ | | | √ |
| Access control | √ | √ | | √ | | √ | √ |
| TPA | | | √ | | √ | | √ |
| Isolation | √ | | | √ | | | √ |
| Trust | √ | √ | √ | √ | | | √ |
| TPM | √ | | | √ | | √ | |
| Governance | | | √ | √ | | | √ |

TPA: third-party audits, TPM: trusted platform module.

encrypted data or information.

Encryption could be an effective solution to a loss of control situation. When a CSP is safeguarding a CSU's data, encryption could serve as an extra layer to prevent security breach. For the same reason, encryption helps with the multi-tenancy and virtualization challenges since it provides additional protection against a potential attempt from a tenant to steal the data or information belonging to another tenant who may be residing on the same physical machine.

Related to security management, encryption, in fact, generates more problems due to the additional complexity introduced by various cloud computing scenarios. For example, one apparent problem is deciding on who is responsible for doing the encryption. Is it the CSU, CSP, or third party? How should encryption keys be handled? Who has the right to decrypt the data? These questions are remaining to be answered by emerging research works in cloud computing security.

The major limitation of encryption algorithms is the encryption overhead, especially the computational burden. This burden becomes even bigger when the data to be encrypted is more dynamic in nature. For example, a log file is constantly updated, which will require an additional number of encryption attempts compared to more static files.

**Access Control:** By appropriately defining whether a user has the privilege to perform a given action on an object at a fine-grained level, access control schemes can be deployed by CSPs to effectively resist malicious insiders and DoS/DDoS attacks. Authentication and authorization models are developed to control users' access to the physical and virtual resources in the multi-tenant environment [80, 81]. In additions, CSUs can gain better control over their data/applications by designing their own access control policies [82].

The limitations of access control schemes are twofold. 1) Fine-grained access control schemes may introduce high complexity that limits their scalability. How to simultaneously achieve the goals of fine-grainedness and scalability for access control in cloud computing remains an open issue. 2) Access control architectures usually assume that the data owners and the data servers are in the same security domain, where the data servers are fully trusted to commit access control policies. However, this assumption may not hold in the cloud environment, where data owners and cloud servers are usually in two different security domains [47]. Even if perfect access control policies are made by the data owner, it is still highly risky that cloud servers may arbitrarily access the data by themselves or not strictly follow the policies to control the access from third parties. One feasible solution is to ensure the fulfillment of data owners' access control policies through other solutions, such as encryption.

**Third Party Auditing:** TPA is helpful with deterring malicious insider attacks. By auditing the activities of the employees, it is more probable for a security team to detect any suspicious activities indicating the existence of a malicious insider. Since auditing is typically done after the fact, TPA may not be able to detect DoS attacks in real time. However, there is an emerging trend to automate the auditing process, and the detection of DoS attacks could be one of the responsibilities of TPA, but the reporting of the attacks may still occur once they are over.

TPA can be a primary control to prevent loss of control since it can be used to assess and evaluate how much of the control over IT resources is truly transferred to a CSP when a CSU adopts cloud computing. Due to the ongoing nature of auditing, a CSU can effectively track the balance between its own control over the IT resources and that of a CSP.

TPA can also improve the transparency of a CSP by demanding more information on various aspects of CSP security readiness. How much information could be available to a CSU still depends on the CSP, but the leverage the CSU has in terms of purchasing the cloud services and offering revenue potentials for the CSP can have a significant impact on the degree of transparence to be demonstrated by the CSP.

TPA can partially handle multi-tenancy and virtualization challenges by helping to discover potential security breaches in the multi-tenancy and virtualization environments. Finally, TPA is an essential mechanism in managing security. Without auditing, it is impossible to do any type of security management.

The major limitation of TPA is its after-the-fact nature which makes it incapable of detecting an anomaly and reacting to it in real time. Furthermore, there are some areas of TPA that have not been heavily studied. For example, the auditing of data availability and access control problems, such as authorization and accountability, are largely missing in the discussions of the existing literature. This indicates much room for growth in terms of research in these topics.

**Isolation:** Isolation based schemes are mainly proposed to address security issues caused by multi-tenancy and virtualization. By creating dedicated logical devices for each single tenant, the isolation based schemes aim to ensure perfect isolation where one tenant's performance is not interfered with by other tenants running on the same physical hardware. However, due to the absence of physical isolation, smart attackers are still able to launch attacks penetrating the virtual boundaries among tenants [30]. Although extensive schemes are proposed to patch the vulnerabilities on the virtual boundaries [83-87], they are either application-specific or insufficient for fully mitigating the risk. At the current state of the art, there is no practical way to guarantee unconditional security except for physically isolating cloud users [29].

**Soft Trust:** The establishment of trust in the cloud could improve the detection of malicious behaviors, promote collaborations among trustworthy parties and further facilitate the broad adoption of cloud computing technology. Specifically, trust based solutions can detect and prevent malicious insiders through the evaluation of insiders' trustworthiness. Through the establishment of trust, CSUs will be more confident about CSPs' protection of their data, and the concerns about loss of control can be relieved. There are efforts being made to establish a reputation profile for CSPs based on CSUs' experiences. Such a reputation profile provides an effective way to improve a CSP's transparency. Furthermore, through the evaluation of users' trustworthiness, trust-based solutions can reduce the risks of multi-tenancy and virtualization by excluding users of low trustworthiness from the resource sharing environment.

There are also some limitations of current trust-based schemes. 1) While extensive studies have been conducted on evaluating a CSP's trustworthiness, the evaluations on CSUs, computing resources and other entities in the cloud are still in their initial stage. 2) Trust evaluation criteria in different studies are not consistent. The lack of standardized evaluation criteria makes it extremely difficult to compare different trust evaluation results. 3) Entities' trustworthiness is mainly evaluated qualitatively. Quanti-

tative trust computation algorithms are required to accurately evaluate and compare the reliability of entities. 4) Current schemes are mostly ad-hoc, which can only partially ensure the cloud security and privacy [88]. A unified framework which integrates comprehensive trust evaluations on diverse entities involved in the cloud environment is on demand. Advanced trust-based solutions are under investigations to address such limitations.

**Hard Trust (TPM):** TPM serves as a physical device to measure trust indicators in open platforms. It is bundled with commodity hardware that provides great flexibility in addressing some common security issues in cloud computing (e.g., restricting malicious insiders, access control in a multitenant environment, etc.). The success of cloud computing heavily depends on how comfortable the customers are in outsourcing their sensitive data, losing control, and relying on the CSP's security controls. The CSUs need assurances from CSPs before the actual migration. TPM can play a vital role in strengthening the customer's trust by providing strong assurances about the integrity of their data and the cloud infrastructure.

TPM can be effectively used to prevent insiders from performing different malicious activities such as gaining access to customers' confidential information or accessing the shared resources without proper authorization, etc. In particular, TPM provides a federated identity management framework with a single sign-on to support the tasks of authentication, authorization, and identity federation in a trusted computing framework. The implementation of TPM at the service provider level provides both local and remote user authentication protocols that serve as the first layer of defense against the malicious insiders.

TPM can effectively protect both platform and information integrity in the multi-tenant environment through a remote authentication mechanism with hardware-based attestation capabilities. Furthermore, in a virtualized environment where multiple operating systems run concurrently, VTMP provides an effective solution to facilitate the secure migration of virtual machines between similar and different platforms. Moreover, TPM-based authentication protocols provide both the elements of trust (e.g., establishing the trusted log between the communication parties) and privacy for secure authentication and platform integrity in the cloud.

Since TPM was originally designed to provide security guarantees on a single node, performance can suffer in a distributed environment, such as cloud data centers where multiple operating systems, applications, and cloud services run concurrently. Cloud services are expected to be highly scalable at run time, which becomes an issue when TPM is used as a primary security measure. Moreover, TPM allows customers to remotely verify data integrity or perform remote attestation, which can overexpose the cloud infrastructure and provide valuable information to outsiders. The external attackers can make use of this

**Table 2.** Security & privacy challenges vs. solutions

| | LoC | LoT | Multi-tenancy | Virtualization | Management |
|---|:---:|:---:|:---:|:---:|:---:|
| Encryption | √ | | √ | √ | √ |
| Access control | √ | | √ | √ | |
| TPA | √ | √ | √ | √ | √ |
| Isolation | | | √ | √ | |
| Trust | √ | √ | √ | √ | |
| TPM | | | √ | √ | |
| Governance | | | | | √ |

TPA: third-party audits, TPM: trusted platform module, LoC: loss of control, LoT: lack of transparency.

information to trace the potential vulnerabilities in the infrastructure and set up the actual attack.

**Governance:** Governance solutions mainly address the managerial challenges in cloud security. However, all the technical solutions to the technology-centric cloud security challenges are also dependent on how well the technical countermeasures are managed in one way or another. For example, the managerial aspect of encryption is critical. If users do not safeguard their encryption keys, whether data is encrypted or not does not matter anymore. A similar situation arises for the strength of encryption keys.

Access control is also heavily dependent on management. To develop an efficient access control list, it is crucial to first develop proper policies and identify what to protect. Prioritization is another important facet of access control since not every asset can be protected. Developing policies, enumerating assets, and prioritizing them all require human intervention, which is part of the security management process.

Human auditors are at the forefront of TPA. It may be possible to collect some information automatically, but a significant portion of TPA is conducted by human auditors. They interview relevant personnel in an organization being audited, who can, in turn, collect either manually or automatically generated data for the auditors. Audit report writing is another part of TPA, which cannot afford full automation. Auto-generated audit reports are possible, but they could be overwhelming in terms of the amount of data being presented. An auditor still needs to sift through the data to emphasize more relevant data while deleting unimportant data. In addition, an in-depth analysis section of the audit report cannot be automatically generated.

Different isolation levels can be set to separate a VM from its neighboring VMs. If the VMs are from different CSUs who specify strong isolation in the SLAs, it is necessary for CSPs to strive to set the isolation level of the VM to its maximum degree. However, human errors can still occur and misconfiguration is possible. Therefore, management is an important factor here, too.

Trust is partially related to TPA. The auditing can also be done by internal auditors. Whether conducted internally or externally, the auditing process should be managed well to produce meaningful results. Positive audit results over an extended period of time form a basis of building trust between CSUs and CSPs. Most of the trust model services that are available today involves auditors compiling and analyzing audit results to make an objective security assessment of a CSP. Therefore, management activities are again indispensable in the context of trust. Since the scope of security governance is overwhelming, managing expectations and prioritizing various governance activities themselves become a challenge. In addition, as mentioned in Section II-E, one of the biggest deficiencies in cloud security governance today is a lack of cloud-specific governance frameworks. However, this deficiency is slowly and partially being addressed by newly emerging standards addressing cloud-specific governance concerns, such as ISO/IEC 27017.

**Summary:** We summarize the relationship between security/privacy challenges and the existing solutions in Table 2, where each row represents a specific solution, and each column represents one security/privacy challenge. The cell in row *m* and column *n* is checked if solution *m* can be used to address or partially address the challenge *n*.

## V. FUTURE DIRECTIONS

As an emerging and rapidly developing computing scenario, cloud computing has introduced a number of challenges. In this paper, we have analyzed some critical security and privacy challenges in cloud computing, categorized diverse existing solutions, and have compared their strengths and limitations. Based on the discussions, we envision three future research directions to secure the cloud environment.

First, the development of advanced solutions to address the management-oriented security/privacy challenges is urgent. From Table 2, we can observe that the lack of

transparency and management issues are two remaining challenges which are not covered by many existing solutions. Different from other challenges, which are technique-oriented, these two challenges are more management-oriented. While security/privacy threats from both technique and management aspects may cause severe damage to the cloud environment, most of current studies only focus on the technique-oriented challenges. There is a lack of advanced solutions to deal with the security/privacy issues from the management perspective.

Second, the integration of multiple solutions from different categories provides a great potential to address security/privacy issues that cannot be addressed by a single, ad-hoc security solution.

For example, by integrating encryption and access control, CSUs are able to ensure the fulfillment of their access control policies on the cloud server [47, 82, 89]. By integrating trust models with encryption schemes, CSUs can protect their data confidentiality by only allowing trustworthy CSPs to decrypt and process their sensitive data [90]. Privacy cheating can be discouraged by bridging secure storage and secure computation auditing in the cloud [91, 92]. However, how to seamlessly integrate different security solutions remains an open challenge.

Third, stimulating the security cooperation among diverse stakeholders, including CSP, CSU and many third parties, in the cloud scenario is very challenging. The involvement of diverse parties in the cloud makes the security/privacy issues complicated since security objectives for different parties can be very different, and sometimes these objectives may even conflict with one another. For example, a CSU may require CSPs to be more transparent about their security controls so that it can choose the most secure CSP. Nevertheless, a CSP may need to protect its entire cloud infrastructure by not revealing details about its security settings. Establishing trust relationships among diverse parties, which enables negotiation and tradeoffs, may serve as a promising solution.

While cloud computing is rapidly gaining popularity, diverse security and privacy issues are emerging against this new computing paradigm. However, the development of security and privacy solutions is lagging behind. Research challenges as well as opportunities are remaining. The resolution of these security and privacy issues will serve as the key to enable the rapid adoption of cloud computing.

## REFERENCES

1. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. P. Viswanathan, "Cloud computing – Is it really all that beneficial?" http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm.
3. F. Gens, "New IDC IT cloud services survey: top benefits and challenges," 2009; http://blogs.idc.com/ie/?p=730.
4. D. Sheppard, "Is loss of control the biggest hurdle to cloud computing?" 2014; http://www.itworldcanada.com/blog/is-loss-of-control-the-biggest-hurdle-to-cloud-computing/95131.
5. Top Threats Working Group, "The notorious nine: cloud computing top threats in 2013," 2013; https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
6. Independently Conducted by Ponemon Institute LLC, "Achieving Data Privacy in the Cloud," 2012; http://download.microsoft.com/download/F/7/6/F76BCFD7-2E42-4BFB-BD20-A6A1F889435C/Microsoft_Ponemon_Cloud_Privacy_Study_Germany.pdf.
7. J. R. Raphael, "The worst cloud outages of 2013 (so far)," 2013; http://www.infoworld.com/article/2606768/cloud-computing/107783-The-worst-cloud-outages-of-2013-so-far.html.
8. S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in *Proceedings of 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom),* Indianapolis, IN, 2010, pp. 693-702.
9. A. Murphy, "Storing data in the cloud raises compliance challenges," 2012; http://www.forbes.com/sites/ciocentral/2012/01/19/storing-data-in-the-cloud-raises-compliance-challenges/.
10. R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, Chicago, IL, 2009, pp. 85-90.
11. R. Maggiani, "Cloud computing is changing how we communicate," in *Proceedings of IEEE International Professional Communication Conference (IPCC 2009)*, Waikiki, HI, 2009, pp. 1-4.
12. S. Condon, "FTC questions cloud-computing security," 2009; http://www.cnet.com/news/ftc-questions-cloud-computing-security/.
13. R. Singel, "NetFlix cancels recommendation contest after privacy lawsuit," 2010; http://www.wired.com/2010/03/netflix-cancels-contest.
14. W. Pauley, "Cloud provider transparency: an empirical evaluation," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 32-39, 2010.
15. B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proceedings of 5th International Joint Conference on INC, IMS and IDC (NCM'09)*, Seoul, Korea, 2009, pp. 44-51.
16. Virtualization Special Interest Group and PCI Security Standards Council, "PCI DSS Virtualization Guidelines," 2011; https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.
17. X. Luo, L. Yang, L. Ma, S. Chu, and H. Dai, "Virtualization security risks and solutions of Cloud Computing via divide-conquer strategy," in *Proceedings of 2011 3rd International Conference on Multimedia Information Networking and Security (MINES)*, Shanghai, China, 2011, pp. 637-641.
18. A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," in *Proceedings of 2010 IEEE Interna-*

*tional Carnahan Conference on Security Technology (ICCST)*, San Jose, CA, 2010, pp. 35-41.

19. D. Hyde, "A survey on the security of virtual machines," 2009; http://www.cs.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf.

20. K. Owens, "Securing virtual compute infrastructure in the cloud," Savvis Inc., Town and Country, MO, 2009.

21. M. Zheng, "Virtualization security in data centers and clouds," 2011; http://www.cse.wustl.edu/~jain/cse571-11/ftp/virtual/.

22. W. J. Brown, V. Anderson, and Q. Tan, "Multitenancy-security risks and countermeasures," in *Proceedings of 2012 15th International Conference on Network-Based Information Systems (NBiS)*, Melbourne, Australia, 2012, pp. 7-13.

23. A. Behl and K. Behl, "An analysis of cloud computing security issues," in *Proceedings of 2012 World Congress on Information and Communication Technologies (WICT)*, Trivandrum, India, 2012, pp. 109-114.

24. K. Wood and M. Anderson, "Understanding the complexity surrounding multitenancy in cloud computing," in *Proceedings of 2011 IEEE 8th International Conference on e-Business Engineering (ICEBE)*, Beijing, China, pp. 119-124.

25. P. Sun, Q. Shen, L. Gu, Y. Li, S. Qing, and Z. Chen, "Multilateral security architecture for virtualization platform in multi-tenancy cloud environment," in *IEEE Conference Anthology*, China, 2013, pp. 1-5.

26. H. Aljahdali, P. Townend, and J. Xu, "Enhancing multi-tenancy security in the cloud IaaS model over public deployment," in *Proceedings of 2013 IEEE 7th International Symposium on Service Oriented System Engineering (SOSE)*, Redwood City, CA, 2013, pp. 385-390.

27. A. A. Almutairi, M. I. Sarfraz, S. Basalamah, W. G. Aref, and A. Ghafoor, "A distributed access control architecture for cloud computing," *IEEE Software*, vol. 29, no. 2, pp. 36-44, 2011.

28. F. X. Standaert, "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*. New York, NY: Springer, pp. 27-42, 2010.

29. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, IL, 2009, pp. 199-212.

30. R. Chiang, S. Rajasekaran, N. Zhang, and H. Huang, "Swiper: exploiting virtual machine vulnerability in third-party clouds with competition for I/O resources," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 6, pp. 1732-1742, 2014.

31. V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, and M. M. Swift, "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, Raleigh, NC, 2012, pp. 281-292.

32. C. Momm and W. Theilmann, "A combined workload planning approach for multi-tenant business applications," in *Proceedings of 2011 IEEE 35th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, Munich, Germany, 2011, pp. 255-260.

33. S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," in *Proceedings of*

*2011 International Conference on Cloud and Service Computing (CSC)*, Hong Kong, 2011, pp. 174-179.

34. L. Abate, "Top 5 security challenges of cloud storage," 2010; http://www.nasuni.com/89-top_5_security_challenges_of_cloud_storage/.

35. Y. Peng, W. Zhao, F. Xie, Z. Dai, Y. Gao, and D. Chen, "Secure cloud storage based on cryptographic techniques," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, sup. 2, pp. 182-189, 2012.

36. A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds," *ACM Transactions on Storage (TOS)*, vol. 9, no. 4, article no. 12, 2013.

37. G. Danezis and B. Livshits, "Towards ensuring client-side computational integrity," in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, Chicago, IL, 2011, pp. 125-130.

38. B. R. Sekhar, B, S. Kumar, L. S. Reddy, and V. PoornaChandar, "CP-ABE based encryption for secured cloud storage access," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, pp. 1-5, 2012.

39. S. El-etriby, E. M. Mohamed, and H. S. Abdul-kader, "Modern encryption techniques for cloud computing," in *Proceedings of International Conference on Communications and Information Technology (ICCIT2012)*, Hammamet, Tunisia, 2012, pp. 800-805..

40. S. Sajithabanu and E. G. P. Raj, "Data storage security in cloud," *IJCST*, vol. 2, no. 4, pp. 436-440, 2011.

41. A. A. Atayero and O. Feyisetan, "Security issues in cloud computing: the potentials of homomorphic encryption," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no 10, pp. 546-552, 2011.

42. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proceedings of 17th International Workshop on Quality of Service (IWQoS)*, Charleston, SC, 2009, pp. 1-9.

43. C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1467-1479, 2012.

44. Y. Song, H. Kim, and A. Mohaisen, "A private walk in the clouds: Using end-to-end encryption between cloud applications in a personal domain," in *Trust, Privacy, and Security in Digital Business*. Switzerland, Springer International Publishing, pp. 72-82, 2014.

45. A. O. Joseph, J. W. Kathrine, and R. Vijayan, "Cloud security mechanisms for data protection: a survey," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 9, pp. 81-90, 2014.

46. S. J. Yang, P. C. Lai, and J. Lin, "Design role-based multi-tenancy access control scheme for cloud services," in *Proceedings of 2013 International Symposium on Biometrics and Security Technologies (ISBAST)*, Chengdu, China, 2013, pp. 273-279.

47. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proceedings 2010 IEEE INFOCOM*, San Diego, CA, 2010, pp. 1-9.

48. K. Scarfone, M. Souppaya, and P. Hoffman, *Guide to Secu-*

rity for Full Virtualization Technologies. Gaithersburg, MD: National Institute of Standards and Technology, 2011.

49. R. Weber, *EDP Auditing: Conceptual Foundations and Practice*, 2nd ed. New York, NY: McGraw-Hill, 1988.

50. C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," *IEEE Network*, vol. 24, no. 4, pp. 19-24, 2010.

51. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362-375, 2013.

52. T. A. Parker, "A secure European system for applications in a multi-vendor environment (the SESAME project)," in *Information Security*. London: Chapman & Hall, pp. 139-156, 1993.

53. N. Y. Lee and Y. K. Chang, "Hybrid provable data possession at untrusted stores in cloud computing," in *Proceedings of 2011 IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS)*, Tainan, 2011, pp. 638-645.

54. C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," *ACM Transactions on Information and System Security (TISSEC)*, vol. 17, no. 4, article no. 15, 2015.

55. M. T. Goodrich, R. Tamassia, and A. Schwerin, "Implementation of an authenticated dictionary with skip lists and commutative hashing," in *Proceedings of DARPA Information Survivability Conference & Exposition II (DISCEX'01)*, Anaheim, CA, 2001, pp. 68-82.

56. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proceedings of 14th European Symposium on Research in Computer Security*, Saint-Malo, France, 2009, pp. 355-370.

57. P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," *ACM SIGOPS Operating Systems Review*, vol. 37, no. 5, pp. 164-177, 2003.

58. H. Raj, R. Nathuji, A. Singh, and P. England, "Resource management for isolation enhanced cloud services," in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, Chicago, IL, 2009, pp. 77-84.

59. A. Gulati, A. Merchant, and P. J. Varman, "mClock: handling throughput variability for hypervisor IO scheduling," in *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, Vancouver, Canada 2010, pp. 1-7.

60. B. Verghese, A. Gupta, and M. Rosenblum, "Performance isolation: sharing and isolation in shared-memory multiprocessors," *ACM SIGPLAN Notices*, vol. 33, no. 11, pp. 181-192, 1998.

61. A. Shieh, S. Kandula, A. Greenberg, and C. Kim, "Seawall: performance isolation for cloud datacenter networks," in *Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing*, Boston, MA, 2010.

62. N. Rafique, W. T. Lim, and M. Thottethodi, "Effective management of DRAM bandwidth in multicore processors," in *Proceedings of 16th International Conference on Parallel Architecture and Compilation Techniques (PACT2007)*, Brasov, Romania, 2007, pp. 245-258.

63. K. J. Nesbit, J. Laudon, and J. E. Smith, "Virtual private caches," *ACM SIGARCH Computer Architecture News*, vol. 35, no. 2, pp. 57-68, 2007.

64. S. Jeuk, S. Zhou, and M. Rio, "Tenant-id: tagging tenant assets in cloud environments," in *Proceedings of 2013 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*, Delft, the Netherlands, 2013, pp. 642-647.

65. M. Factor, D. Hadas, A. Hamama, N. Har'El, E. K. Kolodner, A. Kurmus, A. Shulman-Peleg, and A. Sorniotti, "Secure logical isolation for multi-tenancy in cloud storage," in *Proceedings of 2013 IEEE 29th Symposium on Mass Storage Systems and Technologies (MSST)*, Long Beach, CA, 2013, pp. 1-5.

66. L. Q. Tian, C. Lin, and Y. Ni, "Evaluation of user behavior trust in cloud computing," in *Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM)*, Taiyuan, China, 2010, pp. 567-572.

67. H. Sato, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," in *Proceedings of 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT)*, Seoul, Korea, 2010, pp. 121-124.

68. Z. Yang, X. Qin, Y. Yang, and W. Li, "A new dynamic trust approach for cloud computing," in *Proceedings of the International Workshop on Cloud Computing and Information Security (CCIS2013)*, Shanghai, China, 2013.

69. S. K. Prajapati, S. Changder, and A. Sarkar, "Trust management model for cloud computing environment," in *Proceedings of the International Conference on Computing, Communication and Advanced Network (ICCCAN2013)*, Nassau, Bahamas, 2013, pp. 1-5.

70. X. Sun, G. Chang, and F. Li, "A trust management model to enhance security of cloud computing environments," in *Proceedings of 2011 Second International Conference on Networking and Distributed Computing (ICNDC)*, Beijing, China, 2011, pp. 244-248.

71. Q. Guo, D. Sun, G. Chang, L. Sun, and X. Wang, "Modeling and evaluation of trust in cloud computing environments," in *Proceedings of 2011 3rd International Conference on Advanced Computer Control (ICACC)*, Harbin, China, 2011 pp. 112-116.

72. X. Y. Li, L. T. Zhou, Y. Shi, and Y. Guo, "A trusted computing environment model in cloud architecture," in *Proceedings of 2010 International Conference on Machine Learning and Cybernetics (ICMLC)*, Qingdao, China, 2010, pp. 2843-2848.

73. Z. Yang, L. Qiao, C. Liu, C. Yang, and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing," in *Proceedings of 2010 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Shanghai, China, 2010, pp. 329-334.

74. J. Fu, C. Wang, Z. Yu, J. Wang, and J. G. Sun, "A watermark-aware trusted running environment for software clouds," in *Proceedings of 2010 Fifth Annual ChinaGrid Conference (ChinaGrid)*, Guangzhou, China, 2010, pp. 144-151.

75. W. Itani, A. Kayssi, and A. Chehab, "Hardware-based security for ensuring data privacy in the cloud," in *Security Engineering for Cloud Computing: Approaches and Tools: Approaches and Tools*. Hershey, PA: IGI Global, pp. 147-

170, 2013.

76. Trusted computing Group, "Trusted computing," http://www.trustedcomputinggroup.org/trusted_computing.

77. M. Achemlal, S. Gharou, and C. Gaber, "Trusted platform module as an enabler for security in cloud computing," in *Proceedings of 2011 Conference on Network and Information Systems Security (SAR-SSI),* La Rochelle, France, 2011, pp. 1-6.

78. E. Ghazizadeh, M. Zamani, J. L. Ab Manan, and M. Alizadeh, "Trusted computing strengthens cloud authentication," *The Scientific World Journal*, vol. 2014, article id. 260187, 2014.

79. CloudAudit Working Group, https://cloudsecurityalliance.org/group/cloudaudit/.

80. Z. Zhang and Q. Wen, "An authorization model for multitenancy services in cloud," in *Proceedings of 2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS),* Hangzhou, China, pp. 260-263.

81. N. H. Bien and T. D. Thu, "Hierarchical multi-tenant pattern," in *Proceedings of 2014 International Conference on Computing, Management and Telecommunications (ComManTel),* Da Nang, Vietnam, 2014, pp. 157-164.

82. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Automata, Languages and Programming.* Heidelberg, Germany: Springer, pp. 579-591, 2008.

83. D. A. Osvik, A. Shamir, and E. Tromer, "Cache attacks and countermeasures: the case of AES," in *Topics in Cryptology–CT-RSA 2006.* Heidelberg, Germany: Springer, pp. 1-20, 2006.

84. D. Page, "Theoretical use of cache memory as a cryptanalytic side-channel," Department of Computer Science, University of Bristol, UK, 2002.

85. D. Page, "Defending against cache-based side-channel attacks," *Information Security Technical Report*, vol. 8, no. 1, pp. 30-44, 2003.

86. D. Page, "Partitioned cache architecture as a side-channel defence mechanism," Department of Computer Science, University of Bristol, UK, 2005.

87. C. Percival, "Cache missing for fun and profit," 2005; http://css.csail.mit.edu/6.858/2011/readings/ht-cache.pdf.

88. S. M. Habib, S. Hauke, S. Ries, and M. Mühlhäuser, "Trust as a facilitator in cloud computing: a survey," *Journal of Cloud Computing*, vol. 1, no. 1, pp. 1-18, 2012.

89. S. De Capitani Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," in *Proceedings of the 33rd International Conference on Very Large Data Bases*, Vienna, Austria, 2007, pp. 123-134.

90. Y. Liu, J. Ryoo, and S. Rizvi, "Ensuring data confidentiality in cloud computing: an encryption and trust-based solution," in *Proceedings of 2014 23rd Wireless and Optical Communication Conference (WOCC),* Newark, NJ, 2014, pp. 1-6.

91. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371-386, 2014.

92. L. Wei, H. Zhu, Z. Cao, W. Jia, and A. V. Vasilakos, "Seccloud: bridging secure storage and computation in cloud," in *Proceedings of 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops (ICDCSW),* Genova, Italy, 2010, pp. 52-61.

## Yuhong Liu

Yuhong Liu is an assistant professor of Information Science Technology at Pennsylvania State Altoona. She received her Ph.D. degree in Computer Engineering from University of Rhode Island in 2012. She is the recipient of the 2013 University of Rhode Island Graduate School Excellence in Doctoral Research Award. Her research interests include: online social network security, trust management in cyber-physical systems and trustworthy cloud computing. Her work on securing online reputation systems received the best paper award at the IEEE International Conference on Social Computing 2010 (acceptance rate = 13%).

## Yan (Lindsay) Sun

Yan (Lindsay) Sun received her B.S. degree with the highest honor from Peking University in 1998, and the Ph.D. degree in electrical and computer engineering from the University of Maryland in 2004. She joined the University of Rhode Island in 2004, where she is currently an associate professor in the department of Electrical, Computer and Biomedical Engineering. Dr. Sun is an elected member of the Information Forensics and Security Technical Committee (IFS-TC), in IEEE Signal Processing Society. She also serves on the editorial broad of IEEE Security and Privacy Magazine. She is an associate editor of Signal Processing Letter since 2013, and an associate editor of Inside Signal Processing eNewsletter since 2010. Dr. Sun's research interests include power grid security, trustworthy social computing, wireless network security, and reliable biomedical systems. She applied signal processing techniques in modeling, detection, and estimation of abnormal behaviors in various computing and communication systems. Dr. Sun received the best paper awards at the IEEE International Conference on Communications (ICC'14) and the IEEE International Conference on Social Computing (SocialCom'10). She was the recipient of NSF CAREER Award.

## Jungwoo Ryoo

Jungwoo Ryoo is an associate professor of Information Sciences and Technology (IST) at the Pennsylvania State University-Altoona. Ryoo is also a graduate/affiliated faculty member of the college of IST at Penn State. He is a technical editor for the IEEE Communications Magazine and also working with IEEE and Software Engineering Institute (SEI) as a consultant. His research interests include information security and assurance, software engineering, and computer networking. He is the author of numerous academic articles and conducts extensive research in software security, network/cyber security, security management (particularly in the government and medical sector) and auditing (especially in cloud computing), and software architectures. Many of Ryoo's research projects have been funded by both state and federal government agencies. He also has substantial industry experience in architecting and implementing secure, high-performance software for large-scale network management systems. He received his Ph.D. in Computer Science from the University of Kansas in 2005.

## Syed Rizvi

Syed Rizvi is an Assistant Professor of Information Sciences and Technology at the Pennsylvania State University - Altoona. He received his doctorate in Modeling and Simulation from the University of Bridgeport in 2010. His research interests lie at the intersection of computer networking, information security and modeling and simulation. Recently, he has been working on security issues in cloud computing, cognitive radios for wireless communications, and modeling and simulation of large-scale networks. His expertise includes the design, analysis, implementation, optimization, and comparisons of algorithms in the areas of wireless/multiuser communications, information security, and parallel/distributed systems. He has authored and coauthored several technical refereed and non-refereed papers in various international conferences, journal articles, and book chapters in research and pedagogical techniques. He is a member of IEEE Communications Society and the ACM.

## Athanasios V. Vasilakos

Athanasios V. Vasilakos is recently Guest Professor with Lulea University of Technology. He served or is serving as an Editor for many technical journals, such as the IEEE Transactions on Network and Service Management; IEEE Transactions on Cloud Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cybernetics; IEEE Transactions on Nanobioscience; IEEE Transactions on Information Technology Biomedicine; ACM Transactions on Autonomous and Adaptive Systems; the IEEE Journal on Selected Areas in Communications (May 2009, Jan 2011, March 2011 issues). He is also General Chair of the European Alliances for Innovation (www.eai.eu).