Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Taxonomy for Identification of Security Issues in Cloud Computing Environments

Monjur Ahmed & Alan T. Litchfield

To cite this article: Monjur Ahmed & Alan T. Litchfield (2018) Taxonomy for Identification of Security Issues in Cloud Computing Environments, Journal of Computer Information Systems, 58:1, 79-88, DOI: 10.1080/08874417.2016.1192520

To link to this article: https://doi.org/10.1080/08874417.2016.1192520

Published online: 27 Sep 2016.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
2018, VOL. 58, NO. 1, 79–88
https://doi.org/10.1080/08874417.2016.1192520

Taylor & Francis
Taylor & Francis Group

Taxonomy for Identification of Security Issues in Cloud Computing Environments

Monjur Ahmed and Alan T. Litchfield

Auckland University of Technology, Auckland, New Zealand

ABSTRACT
The emergence of Cloud Computing and consequential changes to infrastructure and work practices leaves little doubt that most computing platforms will be impacted by increased security concerns. Therefore, within the context of a security framework, issues surrounding the exploitation of hard or soft network elements in a Cloud architecture need to be acknowledged. To be applicable to any Cloud architecture, such a framework needs to play a role within the operational context of Cloud Computing. The framework is presented as a taxonomy of security threats specific to Cloud Computing environments.

KEYWORDS
Cloud Computing; security; Cloud architecture; Cloud threat taxonomy

Introduction

As a means of making computing resources available by overcoming geographic constraints, Cloud Computing demonstrates a trend toward an increased use of network and Internet-based computing [22]. In general, it may be said that any computer network may suffer from network security issues [34]. Since Cloud Computing comprises distributed networks, the computing environment in a Cloud scenario is prone to the same risks as any other computer network. Also, new technologies provide new vectors for attackers to exploit. In this context, if prevention or mitigating steps do not already exist, then an increased risk of damage is likely [79]. Consequently, we contend that systems operators and service consumers do not sufficiently comprehend new or Cloud-specific threats. That such threats need to be more thoroughly researched and therefore, it is important for a researcher to have a mechanism for asserting hypotheses in Cloud security researches.

In this article, we present an analysis of contemporary security issues that threaten Cloud Computing environments. To assist researchers that are considering risks and threats, we present a taxonomy developed by applying the intuitive approach of a heuristic methodology [54]. The methodology used to develop the taxonomy in [52] has been applied in prior research, for example, a taxonomy of health IT and medication adherence [52], the taxonomy of Ambient Assisted Living [7], and a taxonomy of industrial service systems enabled by digital product innovation [35]. The intuitive approach of the heuristic methodology is an ad hoc approach. To develop the taxonomy in this approach, researchers use their perception and understanding of objects to be classified. This approach does not entail any explicit method [54]. To verify the taxonomy, it is applied to a number of cases of Cloud breaches.

Core concepts of Cloud Computing include the notion that the Cloud service provider carries the infrastructural burden and that the service consumer “rents” remote hard and/or soft computing resources [2]. That is, the consumer pays the service provider the cost of building and maintaining appropriate infrastructure plus any premium for additional services and perceived value. In general, it may be argued that the burden or responsibility to preserve the safety of systems and data may thus rest with the service provider [64]. However, it may also be shown that service providers would seek to pass off responsibility to the service consumer and that such a passing off effectively equips the consumer with sufficient tools only to fail.

It is assumed that a means to enable user access to remote resources and that the transfer of personal data between end user and Cloud server exist [65]. Additionally, service and application providers frequently ask customers for access to personal data. We argue that the nature of Cloud Computing exacerbates the illegitimate exposure of personal data to third parties either when in transition or stored in remote servers. Security concerns in Cloud Computing applications also challenge claims of reliability and integrity [37] and this highlights concerns about the retention of privacy among Cloud users; [81] therefore, Cloud Computing practices are included in our analysis.

In Cloud Computing, virtualization is significantly embedded as a foundation technology. Virtualization refers to how computing resources, for example, hardware, software, and storage, are shared across instances or aggregated. Sharing allows a single resource to be made available to multiple virtual resources and aggregation allows multiple resources to be used as a single virtual resource [47]. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) [36] defines a virtual system as a computer system composed of virtual resources that may include hosted resources; storage, processing, memory, and networking. Other terms used in the computing industry may include virtual machine, hosted computer, child partition, logical partition, domain, guest virtual machine, and container.

CONTACT Alan T. Litchfield alan.litchfield@aut.ac.nz Auckland University of Technology, Service and Cloud Computing Research Lab, Private Bag 92006, Wellesley Street, Auckland 1142, New Zealand.

The ISO/IEC defines a hypervisor as a virtualization platform, which is a platform that supports virtual systems [36]. So, a hypervisor supports computer systems that are themselves composed of virtual resources. Thus, virtualization management is provided by the hypervisor [80].

To provide a sound epistemological foundation for the study, existing research is used to develop the taxonomy. For example in [28], threat-specific viewpoints presented are architectural, compliance, and privacy issues. In [32], a security taxonomy for Cloud Computing presents four categories as follows: infrastructure, application, platform, and administration. Other research categorizes Cloud Computing threats as responsibility ambiguity, protection inconsistency, evolutional risks, supplier lock-in, business discontinuity, license risks, bylaw conflicts, bad integration, hypervisor isolation failure, service unavailability, data unreliability, abuse of rights of the Cloud service provider, shared environment, and use of insecure Application Program Interfaces (APIs) [45].

We note that as well as from traditional network threats, Cloud Computing threats emerge from its deployment model [17]. This factor makes the deployment model one that needs consideration. Additionally, threats arising from management issues in Cloud Computing, have been identified, for example, costs, benchmarking, change management, legislation, Service Level Agreement (SLA), lack of interoperability, information retrieval, information localization, standardization, single point of failure, service availability, and security issues [13]. In [67], eight threat categories for Cloud Computing are listed: security issues identified by organizations; deployment and service delivery model security; software related security issues; data storage and computational security issues; virtualization security issues;, networking, web, and hardware resources security issues; access; and trust security issues. On the other hand, the discussion in [66] identifies a threat taxonomy on the basis of the classes of participants within a Cloud infrastructure and the specified participants are: service users, service instances, and Cloud providers. As a further categorization, six root categories are outlined: service-to-user, user-to-service, Cloud-to-service, service-to-Cloud, Cloud-to-user, and user-to-Cloud. Considering technical aspects, five categories of concern to Cloud security are identified: hardware components, virtual machine manager, guest operating system, applications network, and governance.

From the above, it may be noted then, that the identification of threats in a Cloud environment are subjected to the context in which they are viewed and it is from this position that the taxonomy presented here is taken. Concerns over the current level of understanding about Cloud Computing security has moved some to make comment on the state of Cloud Computing security as "confusing" [26]. Thus, this taxonomy is more generally applicable and therefore generalizable. To facilitate unambiguous study and categorization of Cloud threats, the taxonomy in this article includes all the genres of threats to Cloud Computing. Consequently, new and emerging threats may be identified, categorized, and subsequently countermeasure for the respective threats may be provided.

In the following section, a context for security concerns in Cloud Computing is created, and Cloud deployment models are presented, the next section addresses virtualization and its significance and scope within Cloud infrastructure deployment. We present six case studies of Cloud breaches that demonstrate some of the threats identified in the taxonomy. Following that, security concerns specific to Cloud Computing are presented and categorized into a generalized Cloud threat taxonomy. Then, recent cases of Cloud breaches are applied to the taxonomy to determine whether the taxonomy holds true.

Cloud Computing

While definitions of Cloud Computing are applied inconsistently [48], the National Institute of Standard and Technology (NIST) provides a formal definition of Cloud Computing [14] as a convenient way to share computing and networking resource, accessed on an on-demand basis with minimal management effort for the end users and with minimum interaction from service providers. Other definitions of Cloud Computing exist [4], for example, where it is described with different terminologies such as pay as you go computing, utility computing, and on-demand computing [8, 27]. Cloud Computing is also defined as a service accessible over the Internet by means of virtualized and dynamically scalable resources [38]. As definitions imply, external resource allocation is a core feature of Cloud Computing and so security concerns become an issue [5].

Cloud Computing is categorized either as a private, public, hybrid, or community Cloud [13, 62, 82].

- **Private Cloud**: The Cloud infrastructure that is operated and managed by private organizations or by some outsourced specialist third party. It could be either off-premise or on-premise.
- **Public Cloud**: The Cloud infrastructure or services open for the public. It is normally operated and managed by single Cloud service provider and services are open to be subscribed by any entity (Cloud users).
- **Hybrid Cloud**: A mix of any of the Clouds above (at least two). The Cloud environment retains distinct characteristics of private and public sectors, but provides portability through load balancing and options to switch services.
- **Community Cloud**: Is shared by more than one organization and is intended for use by a community of entities with common concerns, interests, or goals.

The Cloud deployment model suggests that resources in a Cloud environment use a publicly accessible network, that is, the Internet. Also, since a Cloud environment is a shared platform, it is important that the boundary for each user is defined and that it is consistently applied. However, despite that, the opportunity for security breaches exists because resources are shared by multiple users.

Cloud and virtualization

For achieving cost efficiency and provisioning in the Cloud infrastructure, virtualization is a core technology that reduces costs significantly and benefits Cloud service providers [40, 49]. Also, the reliance on virtualization means that security is of equal importance [49, 45, 60]; however, it has been pointed to as a vulnerable target [3, 60, 68]. Additionally, the virtualization platform, the hypervisor, is a highly dynamic environment, and so concerns about identity and authority management arise. That is, through virtualization, hardware sharing is possible and the possibility of reputation fate sharing becomes a threat. This is where the reputation of one user is affected by another user who shares the same hardware [60, 68].

Further, the loss of a logical segregation of data in virtualization is a serious issue in Cloud security [3, 10, 11, 39, 68]. Exploits at this level are prominent because of the multi-tenancy model [59] and while management of the hypervisor is an issue, if the hypervisor is not robust and secured, then the integrity of the Cloud environment is put at risk [3, 55]. Some consider virtualization and its multi-tenancy feature to be a direct Cloud privacy and security threat [50, 76]. For example, virtualization and its hardware-sharing characteristics provide the conditions for side channel attacks and backdoor channel attacks.

Case studies

In order to build a taxonomy for further analysis of threats against Cloud-based computing environments, nine case studies of Cloud breaches have been analyzed. The method of analysis is a qualitative assessment of the type of breach of security and the extent to which the breach has affected stakeholders. The breaches discussed here have been expanded with more recent exploits to demonstrate the validity of the taxonomy. The purpose of the taxonomy is to ascertain what types of exploit have been successful (as opposed to vulnerabilities that may not have been exploited) and to provide a basis for requirements gathering in the design of a Cloud-based security system. Along with a mapping of attacks into the taxonomy, the following discussion presents the case studies that are summarized in Table 1. To summarize the threats, the relevant literature is presented Table 2. The latter includes a mapping of the taxonomy to threats identified.

The first case is Apple's iCloud service that provides consumer level service to back up smartphones' content (such as music, photos, and data) [71]. Hackers breached the Cloud service on September 1, 2014 and the personal photos of celebrities were made publicly available [57]. The hackers used a brute force password cracking approach to gain unauthorized access to the celebrity photos. Apple refused to take responsibility, stating that it was a targeted attack and not a Cloud breach [71, 72]. Apple claims the incident was not an architecture-wide breach of iCloud but a focused attack on specific user accounts where unauthorized access was gained by obtaining passwords, security questions, and usernames.

This case represents a combination of factors (human and technological) that include the ease with which passwords may be discovered by brute force methods and the simplicity of passwords that are selected by users. In the examples represented above, one cannot simply point the finger of blame at the user because passwords are themselves the most basic form of security. A process that is dependent upon the knowledge of answers to security questions is inherently weak. In a similar case in early 2015, the login details of Uber taxi users were stolen and sold on the Dark Net [73]. This allowed buyers to obtain user credentials and to access Uber services. Uber denies that any attack on its Cloud servers occurred, and lays the blame on users, saying that they should not use the same login details on multiple sites.

Alternatively, Online password manager, LastPass, detected unusual activity in its Cloud servers and some user data was stolen [56]. The servers were put into "lockdown" mode and the network wide malicious activity is not considered a bad breach because the effects of the attack were limited with the option to use multi-factor authentication or not using password reminders.

In April 2011, Sony Corporation's online entertainment system experienced an attack that netted the attackers with the second largest haul to that date. The personal accounts of more than 100 million Sony customers were exposed. In the attack on Amazon's Cloud-based web servers and using an alias, hackers signed up to Amazon's EC2 service and from there they were able to successfully access co-located Virtual

Table 1. Summary of attacks in terms of the taxonomy.

Description of attack	Threat type in taxonomy	Case study
Brute-force password cracking, claimed to be targeted attack instead of an architecture-wide to obtain specific users' password and credentials.	Social Context, Competence	Apple iCloud breach
Hacker's signed up for VM and then accessed co-located SONY's VM on Amazon EC2 server. A cross VM side-channel attack.	Computing Services, Virtualization	SONY server attack through Amazon VM
Weak code execution vulnerability helped attackers to access to access a total of 76 million users' and 7 million small businesses' personal information (names, email addresses, and physical addresses).	Software Tools, Web Services, Competence	JPMorgan server hack
Unprotected for 4 hours, any Dropbox account could be accessed by using any password during the period.	Lack of Competence, Trust	Dropbox
Snapchat server hacked and claimed to be done so by reverse engineering the API by a third party app, which also resulted in noncompliance of end user license agreement for affected Snapchat users.	Social Context, Competence, SLA misinterpretation	Snapchat
Attackers took the vendor's services down by installing malware on end users' devices. Vendor claimed the loophole was in end users' computers, and had nothing to do with their Cloud architecture.	Social Context, Competence, Software tool, web service, Cloud platform, computing services, virtualization,	Spark
Login details of the users were stolen and sold on Dark Net. Uber points the responsibility was on the users, who used same login credentials on different sites.	Social Context, Competence, Trust, Regulation	Uber taxi
Unusual activities detected on server that resulted some user data loss. The network-wide unexpected breach required the servers to take to "lock-down" mode.	Cloud Platform, Social Context, Competence.	LastPass
24 million users' data exposed yet no specific information on how the attack emerged.	Competence	Zappos

Table 2. Threats in literature categorized according to the taxonomy.

Category in taxonomy	Threat	Reference
Trust	Trust, trust management	[28, 30, 41, 54, 60]
Compliance, regulations	Standards, Compliance measures	[68]
SLA misinterpretation	Proper SLA provisioning, Poor understanding of SLA	[15, 24, 68, 70]
Social context, competence, specialization	Social Engineering	[42, 61, 75]
Computing services	Outsourcing Cloud services	[23]
Internal infrastructure	Insider attack	[23]
External networks	Wireless link exploitation	[78]
Local platform	Poor user control on data in smartphones	[27]
Cloud platform	Insider attack	[23]
Network protocols	Peer-to-peer protocol vulnerabilities	[76]
Virtualization	Hyper-jacking, cross-VM side channel attack	[29, 58]
Software tools	Application vulnerability	[29]
Web services	Web based services, HTTP vulnerabilities,	[29, 50]
Security mechanisms	Traditional weakness in cryptography, Theft of cryptographic key, Authentication issues	[25, 27, 29]
Mobile computing	Vulnerable applications spread through mobile devices	[78]

Machines (VMs) on the same cluster [9, 10]. The attack was very carefully planned and executed. The opportunity to use the Cloud servers helped the attackers to maintain anonymity. This case differs from the previous insofar that the method of attack is far more sophisticated and requires significant expertise and knowledge of the Cloud infrastructure. The method of approach resembles a cross VM side channel attack which, to be successful, needs multiple stages to be executed in order for the attacker to get access to the VM encryption keys. The previous case, by using brute force techniques, could be achieved by any attacker who has the patience to wait for a password to be successfully found.

The next case reports unauthorized access to 80 million accounts holders of JPMorgan by means of a weak code execution vulnerability [19]. A total of 76 million users' and 7 million small business' personal information (names, email addresses, and physical addresses) were accessed by the attackers [21]. JPMorgan claim no unauthorized access could be made to account-related information, user IDs, and date of birth or account number and no fraudulent customer activities were found as a result of the incident. It was users who accessed the service through websites or smartphones that were affected. It is probable that the only abuse of the leaked information would be by spammers. For this case, the issue appears to be focused around vulnerabilities in the computer–user interface.

Case 4 occurred in mid-2011, when Dropbox experienced an attack. The website of the Cloud provider was left unprotected and exposed, leaving servers containing personal sensitive data and information of a massive number of users exposed. An estimated 25 million users use Dropbox to store their personal contents such as images, documents, videos or other types of files. During the breach, Dropbox was unprotected for 4 hours, giving anyone the opportunity to access any account with any password. To give its users access to the system, the provider had traded security to bring ease of use by requiring only a simple password instead of having complex encryption keys; and keeping the encryption and decryption process within its own servers [20]. Similar to Case 1, but more extreme, this case represents a failure of security policy and management. Needless to say, this is no longer the case today.

The fifth case involves Snapchat, an instant photo-sharing application. It is claimed that Snapchat's Cloud servers were hacked in October 2014. The claim is that either the service provider's Cloud servers or its end user application or both were hacked. Snapchat denies the claims and points to a third party vendor that had applied a reversed engineering approach to Snapchat's API to store users' data from Snapchat's servers. This third party app, when used, made the Snapchat users noncompliant with the end user license agreement [74]. Such a case represents a complex situation that is likely to become more frequent as more use is made of API's that may offer up vulnerabilities for exploitation. This case provides an example of how technological factors may be combined with human factors to produce conditions that are ripe for an attacker to use.

Another case involves Spark, a telecom service provider in New Zealand. In September 2014, as the consequence of a cyber attack, the vendor's Cloud services were significantly interrupted and subsequently shut down and broadband services became unavailable. The attackers, who are believed to be international cyber criminals, had installed malware on Spark's end users' computers. The malware was equipped with malicious code to effectively launch a denial of service attack. The attack subsequently generated heavy traffic to create a situation of service unavailability. Spark's claim is that its own Cloud architecture did not have any fault but rather it was the end users' computers that were affected and were used to launch the attack [69]. This case represents what is perhaps one of the greatest weaknesses in a Cloud architecture, and that is the human factor. In all of these cases, the underlying theme appears to be that it is this factor that either creates the conditions for or allows for vulnerabilities to be exploited.

Shoe retailer Zappos' data breach in January 2015 exposed 24 million users' data to attackers [63]. There is almost no information on how the attack emerged [12]. However, the case illustrates the importance of focusing on the exploitation of zero day vulnerabilities. The service provider or the computing services Zappos uses to deliver its service appear to be at fault for not addressing vulnerabilities.

Cloud Computing threats

We argue that Cloud Computing is a concept that has substantiated properties. Among those are the social setting within which a Cloud service is operating, thus considerations to take into account are technical and human soft factors such as socio-technical issues, cultural and social contextual issues, domestic or international regulations, and users' computer literacy.

While security concerns and threats for Cloud Computing are important [28], it may be difficult to determine that any breach is a failure of a Cloud technology. That is, Cloud Computing consists of a range of contemporary computing and Internet technologies that has been grouped together in order for people to understand the context they operate in. Cloud Computing specific threats may not be limited to a Cloud architecture. Instead, one must consider all substantial and conceptual properties of Cloud Computing such as the Cloud architecture, users, and intermediate provisioning (Internet or any public or private infrastructure).

To define "threat" for Cloud Computing, the cases have been analyzed to produce genre-based top-down threat taxonomy specific to Cloud Computing (see Figure 1). A high-level categorization of a threat taxonomy provides for most computing technologies that fall within the operational or architectural context of Cloud Computing. Further, a threat to the security of a Cloud Computing environment may be seen as a part of a specific Cloud architecture. This implies that such a threat is a technological and, to some extent, a regulatory and location transparency related problem.

Figure 1 illustrates that at its highest level, Cloud Computing threats can be categorized as *technological factors* (or hard threats) and *human factors* (or soft threats). These are discussed in the following sections. In the computing environment, both technological and human factors play an equally important role, for example [31], [33], [43], and [51]. This approach separates designed and accidental threats through hardware and software as technology from deliberate and non-deliberate threats by human actions.

Human factors

The reference to "soft threats" above relates to threats that arise from human-centric actions that threaten a Cloud infrastructure. Such threats might be associated with government regulations for any given region or country, the lack of data security and consistency in a location independent Cloud Computing case, social engineering, poor computer literacy of service consumers, level of trust among various Cloud stakeholders and might be a direct influence on cultural or

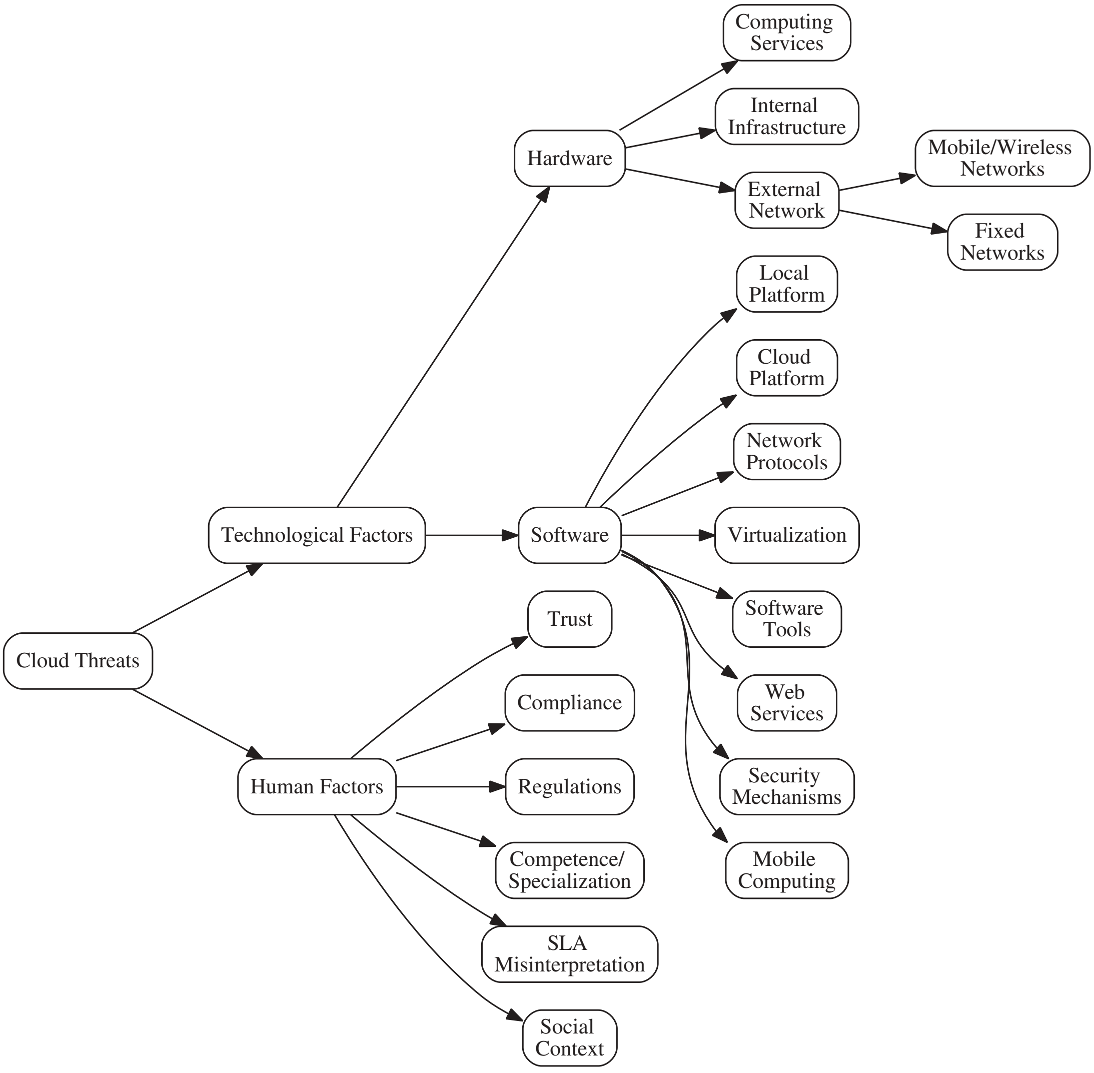

Figure 1. Threat taxonomy for Cloud Computing.

social norms, compliance or lack of well-defined compliance standards. This does not relate to incidents where data security has been breached as a consequence of, say, a staff member who inadvertently leaves a removable drive in a public place.

As dynamic security challenges emerge, two human factors, *compliance* and *competence*, are required for Cloud providers and end users. If compliance is not in place, then out-of-standard procedures are allowed, and threats to security may occur. The competence of IT practitioners and management is a factor where users, developers, and Cloud providers demonstrate good practice to prevent unwanted events.

A constant threat to Internet security and therefore the Cloud environment is social engineering [42]. The *social context* refers to the use of Cloud Computing within the community, which in turn is associated with other factors such as trust and social engineering, specific human related security issues such as a lack of awareness or training, or lack of vigilance or caution when using Cloud services. The social context and related social engineering has been referred to as the dark art that poses a severe threat to confidentiality, integrity, and authenticity of information [75] and alternatively defined as the act of manipulating people to extract or gain access to confidential information [61]. This may have greater effect where a lack of competence is put in service to compliance to aid in the aims of the attacker.

In the Snapchat case study, image access is limited after a short time although images exist on intermediate servers as they move through networks. To bypass the terms and conditions set by Snapchat and to get and store images from Snapchat servers, users installed a third-party application. The application intercepts the data or images and in this situation, images that the originator did not intend to last were captured and, in some cases, were used to embarrass or compromise individuals. It was from ignorance of how the system handles data that users were lulled into a sense of false security. This also illustrates how someone with malicious intent is able to step around a socially ordered agreement.

We are quite familiar with phishing messages purporting to be from banks and other institutions and while people are often warned not to click on attachments, people still do. Or they click on a link to a site masquerading as an official site but that contains an Adobe Flash file which contains malicious code or malware. This may be attributable to a lack of competence or social engineering. Whatever is the case, the effects of large numbers of users that are similarly duped enables the creation of botnets in which a botnet master is able to control functions on computers en masse. In the case of New Zealand telecommunications company, Spark, a significant outage occurred due to a denial of service attack on at least one of their servers. Spark's customers, not the company itself, may have been the target, but the result was that thousands of users lost access to broadband Internet services. The service provider blames users who downloaded and installed malware into their computers by opening infected email attachments.

The taxonomy does not present elements that are mutually exclusive, that is, a specific Cloud breach may incorporate a number of threats. The case of JPMorgan is such an example that while there has been no evidence of abuse of users' accounts, stolen data may have been sold to criminals or spammers. Thus, trust of an organization tasked with maintaining the privacy of user data is brought into question, regardless of whether the reason behind such a breach is technological (e.g. web service, Cloud platform, computing services, and virtualization) or human factors (e.g. social context and competence).

Location transparency is a security concern that is linked to social or regulatory contexts rather than technological issues. If data from one region (e.g. nation and jurisdiction) are transferred to any other region, there is no guarantee that the data are being treated in the same way as the source. This includes the level of security as well as retention and processing of data. Ideally, regulations that address data management would be consistent across jurisdictions. However, this ideal has yet to be reached.

Due to the complexity of Cloud Computing architectures, SLA provisioning needs careful assessment [15]. Also, misinterpretations of the SLA are related to failures in Cloud computer security [68]. For example, there is a tendency for customers to make an agreement, perhaps through a lack of understanding of legal jargon, without actually reading the end user license. Thus, it is important to make a commitment to the SLA to provide an assurance that conditions are met [70]. Conversely, it may be argued that a lack of commitment leads to a lack of monitoring of an SLA [24].

In any case, whether it is through SLA confusion or expectation, trust in the Cloud is a major issue and trust management and security as a key challenge [28, 53]. Trust is a state that helps one party to keep faith and reliance based on transparent control practices, ownership, and security in a Cloud environment [41]. While trust derives from the social sciences, in heterogeneous computing a relationship to security is implied [30]. Users of Cloud-based services are expected to trust the Cloud provider with sensitive, personal, and confidential data [60]. A lack of trust is a conscious state and while it may not be a conscious choice, it is one that is held by the service consumer. This is a technology independent viewpoint and while it relies on a service–consumer perception, trust is affected by the level of policy or procedure development at the micro- or organizational level or at the macro- or regional level, the robustness of a regulatory framework. A crucial concern is how standards are applied and whether compliance measures are sufficiently robust in a given region [68].

Regulation and compliance conformity differ from procedure where a lack of adequate governance affects the level of trust a customer will hold in a Cloud provider. The Dropbox case provides an example of how trust can in Cloud Computing can be affected through either a lack of competence or a failure to predict security requirements, and how security should be integrated into a Cloud service.

Of the cases presented, not all are a direct attack on the Cloud architecture. In the Apple case, user accounts are hacked through brute-force methods and the damage was limited. Though Apple provides strong security mechanisms to safeguard its Cloud architecture, weak user passwords leave accounts and possibly other systems open to attack.

Technological factors

Technological factors refer to threats other than human or social factors. We argue that, in the computing environment, the factors or threats in this category fall into two categories: (1) hardware-related threats that relate to the Cloud infrastructure and network, and (2) software-related threats that relate to platform and application resources above the Cloud infrastructure. Across both categories, Internet-based vulnerabilities provide security concerns because the Internet is the primary means of accessing Cloud resources [29].

Additionally, virtualization, web services, and application and cryptography are associated with vulnerabilities [29]. Virtualization provides a number of software-based security threats [58]. For example, denial of service, and hypervisor exploits such as hyper-jacking, cross-VM side channel attacks and hypervisor escape.

Web services introduce challenges to security, for example, HTTP vulnerabilities that present threats while users access Cloud services [50]. Threats generally include Structured Query Language (SQL) injection, cross-site scripting, lack of web site security, directory traversal, lack of AJAX security from poor programing, Apache web server vulnerabilities, and lack public Cloud provider security measures such as WordPress.

While cryptography is applied when other measures cannot assure security, for example, when data may be encrypted before they are sent to a Cloud service, traditional cryptographic mechanisms may be associated with weaknesses [25], for example, successful interception of data in man-in-the-middle exploits and subsequent decryption of intercepted data. In another example, the theft of cryptographic keys during successful cross-VM side channel attacks.

Mobile computing is becoming a common means for distributed and general computing [18], that mobile Cloud Computing is becoming an inherent part of the total Cloud Computing practice [16], and this has led to the concept of Bring Your Own Device (BYOD) [42]. Security vulnerabilities in mobile technologies are now becoming more apparent, especially in the more open Android development space. The provisioning of mobile computing introduces application and network based threats [27, 44, 77].

Threats can be introduced to the Cloud environment internally, for example, maintenance services such as incident response or routine maintenance provides opportunities for a person (insider or outsider) to access resources they are not entitled to. Failing or malfunctioning hardware provides the opportunity for potential security breaches. However, organizations may not be willing to reveal a Cloud breach or the actual reason for a breach for fear of losing trust or goodwill from stakeholders. A number of breaches listed may incorporate threats that arise from network or hardware component failures, poor configuration, inconsistent maintenance, or poor management of incident response. Vulnerabilities in peer-to-peer network protocols may therefore be exploited [76]. Additionally, an insider attack may be carried out through unauthorized on-premise or remote access to Cloud resources as a consequence of outsourcing Cloud services to third parties [23].

As an example of a local or end user platform specific issue, smartphone apps often require access to more data that are necessarily required to function, that users of smartphones have poor control over data stored on phones [27].

Expectations of social or cultural behaviors are often played out in the cyberworld and is socio-technical in orientation. In the Spark case study, through a complex interplay of social engineering, using end users' computers, a successful attack on the company's server network was launched.

The Uber example represents a case of social context and competence. If users were not aware and shared their login credentials with someone who has then taken advantage of the opportunity to also make use of the user account, then the threat is one of social engineering and therefore has a social context. If the misuse of the user information is due to a technological issue, as a consequence of a third party that is considered a credible and trustworthy service provider and with whom the user has shared Uber login credentials, then the threat can be categorized as trust, regulations, and competence. Trust is a factor between Uber and any other service provider with whom users shared the login credentials. Also, the third party service provider may show a lack of competence.

Aligning cases to the taxonomy may involve more than one category. In the case of LastPass, while the breach is technological (e.g., via the Cloud Platform), the users played a part through their social context and level of competence (and thus related to human factors).

Table 1 summarizes the case studies discussed above and includes short description of the attacks for each case study, along with the possible threat categories of the taxonomy associated with the carried attack. In Table 2, the threats identified in the literature are mapped to the taxonomy.

Further research

The taxonomy is generalized and genre-based and thus provides understanding of the nature of existing and new threats in the Cloud environment, unlike other taxonomies that tend toward specific problem or application areas. As new threats emerge, the taxonomy may be applied to specific problem areas and its value is realized. For example, the taxonomy has been applied to the modeling and design of a distributed application architecture to provide security functions for a Cloud Computing environment [1]. This solution is created to provide a fully redundant, distributed security system with no single point of failure and so far as the attacker is concerned, the system appears to be everywhere. In this instance, the taxonomy identifies where threats are likely to emerge and aids in the classification of threat types when designing functional requirements.

Other potential uses of the taxonomy are in social sciences research, so that the researcher can properly separate hard and soft factors from threats or attacks. For example, human factors are seen to be a significant factor in threats that include the distribution and us of embedded malware, ransomware, and so on. This also provides for the social science researcher the opportunity to propose solutions appropriate to usage patterns by human actors such as educational programs or recommendations for the design of corporate computer use policies. Also in the enterprise space, the taxonomy is useful in the design and planning for enterprise security policy. For example, again, the human factor is often seen as the biggest risk to enterprise systems, whether by misuse, ignorance, or omission. However, policy ought to include the management of technological factors. In this instance, the IS researcher is inclined to consider what technological aspects have been omitted from policy and what impact that may have in the event that the omission is exploited.

The area of trust management is another in which the taxonomy may be applied. Trust is a complex issue and the individual factors that influence the presence or absence of trust combine to make the accumulation of trust in a service difficult to predict. Therefore, it is difficult to put in place plans or policies that will confidently lead to a trust-based relationship between the service provider and consumer.

Conclusion

Cloud Computing incorporates existing and new computing technologies and threats to services are inherited from existing technologies and new threats are introduced. The determination of threats is made difficult due to the range of technologies involved. Therefore, to understand the holistic context of Cloud Computing threats, we consider them from a generalized viewpoint.

To better address Cloud Computing threats in a structured manner by researchers, the analysis of cases is presented as a taxonomy. To better understand the genre and nature of any newly introduced threat, the taxonomy may be applied by categorizing them or by considering how threats are related to other categories. Based on our argument that threats to Cloud Computing exist in other computing fields, the proposed taxonomy is applicable to a wide range of issues.

ORCID

Monjur Ahmed http://orcid.org/0000-0003-1929-3950
Alan T. Litchfield http://orcid.org/0000-0002-3876-0940

References

[1] Ahmed M, Litchfield AT, Sharma C. A distributed security model for cloud computing, In Proceedings of the Americas Conference on Information Systems, 2016, San Diego.

[2] Akande AO, April NA, Belle JV. Management Issues with Cloud Computing, ACM ICCC'13; 2013 December 1–2; p. 119–124.

[3] Alfath A, Baina K, Baina S. Cloud computing security: fine-grained analysis and security approaches. IEEE 2013 National Security Days (JNS3) Conference, IEEE, Rabat; 2013; p. 1–6.

[4] Arshad J, Townend P, and Xu J. A novel intrusion severity analysis approach for Clouds. Future Gener Comput Syst. 2013;29:416–428.

[5] Azeemi IK, Lewis M, Tryfonas T. Migrating to the cloud: lessons and limitations of 'traditional' is success models. Procedia Comput Sci. 2013;16:737–746.

[6] Beevi FHA, Wagner S, Hallerstede S, Pedersen CF. Data quality oriented taxonomy of ambient assisted living systems, IET International Conference on Technologies for Active and Assisted Living (TechAAL); 2015 November 5-5; London.

[7] Behl A, Behl K. An analysis of cloud computing security issues, World Congress on Information and Communication Technologies (WICT), IEEE; 2012; Trivandrum; p. 109–114.

[8] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Gener Comput Syst. 2009;25:599–616.

[9] Bloomberg. Amazon.com server said to have been used in Sony attack. 2011. http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html.

[10] Bloomberg. Sony network breach shows amazon cloud's appeal for hackers. 2011. http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html.

[11] Bouayad A, Blilat A, Mejhed N, Ghazi ME. Cloud computing: Security challenges. Colloquium in Information Science and Technology (CIST), IEEE, Fez: 2012; 26–31.

[12] Bradley T. Zappos hacked: What you need to know. 2015. Available from http://www.pcworld.com/article/248244/zappos_hacked_what_you_need_to_know.html

[13] Cardoso A, Simões P. Cloud computing: Concepts, technologies and challenges. ViNOrg 2011, CCIS 248, Springer-Verlag Berlin Heidelberg; 2012, 127–136.

[14] Casola V, Cuomo A, Rak M, Villano U. The CloudGrid approach: security analysis and performance evaluation. Future Gener Comput Syst. 2013;29:387–401.

[15] Casalicchio E, Silvestri L. Mechanisms for SLA provisioning in cloud-based service providers. Comput Networks 2013;57:795–810.

[16] Cheng F. Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm. Mobile Networks Appl. 2011;16:304–336.

[17] Chou T. Security threats on cloud computing vulnerabilities. Int J Comput Sci Inf Technol. 2013:5(3):79–88.

[18] Chow R, Jakobsson M, Masuoka R, Molina J, Niu Y, Shi E, Song Z. Authentication in the Clouds: A Framework and Its Application to Mobile Users. ACM, CCSW'10; 2010 October 8; Chicago, Illinois, USA, p. 1–6.

[19] CNN. JPMorgan: 76 million customers hacked. 2014. Available from http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack/

[20] CNN. Dropbox's password nightmare highlights cloud risks. 2011. Available from http://money.cnn.com/2011/06/22/technology/dropbox_passwords/

[21] Computerworld. JPMorgan Chase breach affected 83 million customers. 2014. Available from http://www.computerworld.co.nz/article/556581/jpmorgan-chase-breach-affected-83-million-customers

[22] Dahbur K, Mohammad B, Tarakji AB. A survey of risks, threats and vulnerabilities in cloud computing. ACM, ISWSA'11, Amman, Jordan: April 18–20, 2011.

[23] Duncan A, Creese S, Goldsmith M. Insider attacks in cloud computing. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications; 2012; p. 857–862.

[24] Emeakaroha VC, Netto MAS, Calheiros RN, Brandic I, Buyya R, Rose CAFD. Towards autonomic detection of SLA violations in cloud infrastructures. Future Gener Comput Syst. 2012;28:1017–1029.

[25] Fan C, Huang S. Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. Future Gener Comput Syst. 2013;29:1716–1724.

[26] Fernandes DAB, Soares LFB, Gomes JV, Freire MM, Inácio PRM. Security issues in cloud environments: A survey. Int J Inf Secur. 2014;13:113–170.

[27] Fernando N, Loke SW, Rahayu W. Mobile cloud computing: A survey. Future Gener Comput Syst. 2013;29:84–106.

[28] Gonzalez N, Miers C, Redıgolo F, Simplıcio M, Carvalho T, Naslund M, Pourzandi M. A quantitative analysis of current security concerns and solutions for cloud computing, J Cloud Comput Adv Syst Appl. 2012;1(11):1–18.

[29] Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities, IEEE Security and Privacy 2011, March/April, 2011, p. 50–57.

[30] Guo Q, Sun D, Chang G, Sun L, Wang X. Modeling and evaluation of trust in cloud computing environments. 2011 3rd

International Conference on Advanced Computer Control (ICACC 2011); 2011. p. 112–116.

[31] Haniff DJ, Baber C. Wearable Computers for the fire service and police force: Technological and human factors, ISWC '99 Proceedings of the 3rd IEEE International Symposium on Wearable Computers, ACM; 1999, p. 185–186.

[32] Hashemi SM, Ardakani MRM. Taxonomy of the security aspects of cloud computing systems – A survey. Int J Appl Inf Syst. 2012:4 (1):21–28.

[33] Hawkey K, Gagne A, Botta D, Beznosov K, Werlinger R, Muldner K. Human, Organizational and Technological Factors of IT Security, CHI 2008 Proceedings, Florence; April 5–10 2008; Italy, p. 3639–3644.

[34] He X, Chomsiri T, Nanda P, Tan Z. Improving cloud network security using the tree-rule firewall. Future Gener Comput Syst. 2014;30:116–126.

[35] Herterich MM, Buehnen T, Uebernickel F, Brenner W. A Taxonomy of Industrial Service Systems Enabled by Digital Product Innovation, 49th Hawaii International Conference on System Sciences; 2016 January 5–8; Hawaii, p. 1236–1245.

[36] ISO/IEC 19099 Information technology — Virtualization management specification. British Standards Organization. 2014.

[37] Jaeger PT, Lin J, Grimes JM. Cloud Computing and information policy: computing in a policy cloud?. J Inf Technol Politics 2008;5 (3):269–283.

[38] Jorissen K, Vila FD, Rehr JJ. A high performance scientific cloud computing environment for materials simulations. Comput Phys Commun. 2012;183:1911–1919.

[39] Khalil IM, Khreishah A, Bouktif S, Ahmad A. Security Concerns in Cloud Computing, 10th International Conference on Information Technology: New Generations, IEEE; 2013; Las Vegas, p. 411–416.

[40] Khan AN, Kiah MLM, Khan SU, Madani SA. Towards secure mobile cloud computing: A survey. Future Gener Comput Syst. 2013;29:1278–1299.

[41] Khan KM, Malluhi Q. Establishing trust in cloud computing, IT Pro, (September/October), 2010, p. 20–26.

[42] Krombholz K, Hobel H, Huber M, Weippl E. Social Engineering Attacks on the Knowledge Worker, ACM SIN '13; 2013 November 26–28; Aksaray, Turkey, p. 28–35.

[43] Kueppers S, Schilingno M. Getting our act together: Human and technological factors in establishing an on–line knowledge base, SIGUCCS 99, ACM, Denver, Colorado: 1999, p. 135–139.

[44] Kulkarni P, Khanai R. Addressing mobile cloud computing security issues: a survey, IEEE ICCSP 2015 conference; 2015; Bangalore, India, p. 1463–1467.

[45] Kulkarni G, Gambhir J, Patil T, Dongare A. A Security Aspects in Cloud Computing, IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS), IEEE; 2012; Beijing, China, p. 547–550.

[46] Lee K. Security threats in cloud computing environments. Int J Secur Its Appl. 2012;6(4):25–32.

[47] Liangli M, Yanshen, C., Yufei, S, Qingyi W. Virtualization maturity reference model for green software, International Conference on Control Engineering and Communication Technology, IEEE; 2012 December 7–9; China, p. 573–576.

[48] Litchfield AT, Althouse J. A systematic review of cloud computing, big data and databases on the cloud, In Proceedings of the Americas Conference on Information Systems; 2014; Georgia, Savannah, US, p. 1–19.

[49] Liu W. Research on cloud computing security problem and strategy, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), IEEE, Yichang, 2012, 1216–1219.

[50] Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in Cloud. J Network Comput Appl. 2013;36:42–57.

[51] Mohamadi M, Ranjbaran T. Effective factors on the success or failure of the online payment systems, focusing on human factors, 7th International Conference on e-Commerce in Developing Countries with Focus of e-Security, IEEE; 2013 April 17–18; Iran, p. 1–12.

[52] Mrosek R, Dehling T, Sunyaev A. Taxonomy of health IT and medication adherence. Health Policy Technol. 2016;4:215–224.

[53] Nickerson RC, Varshney U, Muntermann J. A method for taxonomy development and its application in information systems. Eur J Inf Syst. 2013;22:336–359.

[54] Noor TH, Sheng QZ, Zeadally S, Yu J. Trust management of services in cloud environments: obstacles and solutions. ACM Comput Surv. 2013;46(1):12:1–12:30.

[55] Patel A, Taghavi M, Bakhtiyari K, Junior JC. An intrusion detection and prevention system in cloud computing: a systematic review. J Network Comput Appl. 2013;36:25–41.

[56] Paul I. The LastPass security breach: what you need to know, do, and watch out for. [16 June, 2015] Available from http://www.pcworld.com/article/2936621/the-lastpass-security-breach-what-you-need-to-know-do-and-watch-out-for.html

[57] PCWorld. Don't blame iCloud Yet for Hacked Celebrity Nudes. 2014. Available from http://www.pcworld.com/article/2601081/dont-blame-icloud-yet-for-hacked-celebrity-nudes.html

[58] Perez-Botero D, Szefer J, Lee RB. Characterizing hypervisor vulnerabilities in cloud computing servers. ACM, CloudComputing'13; 2013 May 8; Hangzhou, China, p. 3–10.

[59] Rabai LBA, Jouini M, Aissa AB, Mili A. A cybersecurity model in cloud computing environments. J King Saud Univ Comput Inf Sci. 2013;25:63–75.

[60] Roberts JC, Al-Hamdani W. Who can you Trust in the Cloud? a Review of Security Issues within Cloud Computing, ACM Information Security Curriculum Development Conference 2011; 2011 October 7–9, p. 15–19.

[61] Robling G, Muller M. Social engineering: A serious underestimated problem. ACM ITiCSE'09; 2009 July 6–8; Paris, France, p. 384–387.

[62] Rong C, Nguyen ST, Jaatun MG. Beyond lightning: a survey on security challenges in cloud computing. Comput Electr Eng. 2013;39:47–54.

[63] Schwartz MJ. Zappos breach: 8 Lessons Learned; 17 January, 2015 Available from http://www.darkreading.com/attacks-and-breaches/zappos-breach-8-lessons-learned/d/d-id/1102303?

[64] Sen A, Madria S. Off-line risk assessment of cloud service provider, IEEE 10th World Congress on Services, IEEE; 2014 June 27 – July 2, p. 58–65.

[65] Shaikh FB, Haider S. Security Threats in Cloud Computing, 6th International Conference on Internet Technology and Secured Transactions, IEEE, Abu Dhabi, United Arab Emirates: 2011 December 11–14, p. 214–219.

[66] Singh A, Shrivastava M. Overview of attacks on cloud computing. Int J Eng Innovative Technol. 2012;1(4):321–323.

[67] Soares LFB, Fernandes DAB, Gomes JV, Freire MM, Inácio PRM. Cloud Security: State of the Art, Security, Privacy and Trust in Cloud Systems, 2014, (3), Springer-Verlag Berlin Heidelberg, DOI: 10.1007/978-3-642-38586-5_1.

[68] Srinivasan MK, Sarukesi K, Rodrigues P, Manoj SM, Revathy P. "State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud computing environment". ACM ICACCI '12; 2012 August 03–05; Chennai, India, p. 470–476.

[69] Stuff.co.nz. Spark broadband still down for many. 2014. Available from http://www.stuff.co.nz/business/10468128/Spark-broadband-still-down-for-many

[70] Sun L, Singh J, Hussain OK. Service Level Agreement (SLA) Assurance for Cloud Services: A Survey from a Transactional Risk Perspective, ACM MoMM2012, Bali, Indonesia; 2012 December 3-5; 263–266.

[71] TechTimes. 2014. Apple denies iCloud, Find My iPhone security breach: Only very targeted attacks. Available from http://www.techtimes.com/articles/14717/20140907/apple-denies-icloud-find-my-iphone-security-breach-only-very-targeted-attacks.htm

[72] The Wall Street Journal. Apple Denies iCloud Breach. 2014. Available from http://online.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803

[73] TheGuardian. Uber denies security breach despite reports of logins for sale online. March, 2015. Available from http://www.theguardian.com/technology/2015/mar/30/uber-denies-security-breach-logins-for-sale-dark-web

[74] TheRegister.co.uk. Slap for SnapChat web app in SNAP mishap flap: '200,000' snaps sapped. 2014. Available from http://www.theregister.co.uk/2014/10/10/new_photo_hack_claim_200000_snapchat_photos/

[75] Thornburgh T. Social Engineering: The "Dark Art". ACM InfoSecCD Conference'04; 2004 October 8; Kennesaw, GA, USA, p. 133–135.

[76] Tong J, Xiong G, Zhao Y, Guo L. 2013. A research on the vulnerability in popular P2P protocols, 2013 8th International Conference on Communications and Networking in China (CHINACOM), 2013, p. 405–409.

[77] Vaquero LM, Rodero-Merino L, Morán D. *Locking the* sky: a survey on IaaS cloud security. Computing 2011;91:93–118.

[78] Vikas S, Gurudatt K, Pawan K, Shyam G. Mobile Cloud Computing: Security Threats, 2014 International Conference on Electronics and Communication Systems (lCECS -2014); 2014 February 13-14; Coimbatore, India.

[79] Yang Z, Lui JCS. Security adoption and influence of cyber-insurance markets in heterogeneous networks. Perform Eval. 2014;74:1–17.

[80] You P, Peng Y, Liu W, Xue S. Security issues and solutions in cloud computing, 32nd International Conference on Distributed Computing Systems Workshops; 2012 June 18-21; Macau, China, p. 573–577.

[81] Zhang G, Yang Y, Chen J. A historical probability based noise generation strategy for privacy protection in cloud computing. J Comput Syst Sci. 2012;78:1374–1381.

[82] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst. 2012;28:583–592.