10

CLOUD AND MOBILE CLOUD ARCHITECTURE, SECURITY AND SAFETY

C. Mahmoudi
Algorithmic, Complexity and Logic Laboratory - Paris-Est Créteil University, Créteil, France

10.1 Introduction to Cloud Computing

Cloud computing has become a significant technology trend [1]. As anticipated by many experts, Cloud computing has reshaped information technology processes and the information technology marketplace as a whole. The most relevant Cloud computing definition [2] is a style of computing architecture that offers dynamic scalability and provides virtualized resources as services or as a container of services over the Internet. Cloud computing technology supports interaction with a variety of devices, including desktops, laptops, smartphones, and the Internet of Things to access services provided by the Cloud over the Internet. The Cloud services can be programs, storage, or application-development platforms offered by Cloud computing providers.

The Cloud computing paradigm introduces some advantages that include cost savings, high availability, and ease of scalability. These advantages help address the needs of the industry during the evolution of information technology architectures [3]. As illustrated in Fig. 10.1 the evolution of computing paradigms took place in five phases. In the first phase, called *mainframe computing*, many users were sharing powerful mainframes using terminal servers. In the second phase, called *desktop computing*, standalone computers became powerful enough to meet the majority of users' needs. In the third phase, *network computing*, computers and servers were interconnected through local networks. These connections aim to enable sharing of computing resources and data in order to increase performance. In the

Handbook of System Safety and Security. DOI: http://dx.doi.org/10.1016/B978-0-12-803773-7.00010-3

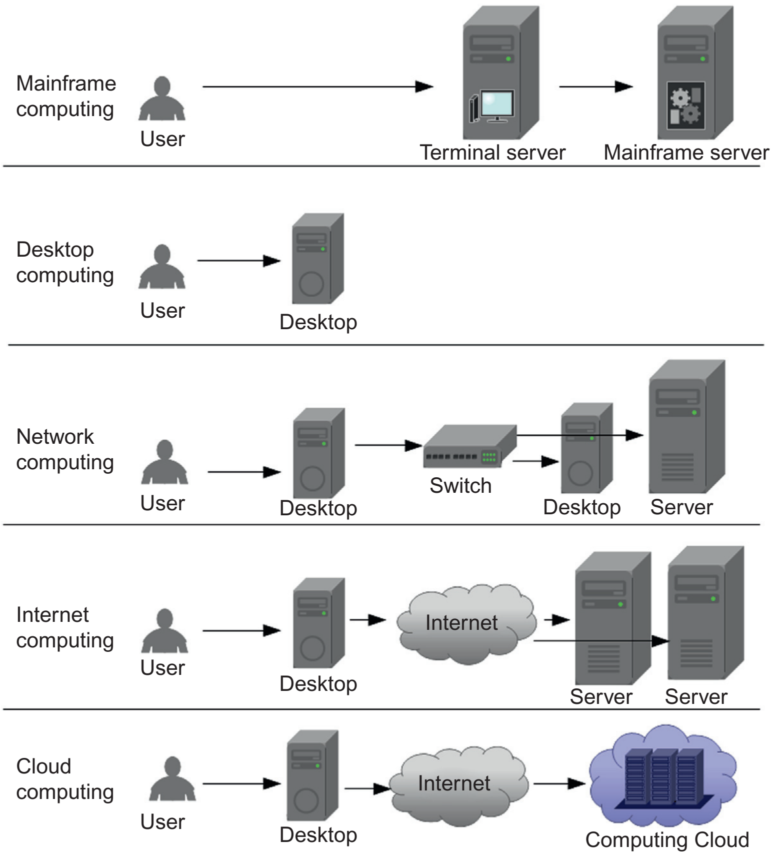

Figure 10.1 Evolution of the computing paradigms.

fourth phase, *Internet computing*, the technologies the Internet replaced the local networks. This global network emerged from the interconnection of different local networks in an effort to utilize remote applications and resources provided by other tiers. In the fifth phase, *Cloud computing*, the paradigm provides shared resources as services on the Internet where the Cloud provider manages the scalability and hides the complexity in a way that transparent to Cloud users. Comparing the Cloud computing paradigm to the other four computing paradigms, it appears that the Cloud computing model is very close to the one in the original mainframe computing paradigm. However several important differences differentiate these two computing paradigms. One of the differences lies in the fact that the computing power offered by Cloud computing is almost unlimited because of the scalable architecture behind it. Mainframe computing offers finite computing power because of the lack of scalability resulting from the isolation of the Mainframe backend. Another notable difference relates to do with the access technology to the services. While Mainframe services are accessed using terminals with no computational power, Cloud computing uses powerful local computers those themselves can use Cloud services and execute applications built on top of such services.

10.1.1 What Problems Does Cloud Computing Solve?

Obviously Cloud computing has become a major trend that makes business processes more efficient in terms of service availability and scalability. This is driven by the fact that Cloud computing can solve many of the problems faced by businesses as well as academic and government institutions. We discuss in this section four examples of problems that can be solved using the Cloud.

The first example illustrates how Cloud computing can solve problems in academic information system. Let us suppose that a university needs to organize an international conference to be webcast to all students with access to the university network. The video stream is in full HD, 1080 pixels at 50 frames per second, with the rendering quality of the video stream being a key indicator of the success of this conference. The publicity chair of this conference done a very effective job. One week before the content was to take place on day one of the conference, and because of a good job by the publicity chair, the online registration shows an unexpectedly high number of registrants that was not anticipated by the technical infrastructure. The university technicians concluded that their local infrastructure was not powerful enough to support the webcast to all the subscribers. The main reason for this conclusion was that a single frame of the webcast would take 1 hour to render through their own data center. Rendering the whole conference webcast would take many years. Short of using the Cloud, the university would have to buy more hardware to support this event, which is a very expensive alternative knowing that the current infrastructure has plenty of resources to support the university's everyday activities. The Cloud solution for such problems is a very efficient one. The university can get all the server infrastructure needed to support the event in a very short time. Moreover, by using a Cloud provider for this event, the university will not adversely affect everyday operations because of this event. In addition, if the number of online attendees keeps increasing unexpectedly, the Cloud provider offers the needed scalability to adapt the Cloud services to the demand.

This second example discusses how the Cloud could solve the problem of data processing for a government laboratory attached to a US government department needs to carry out data-intensive processing in-house. This processing requires very expensive and extensive computer infrastructure that would need to run for an extended period to produce an output consisting of a small size report. As a specific instance of this example, consider what the National Institute of Standards and Technology would need to process the data collected for the analysis of Internet routing protocols like Border Gateway Protocol. Without any special arrangement, this analysis took in some cases more than a week. A solution that would set up a dedicated infrastructure and associated human resources to maintain it would cost more than $0.5 million per year. The decision was to migrate the analysis to the Cloud and use distributed computing power from a farm of processors turns out to be a cost-effective solution. Once the researchers ran the analysis in a Cloud-based platform, the results were impressive. Indeed, the same analysis that took more than a week to complete in-house now takes less than an hour in the Cloud. In addition the Cloud platform is available for sharing among other research teams that can use the same infrastructure for other kinds of analysis when it is available.

In the third example we consider an online florist that runs a small business. For 98% of the year, this kind of business needs relatively little information technology infrastructure requirement to support a limited volume of sales. A single machine can normally handle the infrastructure needed for a website for the e-commerce activities and management applications. However, at peaks like Valentine's Day and Mother's Day, their infrastructure requirements change drastically as their business increases by 4000–5000%. The Cloud offers two kinds of solutions to businesses with similar sales profile. The first one consists of a Cloud service with the scalability being managed by the Cloud provider. Under this solution the business owner has chosen to host all his services are hosted in the Cloud. An alternative solution known as *Cloud bursting*. This solution offers the business owners the ability to continue hosting their applications on their local infrastructure, but uses a Cloud environment to expand their infrastructure at peaks of activity. In this way consumers are on special occasions that experience peaks in sales volume. By operating in this fashion, the customers will always able to access the sales website and avoid any potential overload that can overwhelm the servers. By keeping its customers satisfied, the small business will not miss the opportunity to benefit from any seasonal increase in business volume.

The last example has to do with the availability of services in hostile environments or during major natural disasters. During events such as a tsunami or an earthquake, companies do not want to experience any loss of business data. Moreover, emergency response teams in affected areas need to have access to critical information to carry out their rescue missions. With Cloud computing adoption, companies should be able to recover the majority if not all of their data following a major disruption without having to pay for a backup facility. As most large Cloud providers have data centers deployed in multiple geographic locations, this deployment diversity allows them to provide backup and recovery. Cloud caching or Mobile Cloud Computing (MCC) [4] provides recovery and business continuity facilities even while basic infrastructures like the electricity grid or the optical fiber networks have not yet recovered from the disruption. Instead of building and managing a facility that will only be used in disaster situations, companies can now get the benefits of recovery and service continuity with a reasonably priced Cloud service.

10.1.2 Cloud Computing Is Not a Cure-All for Computing Challenges

Cloud computing introduces many features that help enterprises and government agencies build scalable and robust information technology systems. However Cloud computing cannot deal with every issue that these systems may face. In this section we discuss some problems for which the Cloud cannot offer a resolution.

One important issue that Cloud computing will not be able to improve is the performance of badly designed applications. The Cloud offers a well-defined architecture and patterns for Cloud services. Porting an application from a client/server architecture to the Cloud does not imply an automatic fix to any programming design deficiencies. Even if the Cloud platforms can mask the inefficiencies of the ported application, this does not mean that the application behavior and performance have been improved. The invoice from the Cloud provider will reveal those inefficiencies due to the excess consumption of Cloud resources due to inefficiencies of the deployed application will show up in terms of an excessive bill from the Cloud service provider.

Along the same theme of design issues, Cloud computing will not eliminate silos. In fact, it may even create new ones if the application design does not explicitly prevent this from happening. Silos may exist in information technology systems in terms of isolation of data, processes, and services. Using the Cloud may introduce new silos in companies' information systems as they create new entities that live in the Clouds.

10.2 Architecture: From the Cloud to the Mobile Cloud

In this section we present a "big picture" description of the concept of Cloud computing and we define the layers and the Cloud services provided by each layer. We introduce the differences between the types of the Cloud computing and present features, business benefits, metrics, and the key platforms from the vendors. We discuss also Cloud caching, as a base for *MCC*, and the integration of Cyber-Physical systems (CPSs) into the Cloud. We conclude the section with guidance as best practices to define a robust Cloud architecture.

The Cloud computing paradigm is based on a layered architecture. Each layer offers a collection of services, which can be presented as a layered *Cloud computing architecture* illustrated in Fig. 10.2. On the bottom of the stack, Infrastructure as a Service (IaaS) refers to computing resources as a service. This

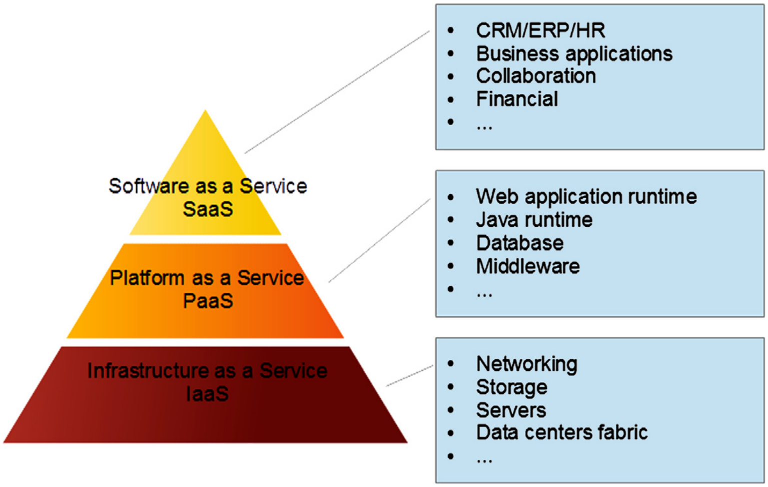

Figure 10.2 Cloud computing services' layers.

includes virtualized computers, processing power, reserved networking bandwidth, and storage services. IaaS services are offered by a variety of providers like Amazon AWS, Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM SmartCloud Enterprise. Amazon Web Services [5], for example, offers a full range of computing and storage offerings in the IaaS layer. This offering includes on-demand instances such as virtual machines. Moreover it offers specialized services such as Cluster GPU instances, Amazon Elastic Map Reduce (EMR), high-performance SSDs on the storage side, and Elastic Block Storage (EBS). In addition the Amazon AWS IaaS solution offers infrastructure services such as archival storage called Amazon Glacier, in-memory caching services called ElastiCache, and both NoSQL and relational databases.

The middle layer of the stack is the Platform as a Service (PaaS) layer; this layer shows some similarities to IaaS. However, the PaaS includes required services, including the operating system needed for a particular application. The PaaS layer offers programming languages support for your application, server side technologies, and data storage options. The support for developer tools and applications integration is also very important. PaaS services are offered by a variety of providers like Engine Yard, Red Hat OpenShift, Google App Engine, Heroku, AppFog, Windows Azure Cloud Services, Amazon AWS, and Caspio. To illustrate the PaaS services, we give as example the services offered by Engine Yard. This provider is designed for web application developers using Ruby on Rails, PHP, and Node.js. Engine Yard allows developers to take advantage of Cloud computing without responsibility for the management operations in the infrastructure level. Engine Yard runs its PaaS platform on top of the Amazon Cloud and provides key operations tasks such as performing backups, load balancing, managing clusters, administering databases, and managing snapshots.

The top layer on the Cloud stack is Software as a Service (SaaS). At this level businesses delegate the hosting and the management of their applications to Cloud providers. The applications are available on-demand and typically paid for on a subscription basis. SaaS providers offer solutions including anywhere access, minimal administration, minimal maintenance, and improved communication.

When we talk about the Cloud layers, they may be implemented in three different ways [6]: as a public, private, or hybrid Cloud. An implementation on a public Cloud means that the complete computing infrastructure is located on an external Cloud computing provider that offers the Cloud service. In this type of Cloud the provider has the physical control over the infrastructure and the location of the resources allocated to the consumer. The advantages of the public Clouds are the usage of shared resources, they do excel mostly in performance. However, the drawback is vulnerability to various attacks. In the private Cloud, the infrastructure is used solely by one organization and those resources are not shared with any others. The organization acts at the same time as a Cloud producer and consumer. The resources may be local or remotely located. Some Cloud providers, such as a private Cloud externally hosted, offer solutions. To keep a physical control over the infrastructure, the organizations have an option of choosing an on-premise (or locally hosted) private Cloud as well which is more expensive. The advantages of the private Cloud reside in the usage of private network that introduces a higher level of security and control. The drawback is the cost of the infrastructure. Thus the cost reduction is minimal in such solution where the organization needs to invest in an on-premise Cloud infrastructure. In the hybrid Cloud the organization uses an environment that combines multiple public and private Cloud solutions. A typical usage of the hybrid Cloud is to use the public Cloud to interact with customers and keeps the data secured through an on-premise infrastructure in the private Cloud. However, this kind of usage introduces a drawback in the additional complexity of determining the distribution of applications across both a public and private Cloud.

The hybrid Cloud is used nowadays as a basis for the *MCC*. Mobile devices have more constraints on their processing power, battery life, and storage than regular computers. Cloud computing is used to provide an illusion of infinite computing resources for those devices. MCC is thus a platform combining the mobile devices and Cloud computing to create a new infrastructure and architecture for the development and the usage of the mobile applications. This architecture delegates the heavy lifting of computing-intensive tasks and storage of massive amounts of data to the Cloud infrastructure. Fig. 10.3 illustrates the architecture proposed for the MCC and its position in the general Cloud architecture.

Mobile devices are increasingly essential to everyday human life as the most effective and convenient communication tools. The unbounded time and place usage introduced by those devices allows mobile users to accumulate a rich experience of various services and applications. The execution of those services is not limited to the mobile device itself, more and more applications use nowadays remote servers via wireless networks

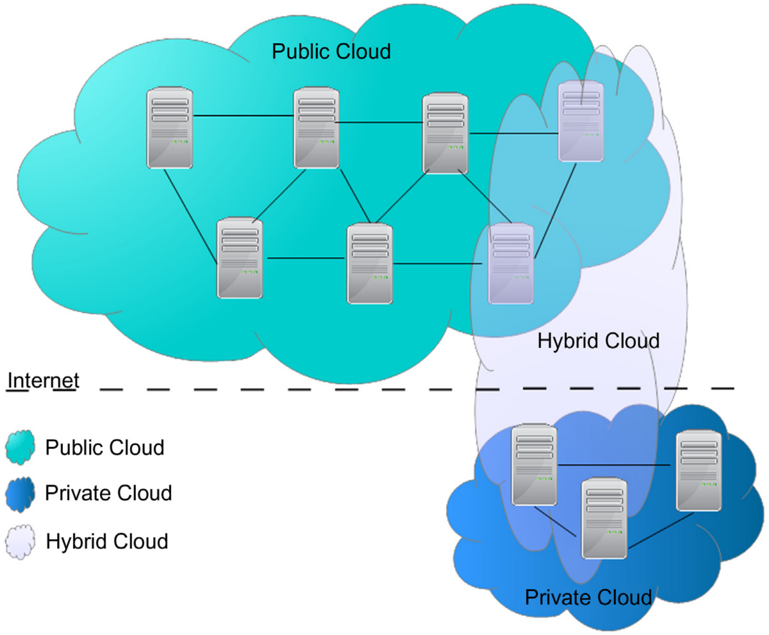

Figure 10.3 Cloud types.

to interact with services. Architectures based on *n-tier computing* have become a powerful trend in the development of information technology as well as in commerce and industry fields on mobile computing. Such systems can accept any (finite) number of layers (or tiers). Presentation, application processing, and data management tiers function is physically separated from the others.

However, mobile devices have considerable hardware limitations. Mobile computing faces many challenges in attempting to provide the various applications living on a single device with limited resources such as battery, storage, and bandwidth. Communication challenges like mobility and security arise, too. Those challenges motivate the delegation of the resource-consuming application modules to remote servers using Cloud service platforms. Google offers one of the major solutions called AppEngine allowing developers who do not need to have any previous understanding or knowledge of Cloud technology infrastructure to deploy services and use the Cloud. This platform executes the deployed services and exposes them as a remote service. This approach is used to delegate massive computation pieces of mobile software to the Cloud infrastructure.

Indeed, the mobile Cloud is a hybrid Cloud that offers services for mobile devices and CPSs [7] like *smart cars* and more

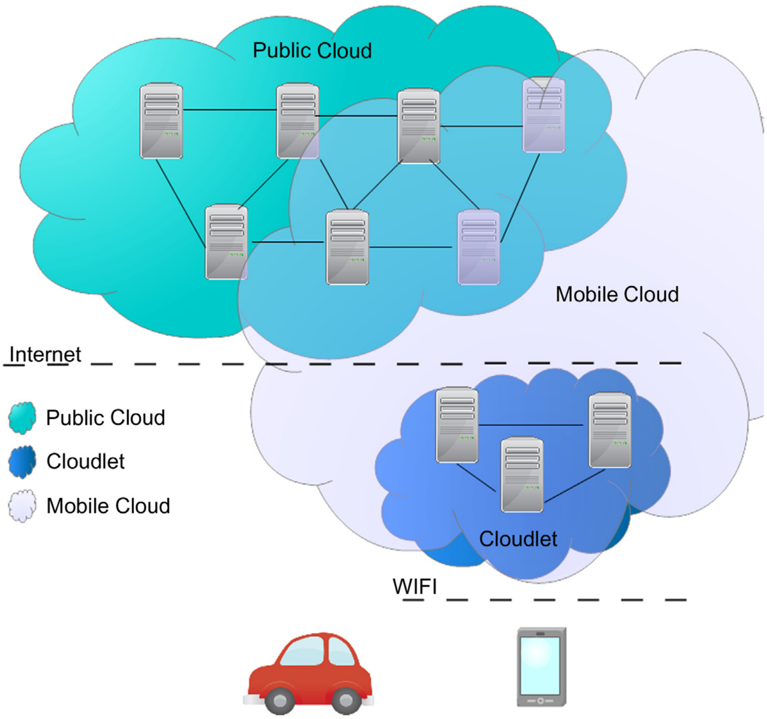

Figure 10.4 Mobile Cloud.

generally to smart devices in the transportation domain. Automobile makers are already in the process of migrating *navigation services* to the Cloud. This Cloud extends the processing capabilities for those devices using the Cloud paradigm. As illustrated in Fig. 10.4, the mobile Cloud uses a hybrid Cloud composed of a public Cloud and a private Cloud, sometimes referred to as a “Cloudlet.” The Cloudlet is a private Cloud infrastructure directly accessible from the mobile devices and contains virtualization capabilities adapted to mobile systems. The mobile Cloud allows consumers to access the Cloudlet when possible—if the Cloudlet is not available, the public Cloud is used to run the mobile applications.

In the case of CPSs the mobile Cloud offers *virtually* unlimited resources to the “Cyber” part of the CPS. CPSs are systems that integrate decision/computation and the ability to sense or impact physical processes, where the measurement of physical processes may provide inputs to decisions or computations whose outputs may trigger actions that modify the energy and material flows that make up the physical world. The mobile Cloud offers a solution that extends these *feedback loops* to the

Cloud in a way that can integrate remote computing infrastructure with the sensors and actuators. Cloudlets offer a way to have an on-premise infrastructure that is available even if the remote access to the public Cloud is unavailable. Such mechanisms are very important for CPSs as they may be part of systems that help the rescue efforts to organize evacuation after an earthquake of in other situation in environments qualified as hostile. Because they operate in hostile environments, CPSs need to be agnostic to the global network, for example, in case of *emergency response systems*. Using mobile Cloud services for CPS gives many benefits. In addition to the security introduced by using a private network, the continuity of services is clear benefit of such a solution. Moreover the Cloud offers a level of scalability that cannot be achieved by using embedded microcontrollers for the CPS. In the case of important updates of the CPSs, the Cloud offers also the possibility to *remotely update* all the cyber parts at a vastly reduced cost.

10.2.1 Business Benefits

Building applications in the Cloud offers several benefits to organizations. One important benefit is related to the cost of installation. Building a large-scale system is a big investment in terms of cost and complexity. It requires investment in hardware infrastructure including racks, servers, routers, and backup power supplies. It also requires a location for the data center that requires investment in real estate and physical security. Moreover it necessitates recurring charges for hardware management and operations personnel. The delays to obtain approvals for this high upfront cost would typically involve several rounds of management approvals before the project could even get started. The Cloud-based solution bypasses such startup costs.

Even if the organization has an existing on-premise infrastructure, the scalability of an application could be a problem if this application became popular. In such cases you become a victim of your own success when the on-premise infrastructure does not scale to offer the resources needed by the application. The classical solution of this kind of problem is to invest heavily in infrastructure, hoping that the popularity of the application will be addressed by the size of the infrastructure. By using a Cloud infrastructure, the Cloud provider manages the infrastructure and you can rescale the infrastructure allocated to the deployed application in a just-in-time manner. This feature increases agility, helps the organization reduce risk, and lowers operational cost. That means that the organization can scale only as it grows. Moreover the organization only pays for their real resource usage.

To have a more efficient resource utilization, system administrators have to deal with ordering delays while procuring hardware components when the datacenter runs out of capacity. They also have to shut down some parts of the infrastructure when they have excess and idle capacity. By using the Cloud, the management of resources becomes more effective and efficient, since system administrators can have immediate resources *on-demand*.

Cost is one of the most important factors for businesses. With on-premise infrastructures, organizations have fixed costs, independent of their usage. Even if they are underutilizing their data center resources, they pay for the used and the unused infrastructure in their data centers. The Cloud introduces a new dimension of cost saving that is visible immediately on the next bill and provides cost feedback to support budget planning. The usage-based costing model is very interesting for organizations that actively practice application optimization. Applying an update that uses caching to reduce calls to their back office by 50% will have an immediate impact on costs. This savings will accrue immediately after the update. This on-demand costing model also affects organizations that have picks of activity. The picks will be reflected on their invoice as an additional charge.

Organizations where the business is *data analysis oriented* can get impressive results in term of the reduction of *time to market* by using the Cloud. Since the Cloud offers a scalable infrastructure, *parallelization* of data analytics is one effective way to accelerate time to results. Putting parallel analysis processes, which normally take 100 hours of effort on a machine, on 100 instances in the Cloud will reduce the overall processing time to 1 hour. Swapping machine instances is at the heart of the Cloud IaaS. Moreover Cloud providers offer specific solutions to exploit parallelization using big-data techniques. By using this elastic infrastructure provided by the Cloud, applications can reduce time-to-market *without any upfront investment*.

10.2.2 Metrics

This section introduces an approach to defining and representing the concepts and uses of measurement within the context of Cloud services and their underlying components. However *Cloud metrology* is not necessarily well understood by the stakeholders. Metrics and measurement artifacts often have several definitions, which make it very difficult for the service customer to use these metrics as a thrusted and standard measurement method. We propose a focus on Key Performance Indicators (KPIs) [8] as a framework to help organizations to define and measure progress toward organizational goals. The KPIs in Cloud services aim to be the measurement indicators for the adaptation and the progression of the Cloud services according to the organization's objectives.

Acquiring new customers and growing the business are the main challenges of organizations that are using the Cloud services to host their applications. These organizations need to consider seriously the metrics that show their ability to generate recurring revenue, retain customers, and to attract customers at a reasonable acquisition cost. Organizations nowadays use some common Cloud metric KPIs as described below.

One of the most important Cloud KPIs is the Customer Retention Rate (CRR). This KPI has three main impacts on subscription-based businesses. It affects the customer satisfaction levels, the recurring revenue, and the growth of the business. The value of the consumer retention is very hard to overstate and this holds for all the organizations, independent of their activity sector. According to research [9], an increase in consumer retention, even a modest increase, can have a big impact on the profits. This study shows that a 5% increase in consumer retention can bring an increase of more than 50% on the organization profits. The *consumer retention rate KPI* is interesting for organizations since they can anticipate the investment in marketing required to keep their sales rate stable. Indeed, generating revenue from loyal customers is less expensive than generating revenue by acquiring new consumers.

Financial institutions and telecommunication companies tend to have subscription-based businesses. The monthly recurring revenue is at the center of those organizations business model. One of the top priorities for these types of organizations is increasing the revenue from current customers. The *Monthly Recurring Revenue (MRR) KPI* helps those organizations to measure customer satisfaction and loyalty.

Indicators and metrics related to consumers and revenue are very important to the Cloud-based businesses. However they are not the only important metrics that organizations should monitor. KPIs related to the software development and deployment life cycle have a big impact on their businesses. The ability to deliver software updates faster to meet the consumer needs, with fewer malfunctions, and faster resolution of reported problems allows organizations to produce valuable software that will be deployed in the Cloud. DevOps [10] is a development methodology that helps organizations to achieve those objectives.

DevOps-related KPIs are used to define measurable goals that associate the development and the deployment life cycle to the organization's objectives. They are used to analyze what went wrong and allow teams to be transparent and share metrics with other teams on the organization like customer support and sales.

One important indicator for DevOps is the *Feature vs Bug (FVB) KPI* that monitors the number of bug issues as compared to the number of feature issues. This indicator allows the team to see how bugs, which are issues related to failure to meet specifications that teams have to fix, compare to feature issues that require changes to specifications. This indicator helps to adapt the speed of the team's efforts to fix these fundamentally different issue types. Teams use this indicator to monitor whether feature issues are within feature limits and that the current bug issues are within bug limits.

Another interesting indicator is the *Project Burndown (PBD) KPI*. Since Agile [11] methods recommend an *iterative and incremental cycle*, the PBD KPI is a metric that displays and compares project iteration projections to the number of iterations completed in the project. This metric allows you to keep a close eye on project iterations and, especially, on how they compare to the number of iterations that the DevOps team thinks they can complete.

10.3 Safety Concerns

Safety is a topic that is a challenge to Information and Communications Technology (ICT) in general. Safety is the concern about hazards that may result from malfunctioning behaviors of a system, whether they be from the cyber or the physical realizations of the system or from interactions between them. This challenge is also relevant to the Cloud since it has a prominent place in the organizations' ICT strategy. The organization that uses the Cloud needs protection from failures, damage, accidents, and harm. Moreover, they need to define boundaries and responsibilities in terms of harms and hazard against their Cloud provider. Indeed, the Cloud is used in many applications that enable sensing and actuation in the real world. Consider the emergency response example presented in Section 10.1.1. The Cloud is an active part of the emergency system and may affect the physical world through the actuators. Nevertheless the controllers of such systems are actually deployed in the Cloud, any dysfunction of the Cloud may introduce severe hazards into the system. Those hazards are directly related to the applications built on top of the Cloud. Those hazards are not related to the essence of the Cloud as it is used to host the virtual part of such a system. However they are relevant to the overall system where the Cloud deployed services are connected with the physical part of the system to build the CPS system.

The rest of this section discusses safety concerns related to the Cloud in order to help organizations define an efficient control of recognized hazards to achieve an acceptable level of risk. This section focus on two aspects of the Cloud where the risk is omnipresent: on-premise Cloud and Cloud storage.

The sections that follow deal with hazards for Cloud infrastructure for owners, operators and some hazards for Cloud customers. A complete safety analysis of Cloud computing should also examine hazards to owners and users of the systems 'connected by the Cloud' and would involve some kind of distributed interface agreement between Cloud and Cloud customer, at a minimum. This is little study of this topic currently but the reader should anticipate a much broader and deeper discussion of Cloud computing safety.

10.3.1 Data Centers

By opting for an on-premise Cloud solution, the organization has to manage server and hardware in data centers. To ensure a safe working environment in such space, the potential risks that hardware and the personnel may be exposed to need to be considered seriously. The risks include common risks such as fire and natural disasters. It also includes specific risks of information technology systems such as hardware failure, outages, electrocution, and physical injuries. To avoid and mitigate these risks, proper inspections, procedures, and training need to be part of the initial investment. Failure to prepare for such risks can be the main cause of outages in your data center. Moreover, the impact may be an Occupational Safety and Health Administration (OSHA) [12] noncompliance issue or injury to an employee. Organizations that choose an on-premise solution cannot expect that safe workplaces just happen, they have to put safety as a primary concern and plan and act to have a safe work environment.

Safety begins at the design level. Indeed, data center safety planning should be part of the initial design. This plan needs to take in consideration the analysis of the operations done to install and maintain the hardware. This includes the physical implementation steps that operators take to mount/relocate racks, load/unload servers, monitor the servers, and to perform the routine physical maintenance tasks. One of the actions that can be taken at the design level is the development of a well-designed floor plan that maximizes safety and simplifies emergency evacuation. In addition, improvement of the center's wiring contributes to data center safety. The organization should remove hardware hazards like the "spaghetti" of networking cables or holes in raised flooring those employees might trip on. Organizations should not minimize the impact of such simple and straightforward practices, neglecting those practices when facilitating server upgrades or network expansions may adversely impact the real possibility of physical injury.

Maintenance of the safety-related installations is an important item for the operating data centers safety. For business purposes, organizations focus the maintenance activities on testing the reliability of backup electrical systems like power distribution units and UPS's. However, fire detection and suppression systems deserve attention when it comes to maintenance. It is critical that these safety installations be regularly inspected and maintained. Nevertheless evacuation plans should be kept fully uptodate and available. Not only the evacuations plans, but also all the work instructions have to be clear and well defined. The employees working in data centers should know precisely what the organization expects of them. Providing thorough training, unmistakable diagrams, and clearly written instructions is the best way to help employees understand their responsibilities. Basic data center safety instructions for lifting hardware and operating a server lift should be included in the organization's work process documentation.

The safety process is not a one shot effort; the organization managers should watch and learn how each employee performs their everyday operations. This tracking has two objectives. The first is to have the assurance that the employees are following the safety procedures. Especially the assurance that they are not taking shortcuts that could compromise data center safety and expose them to injury or other risks. The second is to improve the existing procedures based on the employees' feedback. The safety process should not be limited to every day operations. The organization needs to include procedures for natural disasters in the safety process. Employees should be trained on preparedness for natural disasters that includes earthquakes, floods, hurricanes, and tornadoes. In some geographic areas, those who are most prone to these types of disasters, common practices verification such as anchoring equipment and storing materials in addition to the procedures for evacuation and holding areas should all be well-defined, tested, and well-understood by all the employees.

10.3.2 Cloud Data Storage

Multiple elements define just how safe Cloud storage is and which are the different security aspects that define safety. An organization that uses the Cloud, especially for critical data, needs to have assurance of the safety and the reliability of the infrastructure on which their information will be stored. The Cloud storage providers apply many safety mechanisms. Even with the hackers' attacks on those infrastructures, those of the Cloud providers, Cloud storage remains one of the safest and the most reliable ways to store data. The Safety of the stored data is one of the main reasons that encourage Cloud consumers to use such platforms. Thus Cloud storage providers use many techniques to assure this safety.

The storage safety involves keeping data out of the reach of hackers. For the data safety the providers use encryption as front line of defense to avoid hackers' attacks. The encryption methods used to transfer the data from/to the Cloud storage are based on complex ciphering algorithms for better protection. A key is shared between the Cloud provider and the consumer. This key allows both of them to cipher and decipher the transmitted data. Even if the hacker is able to get the data by sniffing the network, he will need the key to decipher the encrypted data. Although encrypted information may be cracked, decryption requires processing power that is not available everywhere, dedicated software for forensics, and enough time, all of which discourage malicious attackers. To achieve 100% safety assurance, relative to network-based attacks; the only solution is to keep the data offline. However Cloud storage providers utilize more complex security methods than average organizations [13]. Those methods allow the Cloud storage providers to achieve an acceptable safety assurance for the majority of businesses. Nevertheless the data stored in the Cloud profits from an added level of protection since organizations delegate safety to the providers that have this concern at the heart of their business.

When organizations use Cloud storage infrastructure from a provider, it implies that they delegate all the safety concerns related to the physical storage to the Cloud provider. The concerns that remain the responsibility of organizations are those related to the safety of data transfer and the robustness of the procedures implemented by the provider. Security is one of the decisive arguments for an organization in migrating to the Cloud. Safety is one of the top priorities of the majority of the institutions. Especially for government agencies and financial institutions, safety is paramount. The Cloud providers cannot assure a 0% risk on their platforms, the risk of a data breach is always a possibility.

Organizations need to evaluate this risk to enjoy the benefit of the Cloud without ruining their business. To evaluate the risk of data breaches, organizations need to realize that those data breaches occur on out-of-date online systems that are still using out-of-date security measures. Migration to the Cloud challenges organizations to rethink the design of their systems, embracing the latest technology means that the organization will avoid all known data breaches and assure the best state-of-the-art safety methods' usage. Organizations should not be afraid to upgrade their systems to use Cloud storage. The Cloud will encourage them to use safer technologies and methods that will not introduce new risk for security breaches. Cloud storage is safer than the legacy servers are. However migration to the Cloud should be accompanied by the employment of best practices to keep the business safe.

Mobile devices introduce new challenges [14] in addressing Cloud safety concerns. Bring Your Own Device (BYOD) is an Information technology policy where employees are encouraged to use their personal mobile devices to access the organization's data storage and systems. Organizations have to know the devices and the employees that are using those devices. Indeed, some employees do not prefer to have separate devices for personal use and for work. Especially on the modern workplaces where the teleworking is encouraged. From the organization's perspective, the BYOD may be efficient if everyone understands how to keep the devices and the systems safe. Safety procedures should be defined for the usage of all the personal devices in addition to a good monitoring solution to track the access of those devices to the system. Nevertheless holding frequent meetings to communicate and inform about safety concerns is important. For example, what applications are secure and which personal device is safe in addition to reminding employees about the mandatory protection rules whenever they are away from their desks.

Once again, a complete study of Cloud computing safety remains to be done and will surely be the topic of future publications on the topic.

10.4 Cloud Security

An organization that moves its applications to the Cloud will not make the application security responsibilities disappear by design. The organizations need to anticipate risks and develop creative ways to mitigate them. This section discusses why the organizations should not fear the switch to the Cloud, stresses the threat profile associated with the Cloud usage, and gives a list of the best practices that the organizations should apply to secure their deployed applications on the Cloud.

Indeed, information technology businesses are known for their propensity for innovation. However many of those businesses struggle with lingering apprehensions about switching to the Cloud. The hesitation is not caused by specific security concerns, but a limited number of common security issues. These common concerns cause them to overestimate the risks involved in switching to the Cloud. One of the main concerns that cause anxiety for decision makers of the organizations is the simple fact that the security means different things to different decision makers. The Cloud is associated by many with a convenient place to store music and photos online. However, for technically oriented employees, it means a complete software execution environment of an infrastructure for desktop-as-a-service desktop virtualization.

To establish security protocols [15] that allow organizations to stay protected while switching to the Cloud, the role that the Cloud should play has be clear and well-defined. Misunderstanding the role of the Cloud may have a negative impact on the security. Since the Cloud includes multiple concepts, designed to address many business needs, those concepts should not be merged into a solution without fully understanding the desired outcomes. Clearly articulating the needs and the Cloud concepts addressing those needs is the key to success in the switch to the Cloud.

Cloud migration changes the way that organizations manage the information technology infrastructure. Organizations need to give up some control of hardware to the Cloud providers and, relinquishin doing so, relinquish control over where their data are stored and who is accessing the servers where their data are stored. The organization needs to understand that once the data are transferred to the Cloud, their teams are no longer responsible for the data and it is instead the Cloud provider professional that is responsible for all the aspects of the data storage including the security and the isolation of the data.

Giving up the control to the Cloud provider may cause concern from the organization's employees. If the organization is migrating from an on-site infrastructure to an external Cloud provider for example, delegating the management and the control of the servers and the data storage to the Cloud may cause a fear of losing jobs. The managers need to explain that this drastic organizational change may be a good opportunity for the impacted employees to stay current and adopt new skills. The employees need to understand that maintaining outdated resources is not the interesting part of the organization's business and they need to focus on new skills that are of more value to the business. Moreover, since technology changes all the time, this is an opportunity to acquire and maintain state-of-the-art skills. This change will benefit at the same time the employees' resumes and the organization's business.

Potential for data loss is one of the most persistent and concrete fears associated with Cloud storage. There is no assurance of 100% security and safety for the data neither on traditional systems nor in the Cloud. However organizations can combat this fear by finding a Cloud provider that offers comparable assurance to the traditional system. Some Cloud providers offer back up, disaster recovery, etc.; those features can help the organization to determine if the provider is suitable for the criticality of their business needs.

10.4.1 Threat Profile

Security threats in the Cloud are real. However most of those threat concerns are overstated, unfounded, and easily managed. Organizations need to build a threat profile adapted to their business activities. To build a threat profile, organizations need to consider first the common threats that are known. Based on those threats, they may identify which threat constitutes a real risk depending on their activities.

The possibility of a data breach is one of the biggest fears related to working in a Cloud. External threats from hackers and malware may have their roots in many factors including the design, the implementation, and the configuration of the Cloud application. Since applications run in multitenant environment, organizations cannot control what the other users are doing. This concern is not a specific to the Cloud; even for traditional networked applications, the threat is real. However organizations need to estimate and manage the risks of exposing their applications on the network. The average attack of networked applications for organizations according to [16] is more than 15,000 attacks per year. The Cloud providers offer techniques to avoid such attacks, like Denial-of-service (DDoS) [17] that could compromise organizations' data and services.

The first line of defense for security in the Cloud is encryption. However traffic hijacking is a threat that involves the theft of security credentials. It allows the hijacker later gaining access to an organization's privileged information. Hijackers can use this stolen information to eavesdrop on transactions and perform modifications of data. The objective of the hijackers may be financial gain and it may be to disrupt the business. Even organizations that are big players in the Cloud may be affected by this threat. Amazon discovered a cross-scripting bug in 2010 that allowed Hijackers to steal the session IDs of certain users [18]. Amazon kept the number of affected accounts secret. Nevertheless all organizations that migrate to their Cloud might be vulnerable to this type of attack.

Threats do not come only from malicious attacks; hardware failure may cause severe damage to stored data and cause business damage to organizations. The policies regarding disaster management, the backup strategies, and datacenters' location have to be considered seriously by organizations as a part of their benchmarking to find the most suitable Cloud provider. Since they will delegate control over the physical location of the servers, they need to verify the provider's ability to handle emergencies and disasters.

Application programming interfaces (APIs) are exposed by the Cloud providers and used by organizations to access and control resources in the Cloud. Those APIs are designed for the application developers, they may suffer from a lack of documentation, or poor design. In some cases, third parties that adapt those APIs to a specific interface manipulate those APIs. The threat introduced by the APIs may affect the entire system. They are critical Cloud security vulnerabilities for many Cloud providers and consumers.

The DDoS attacks can have catastrophic implications for the organizations. As the pricing model for most Cloud providers is based on resource consumption, DDoS attacks may have a direct impact on costs. Even if Cloud providers have elastic resource allocation to avoid unavailability of the service, degradation of application performance may occur due to a centralized data management for example. The resulting downtime and other access problems due of the DDoS attacks may potentially leave the system open to other types of attacks.

As a multitenant environment, resources are shared between the organizations that are using the Cloud provider's infrastructure. Vulnerabilities may be introduced because of some isolation issues. The challenge in this context is to avoid this shared vulnerability. First, the organization needs to identify which Cloud provider uses the most sophisticated isolation technology to minimize the risk. Second, the organization needs to adopt additional security protocols to enforce the security and mitigate the shared vulnerability. For example, file system encryption for the data stored in the Cloud could avoid the risk of access to this data by malware introduced into the datacenter by other Cloud consumers.

The threat of attack is not only from outside hackers, malicious insiders constitute a growing risk in nowadays data centers. As the Cloud is becoming popular, the data centers are more implanted than ever. The Cloud providers have to manage multiple data centers. They contract freelancers to respond to some urgent demand on maintenance or upgrade on their data centers. The companies that are using the Cloud store their data and run their application on those data centers without any control over this infrastructure. Indeed, this complex task of managing the data centers has raised the possibility of an inside attack from an unscrupulous contractor. That makes insider attacks a growing Cloud security threat.

The Cloud is not only the target for the attacks; hackers use this infrastructure also as a vehicle for attacks. In the same way that the Cloud offers a scalable infrastructure for authorized business uses. Unlawful attacks can use the power of this anonymous infrastructure to launch session hijacking, complex DDoS attacks, spread malware, and share pirated material. The second-largest breach ever [18] was executed using Amazon infrastructure in April 2012 by an anonymous user against Sony's PlayStation Network. This attack allowed an anonymous user to access information of more than 100 million users. Even if these attacks do not affect directly the other applications running on the same Cloud. The Cloud providers cannot determine if the usage of their infrastructure is for authorized or unauthorized proposes. They can react only after checking for compliance for illegal or unethical uses of their infrastructure.

Failure of due diligence is the common characteristic among the majority of the treats related to the security of the Cloud. Organizations have the responsibility to ensure that the chosen Cloud meets their requirement in term of security. Moreover, they do not to rely on the Cloud provider for all aspects of security. They have to enforce the provider's security by adopting protocols and procedures to meet their specific requirements. Before the data or services are migrated to the Cloud, it is imperative to know the risks and understand the provider's security process. The providers have account specialists assigned to the organization to answer their questions. However, organizations need to be able to ask the right questions. Nevertheless organizations have the responsibility to know the legal obligations with regard to the confidentiality of their user's data. They have to be compliant with PCI, HIPAA, and other relevant regulations like data breach, backup failure, or insufficient record keeping.

10.4.2 Best Practices

Organizations outsource control when they move their data or their software to the Cloud environment. However they are able to maintain a perfectly safe and reliable secure system. The Cloud is an environment where the organization can benefit from the convenience and affordability in addition to the security and the safety. Knowing the Cloud security threats should encourage the organizations to implement control at the hardware, software, and procedural levels. This will help mitigate the risk and maintain tools to control and recover in the worst case. The organizations can adopt four main best practices to reduce concerns about the Cloud and make it safer and more secure.

The switch to the Cloud environment is not an arbitrary decision, an organization needs to plan this switch and begin with a thorough risk assessment. It should define how an outage would affect their business workflow, supply chain, and regulatory compliance. Even if the risk of outage exists, planning will help the organization to maintain business continuity in case of an outage or a security breach. The employees should be at the heart of the migration and Cloud-related operations. They should be consulted and informed of new protocols and rules for accessing to the Cloud resources.

The best defense against data and network-related threats is encryption. It assures the confidentiality of the information both on transfer and on the storage levels. The information should not be sent unencrypted to the Cloud. Important data should be encrypted before the transfer to the Cloud. In addition to regular encryption, the usage of an enterprise-grade protocol [19] is highly recommended for the most critical files and applications. Even if the data are encrypted, controlling and implementing privilege-based procedures for accessing data is a key for security. Employees should only access the information required to complete their job. These access policies prevent accidental security breaches and malicious insiders. The organization needs to define clear policies regarding authentication without over complicating [20] the procedure by using mechanisms like two-factor authentication.

The migration of the information technology system to the Cloud should be an integrative operation. Uncontrolled moves to the Cloud may introduce additional risk that is not need. The migration procedure should begin with the least-critical data. This will allow the organization to assess the policies and the procedures based on early feedback. Moreover in this manner employees will have time to become more comfortable with the new platform and to test for vulnerabilities. Some of the software is closely related to some specific data; the organization should determine which applications require interaction or rely on shared data. Those components have to be migrated at the same time to reduce latency issues. Nevertheless the migration to the Cloud is an opportunity for the organizations to update the software and operating systems and especially to update patches and licenses.

Cloud providers offer management and monitoring tools. The organization should take advantage of virtual management software that provides greater visibility into all the infrastructure activity, including networking and data storage. The majority of those tools offer notifications based on network events, suspicious behavior, and other correlations that may indicate an attack. This monitoring is not optional, many regulatory standards expect organizations to collect and monitor log data in order to be compliant with those standards.

The rewards associated with using the Cloud is worth the risk. Cloud computing is a technology that will be with us for a long time. Organizations are realizing the advantages of Cloud usage from the cost savings to scalability and monitoring. The failure of the Cloud migration is mostly due to the lack of preparation by organizations. The price of those failures may be high. Moving to the Cloud involves exchanging one set of responsibilities for another. The organizations give up the control over some aspects of security and they have to focus on other security aspects that are closer to their main business. For sure, it is possible to maintain an effective and proactive security posture after migrating business process to the Cloud.

References

[1] K.Y. Chung, J. Yoo, K.J. Kim, Recent trends on mobile computing and future networks, Pers Ubiquit Comput 18 (3) (2014) 489–491.

[2] P. Mell, T. Grance, The NIST definition of Cloud computing, Natl Inst Stand Technol 53 (6) (2009) 50.

[3] L. Wang, J. Tao, M. Kunze, A. Castellanos, D. Kramer, W. Karl, Scientific Cloud computing: early definition and experience, in: High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on, 2008.

[4] H.T. Dinh, C. Lee, D. Niyato, P. Wang, A survey of mobile Cloud computing: architecture, applications, and approaches, Wirel Commun Mob Comput 13 (18) (2013) 1587–1611.

[5] A. Wittig, M. Wittig, Amazon Web Services in Action, Manning Publications Co., 2015.

[6] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, et al., A view of Cloud computing, Commun ACM 53 (4) (2010) 50–58.

[7] R. Alur, Principles of Cyber-Physical Systems, MIT Press, Cambridge, MA, 2015.

[8] D. Parmenter, Key Performance Indicators: Developing, Implementing, and Using Winning KPIs, John Wiley& Sons, New York, NY, 2015.

[9] S.-C. Chen, A study of customer e-loyalty: the role of mediators, in: Proceedings of the 2010 Academy of Marketing Science (AMS) Annual Conference, 2015.

[10] W. John, C. Meirosu, P. Sköldström, F. Nemeth, A. Gulyas, M. Kind, et al., Initial Service Provider DevOps concept, capabilities and proposed tools, arXiv preprint arXiv:1510.02220, 2015.

[11] R. Levy, M. Short, P. Measey, Agile Foundations: Principles, Practices and Frameworks, London, UK, 2015.

[12] R. Administrators, D. Dougherty, Occupational Safety & Health Administration (OSHA), Washington, DC, 2015.

[13] S. Kamara, K. Lauter, Cryptographic Cloud storage, Financial Cryptography and Data Security, Springer, New York, NY, 2010, pp. 136–149.

[14] A. Bello Garba, J. Armarego, D. Murray, Bring your own device organizational information security and privacy, ARPN J Eng Appl Sci 10 (3) (2015) 1279–1287.

[15] U. Gupta, Survey on security issues in file management in Cloud computing environment, arXiv preprint arXiv:1505.00729, 2015.

[16] A. Potdar, P. Patil, R. Bagla, R. Pandey, Security solutions for Cloud computing, Int J Comput Appl 128 (16) (2015).

[17] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Comput Commun Rev 34 (2) (2004) 39–53.

[18] P. Mosca, Y. Zhang, Z. Xiao, Y. Wang, others, Cloud Security: services, risks, and a case study on amazon cloud services, Intl J Commun Netw Syst Sci 7 (12) (2014) 529.

[19] A.H. Ranabahu, E.M. Maximilien, A.P. Sheth, K. Thirunarayan, A domain specific language for enterprise grade Cloud-mobile hybrid applications, in: Proceedings of the compilation of the co-located workshops on DSM’11, TMC’11, AGERE! 2011, AOOPES’11, NEAT’11, \& VMIL’11, 2011.

[20] B. Schneier, Two-factor authentication: too little, too late, Commun ACM 48 (4) (2005) 136.