Addressing security challenges in cloud computing – a pattern-based approach

Priya Anand, Jungwoo Ryoo
College of Information Sciences and Technology
The Pennsylvania State University
University Park,
PA, USA - 16802
{axg36, jryoo}@ist.psu.edu

Hyoungshick Kim
Department of Computer Science and Engineering
Sungkyunkwan University
Suwon, Gyeonggi-Do,
Republic of Korea
hyoung@skku.edu

***Abstract*—Cloud computing has emerged as a fast-growing paradigm for storing/sharing data and delivering services over the Internet. It provides its users with a way to deal with information or data without investing in any new technology or resources of their own. Although cloud computing environment is viewed as a promising Internet-based computing platform, the security challenges it poses are also equally striking. Despite the rapid advancement of cloud computing technologies, security issues in cloud environments have to be addressed to a greater extent. Cloud security is one of the major issues that hinder the adoption of cloud computing and slow down its acceptance in many sectors. In this paper, we provide an overview of cloud computing, in-depth literature review on cloud security and privacy issues, and its research challenges. We also propose security patterns as a viable solution to cloud security and explain them with a simple template. The research goal of this paper is to provide a better understanding of cloud security and highlight the security concerns that should be addressed to realize the maximum benefits of cloud computing. Security patterns allow cloud developers to use security measures without being security experts. Also, a cloud environment can be reengineered by using security patterns to add missing security features. In this paper, we provide a pattern-based cloud security framework as a good practical approach to ensure security features in cloud environments.**

Keywords— Cloud security, security patterns, data privacy, security framework

I. Introduction

In recent years, the concept of cloud computing has grown from an emerging innovative architecture to one of the fastest growing IT segments. Ryan [1] defines cloud computing as "*the idea that data and programs can be stored centrally, in the cloud, and accessed anytime from anywhere through thin clients and lightweight mobile devices.*" Cloud computing provides many features like data ubiquity and resilience. Cloud computing provides more options to users because the data storage and processing are primarily handled by the cloud computing vendors. Therefore, the data is stored on a remote location, which leaves the user without an exact understanding of the storage location. In this paper, we explain major security challenges faced by cloud computing environments with an extensive literature review on cloud security issues. As our contribution, we propose the use of security patterns [20] in cloud computing as a solution to recurrent software security problems. Cloud computing environment involves multiple stakeholders like clients, software developers, security experts, and cloud vendors. Security patterns [20] are encapsulated solutions for recurring security problems. They also provide a communication vocabulary for software designers, developers and security experts. In an environment like cloud computing which comprises of various stakeholders, security patterns could serve the purpose providing guidelines for security across those stakeholders.

II. Overview of Cloud Computing

Cloud computing technology has been an evolving technology and also got a potential to continue to grow in the future. Cloud computing provides a way to move services and data to an internal or external, centralized facility or contractor[2]. Storing or sharing data in cloud environments would make data access easier, on-demand availability possible, at much lower cost with an enhanced collaboration capability, integration and analysis cheaper on a shared platform. There are many well-known service providers in the market, such as Google, Amazon, Yahoo, and Microsoft. There are also some vendors who provide cloud services in various deployment models and service models. According to National Institute of Standards and Technology (NIST) [19], "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*." NIST lists five essential characteristics, four deployments models and three service models that together categorize ways to deliver cloud services, and those categories are listed in Figure 1. As represented in Figure 1, we can deploy a cloud computing service by using three different models: 1) a private cloud, which functions solely for one organization in a private network, 2) a public cloud, which is owned by a cloud service provider and offers the highest level of efficiency in shared resources, 3) a hybrid cloud is a combination of private and public deployment models, 4) a community cloud is a collaborative share between several organizations from the same community with specific requirements. Cloud computing consists of the following service models: 1) Software as a Service (SaaS), which provides organizations with ready to use applications using a combination of cloud-based computing in storage services (e.g., Microsoft Business Productivity Online Standard Suite). 2) Platform as a Service (PaaS), where an organization is only responsible for the development, maintenance and management of data in the cloud (e.g., Windows Azure Platform). 3) Infrastructure as a Service (IaaS), where an organization gets infrastructure components and control over the entire IT infrastructure. However, those organizations have to allocate resources to maintain and manage the data in the cloud (e.g., Amazon EC2). Figure 1 also depicts five essential characteristics of cloud computing as 1) On-Demand Self-service, 2) Broad Network Access, 3) Rapid Elasticity, 4) Resource Pooling, and 5) Measure Services. The Common Characteristics of cloud computing environments are also enumerated in Figure 1.

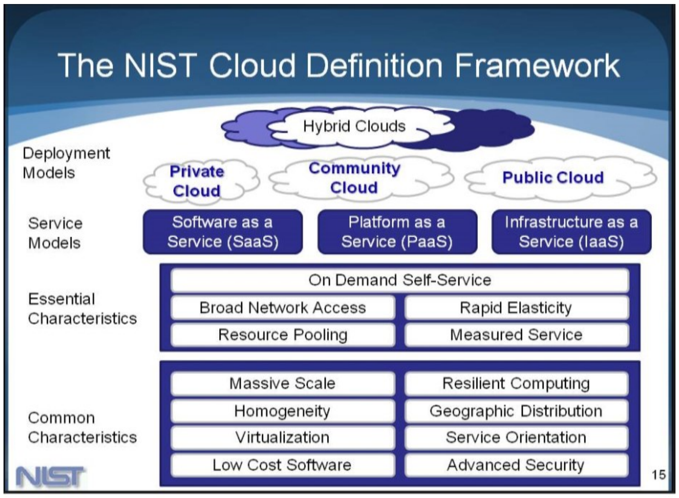


Fig.1. NIST [19] Cloud Definition Framework
Source:https://digitaliser.dk/resource/571879

III. Related Research

A. *Security challenges based on encyption techniques:*

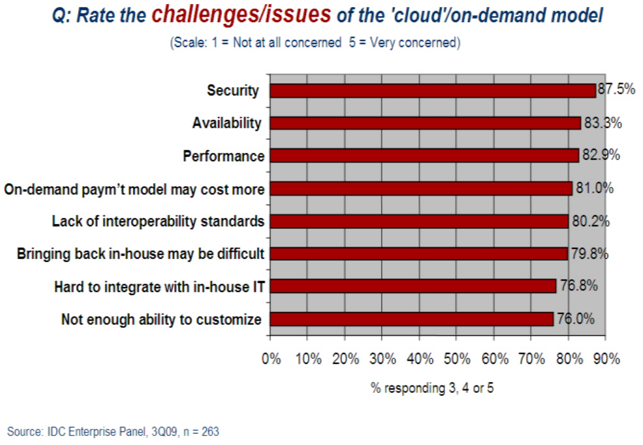
Ryan [1] stated the following aspects of cloud computing security issues: 1) Cloud, being a shared environment allows any sharer to become an attacker, 2) Cloud-based data access is possible from insecure protocols across any public networks 3) Data stored in the cloud may be lost or accidentally/intentionally modified by the cloud vendor, 4) Any employee, sub-contractors or the cloud provider has access to the data stored in the cloud. The author claims that the first three issues are not very specific to cloud computing but stresses that vendors'/employees' data access possibility poses a serious security threat on data confidentiality. Cloud provider may not manipulate the data, but the very fact that the provider can view the data without authorization is a serious security breach. Ryan proposed four different encryption techniques from the literature [10, 11, 12] as potential solutions to block the unauthorized data access by a cloud provider. This paper purely focused on the confidentiality viewpoint of the data. In this study, authors discussed the confidentiality issues by considering cloud-computing-based conference management systems like EDAS [29] and EasyChair [30] as case studies, which are relatively small-sized clouds. From the scalability viewpoint, the proposed encryption techniques may not satisfy the security requirements, and the author confirms it by stating, "*the question of how applicable it is to real cloud computing problems is not clear.*"

B. *Challenges to maintain privacy in clouds :*

Popovic and Hocenski [4] highlighted top ten cloud security concerns in their study. They emphasized the lack of knowledge or control of where the resources run, who controls the encryption/decryption keys, law violation of data seizure (by foreign governments) as major security challenges. Authors also claim data integrity, some government regulations on some sensitive financial or PII (Personal Identifiable Information) data to be remained in their home country as a serious security concern cloud computing technology is facing. Their study concentrates on the difficulty in ensuring the auditability and consistency of records due to the dynamic and fluid nature of virtual machines. After an analysis on current security countermeasures used in cloud computing, Popovic and Hocenski [4] described twenty recommended security management models that should be maintained by cloud service providers. Basically, those management models are focused on security requirements from vendors than a helping model for users. According to the survey conducted by International Data Corporation (IDC), among 263 IT executives to gauge the challenges involved in using cloud services, security was ranked as the biggest challenge (See Figure.2). Jensen et al. [2] identified XML signature, browser security, cloud integrity, binding issues and flooding attacks as significant cloud computing security issues. XML Signature Element Wrapping attacks [13], commonly referred to as wrapping attacks, is an attack on protocols using XML signatures to break the integrity and authentication policies of a system. This attack takes place while using web services, and cloud computing uses web services. Hence wrapping attacks are possible in cloud computing as well. Jensen et al. [2] state that "*current browser-based authentication protocols for cloud computing are not secure when the browsers cannot issue XML-based security tokens by itself.*" Jensen et al. [2] discussed how cloud malware injection attack and Metadata spoofing attack can introduce integrity threats to the data stored in the cloud. The authors investigated the effect of flooding attacks in cloud environments, which occur when a hacker sends a bulk amount of irrelevant or unnecessary requests to a service to launch a Denial of Service (DoS) attack to the server hardware [15].

C. *Security challenges based on cloud types:*

Kuyoro et al [3] studied the cloud computing security issues and challenges by focusing on the cloud deployment and service delivery types. Clouds can be deployed as three different models, Private, Public or Hybrid clouds [3]. Authors stated that the private clouds are much safer than public clouds since all cloud resources are managed by the organization that maintains the cloud. Public clouds, typically a pay-per-use model poses a security threat, since the data is shared with an off-site third-party provider. Hybrid cloud is a combination of private and public clouds that provide more control over the data, and also various users can access those data through the Internet. In this classification model [3], authors failed to compare the cost models in maintaining these deployment models and security trade-offs.



Source: IDC Enterprise Panel, 3Q09, n = 263

Fig. 2. Security challenges and issues in cloud computing Source: Popovic, Kresimir, and Zeljko Hocenski. "Cloud computing security issues and challenges." *MIPRO, 2010 proceedings of the 33rd international convention*. IEEE, 2010

D. *Security challenges based on cloud deployment models:*

Ramgovind et al. [5] explained three broad deployment models: Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS) and highlighted security issues that are specific to each deployment model. Upon deciding on a cloud delivery model (Private, Public or Hybrid) and deployment model (IaaS, SaaS or PaaS), authors enumerated the security concerns that security professionals and users should be aware of in the current cloud computing environment. The authors incorporated several security issues emphasized by Gartner [14] into their investigations on information security issues when dealing with cloud computing, which are privileged access, regulatory compliance (external audits, security certifications, etc.), data location (client's control over the location), data segregation (is encryption available at all stages to all clients?), recovery (disaster management), investigative support (ability to investigate illegal/inappropriate activities), long term viability (if a vendor goes out of business), and data availability (if the vendor moves to a different environment).

E. *Serious threats faced by cloud computing environments: :*

Zissis and Lekkas [7] enumerated the security challenges in cloud computing and identified the key features of cloud computing as flexibility/elasticity (quick and easy access), broard network access (used from heterogeneous platforms – mobile phones, PCs, Laptops, etc.), location independence, reliability (use of multiple redundant sites), economies of scale and cost effectiveness (no maintenance required) and sustainability. Zissis and Lekkas [7] also argued that the adoption of this innovative architecture and its broad key features opened up the window of many uncategorized threats.

Subashini and Kavitha's work [8] surveyed the cloud security issues related to service delivery models. Along with all the aforementioned security challenges, the authors highlighted the need for network security while deploying SaaS model. In a SaaS model, data is obtained from the user, processed by the SaaS application, and the information/data is stored in the cloud. In this process, a large amount of data transfer takes place in the network, and the authors emphasized the need for network security [8].While cloud computing security challenges were discussed by many researchers [3, 4, 7], Morsy et al. [9] identified some root causes and key participating dimensions for security issues in cloud computing. Their research identified multi-tenancy and elasticity to be the key characteristics that could have serious security implications in a cloud. Their proposed solution to accomplish secure multi-tenancy is to maintain isolation among tenants' data by the cloud vendor. The field of cloud computing is not fully mature [9], not to mention that the security aspects of cloud computing is still under exploration. In most cases, security is considered as an afterthought and almost always comes as a Band-Aid solution once the attack takes place.

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

In this section, we elucidate some predominant security threats in cloud computing environments. In 2013, Cloud Security Alliance (CSA) identified the top nine cloud computing threats as "The Notorious Nine," based on its survey among the industry experts [18]. According to the report, nine critical threats are (in the order of severity): 1 – Data Breaches, 2 – Data Loss, 3 – Traffic Hijacking, 4 – Insecure APIs, 5 – Denial of Service, 6 – Malicious Insiders, 7 – Abuse of Cloud Services, 8 – Shared Technology Issues, 9 – Due diligence [18].

A. *Data Breaches*

In cloud computing environments, consumers/users are not the only people to have control over data stored in the cloud. In fact, consumers get a relatively low control over the data than the cloud vendors. In a desktop environment, data or information is not shared with any third party vendors or organizations. This alleviates the confidentiality issue from the desktop computing, which is a serious issue in cloud computing [8]. If a multitenant cloud is not designed with required security measures, an attacker can get access to all data stored in the cloud. A consumer may not be a target of an attacker but still becomes a victim of data breach when his multitenant cloud is compromised.

B. *Data Loss:*

While data loss can happen in any computing environment, the prospect of data theft /loss without a trace is very high in cloud computing. Users can always back-up data to overcome this challenge, but that reduces the advantage of using cloud services. In case of desktop storage, users can implant their own safety measures against natural disasters, and the kind of natural disasters will be immediately notified to the user without relying on a third party.

C. *Traffic Hijacking:*

In cloud computing, every transaction generates network traffic between client and the cloud. When an attacker gets access to a user's credentials, an attacker can eavesdrop on the activities and transactions (i.e., packet sniffing, IP spoofing, information leakage, etc.), manipulate data (therefore breaches data integrity) or redirect the clients' requests to illegitimate sites (e.g., Man-in-the-Middle attack) [15]. Hardware or network integrity has to be provided by the cloud vendor.

D. *Insecure APIs:*

A basic cloud architecture relies on the interfaces for cloud management, orchestration and monitoring. Application Programming Interfaces are an integral part of security and availability in cloud services, and it specifies how certain software components should interact with each other. A weak interface or weak APIs can be serious threats to the CIA (Confidentiality, Integrity and Availability) [15] of data stored in the cloud. In a desktop computer, data is usually stored /managed in the same system without any requirements for external interfaces.

E. *Denial-Of-Service:*

This has been a serious Internet threat for years [15], but is becoming more challenging when it comes to cloud computing. Many organizations shift to cloud computing mainly relying on 24/7/365 availability, which is possible because cloud services are offered through the Internet. Unfortunately, all Internet attacks are applicable to cloud computing environments as well.

F. *Malicious Insiders:*

We cannot categorize that a malicious insider attack is very specific to cloud computing environments, and it is also possible in other computing environments as well. When the authorization policies are weak in a system (either cloud-based or desktop-based), any attacker or a disgruntled employee can get access to a system. So, this is a universal problem that has to be addressed in a cloud computing environment as well.

G. *Abuse of Cloud Services:*

A hacker may use a cloud server to launch a Distributed DoS attack [15], propagate viruses, worms, or to share pirated software. It is the biggest challenge for cloud vendors to secure their servers, and a failure to do that may expose their clients to the attacks. When a cloud is abused, there is very little left for consumers to protect their data/system. Data stored in a desktop is often not relying on any external servers, and it is relatively free from the attacks to which clouds are more vulnerable.

H. *Shared Technology Issues:*

Cloud services are provided as infrastructure, platforms and applications as delivery services to the clients. CSA states that "*they were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployment platforms (PaaS) or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models*" [18]. Any shared platform would expose the entire environment to potential security issues. When a desktop environment stays as a stand-alone device, without any shared technology applications, it faces a minimal amount of potential shared technology threats.

V. Pattern-Based cloud security framework

Our literature review on cloud security issues in section IV provides a glimpse of various challenges to ensure cloud security. The origin of those challenges depends on various contexts, and not all security issues emerge from one vulnerability. Cloud security challenges have various sub-categories in them, but the only group who can fix those challenges could be CSP or software developers. In a cloud development environment, we cannot expect a system developer or a cloud service provider (CSP) as a security expert. We have to accept the fact that under certain circumstances, security engineering is done by non-security experts. In a cloud environment, service requirements and security expectations are decided by clients, and cloud developers work on satisfying those requirements. On the other hand, security experts may provide some solutions at a superficial level, which may not be applicable to the current environment. Therefore, we need a common domain where system developers and security experts can converge to share the requirements and find a solution to start thinking about security measures at an abstract level. Using security patterns [20] is one such domain to satisfy this requirement, because we can apply the abstraction through the use of patterns. In simple words, a software security pattern describes a particular recurring security problem that arises in specific contexts and presents a well-proven general scheme as a potential solution.

Based on our literature review [3, 4, 7, 8], we could identify that data breach and data loss are the top security concerns in the cloud computing environment. Any internet-based attacks are possible for cloud computing environment as well, since the Internet is the primary network medium between clients and cloud servers. Security patterns may not bring any impact on consumers' awareness on data location or abusive third party vendors, but it can strengthen the security measures from the authentication, encryption and input validation perspectives.

The concept of security pattern is capturing the already existing security solutions in a structured way and to enable the reuse of those solutions. A pressing need is to classify these security patterns to help system developers navigate through the library of patterns and select suitable patterns without ambiguity. However, there are some patterns that could be leveraged to strengthen the cloud security. To our best knowledge, there is no classification or organization of security patterns for cloud computing environments. An attempt of pattern classification for cloud computing may lead to the identification of further or related patterns, but organizing security patterns for cloud computing environments would be beyond the scope of this paper, hence, we decided to select a set of patterns from the pattern language [21] and designed a pattern-based security framework for cloud computing environment. We used the following security patterns in our model: Authenticator Enforcer, Account Lockout, Role-Based Access Control, Encrypted Storage Key Pattern, Protected

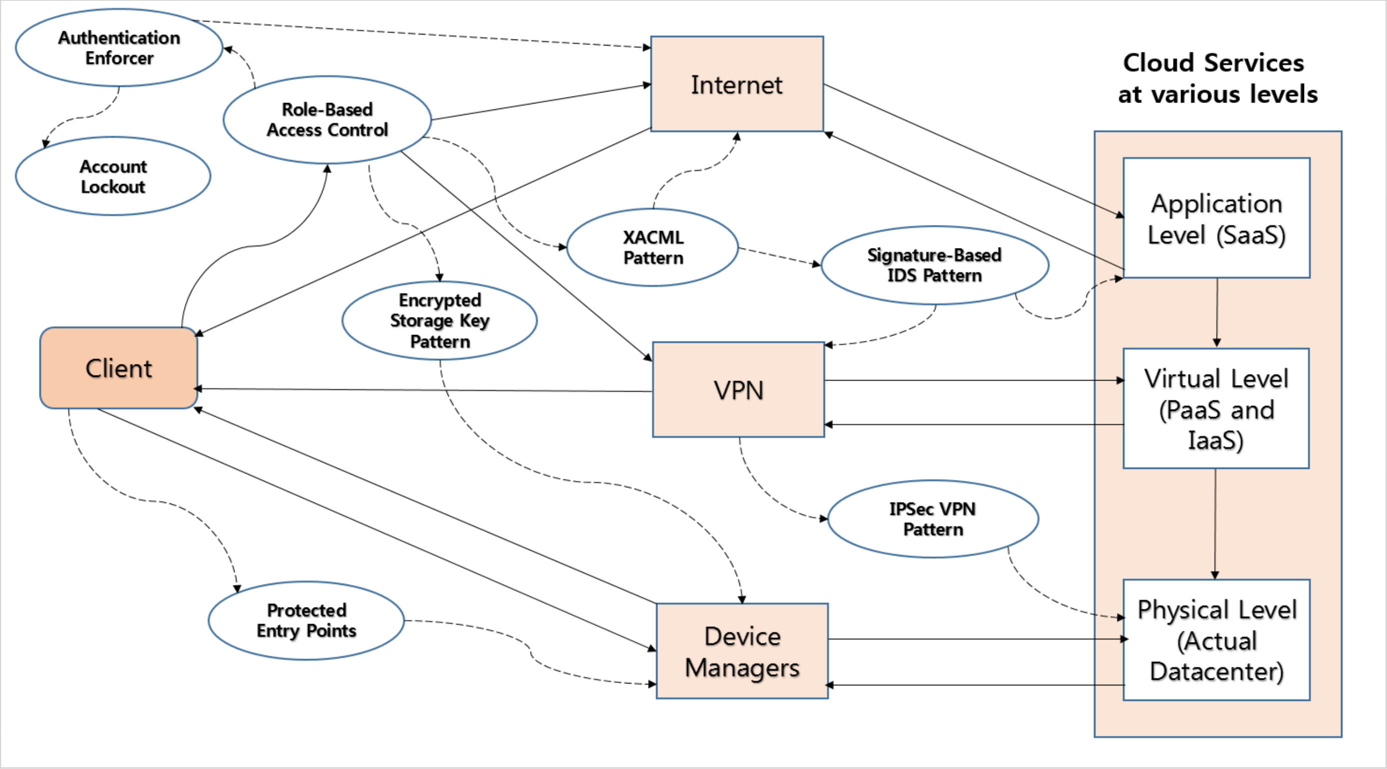

Authentication Enforcer
Account Lockout
Role-Based Access Control
Internet
Cloud Services at various levels
Application Level (SaaS)
XACML Pattern
Signature-Based IDS Pattern
Encrypted Storage Key Pattern
Client
VPN
Virtual Level (PaaS and IaaS)
IPSec VPN Pattern
Protected Entry Points
Device Managers
Physical Level (Actual Datacenter)

Fig.3: Pattern-based security framework for cloud computing. A secure communication channel is represented as straight arrow lines. Dashed lines represent alternate paths to access the application using security patterns. Oval-shaped structures represent security patterns. Rectangle shapes indicate various ways to access cloud resources, and a curved-rectangle depicts client organization or an end user.

Entry Points, XACML Pattern, Signature-Based IDS Pattern, IPSec VPN Pattern [23]. Our proposed model is depicted in Figure 3.

Generally, security patterns form a chain connection in which each pattern is derived from another pattern or creates a context for another, and no pattern acts as a mutually exclusive one [22]. One pattern may solve a low-level problem and a combination of patterns may be a solution to a high level or a more challenging security issue. To illustrate how a security pattern could be deployed in cloud computing environments, we selected seven patterns from the pattern language [21] and applied to our model. Patterns are shown as ovals and their relationships are represented in dashed lines. In our model, we mainly focused on cloud security challenges at network level.

Cloud computing is based on a model in which resources are shared with multiple users at the network level, application level and host level. Based on the level where users operate, which can be private, public or hybrid cloud resources, resource availability/access can be categorized as application level, virtual level and physical level . At the application level, end user is usually a person or organization who uses services offered by a cloud provider and pays as per used resources. Software-as-a-Service (SaaS) model comes under this category. At the virtual level, a developer or a moderator refers to a person or an organization that deploys software on a cloud infrastructure, and Platform-as-a-Service (PaaS) and Infrastructure-as-as-Service (IaaS) models are deployed at this level. Physical level generally refers to the actual datacenter or the organization that owns the infrastructure upon which clouds are deployed. Though, any service models are not provided at this level, from security point of view, it becomes important to consider the data storage, network attacks, hardware theft or even natural disasters that can happen at this level. In our proposed model, we considered various ways for a user to get connected to any level in a cloud computing environment. Though there can be more possible ways to access resources, due to space constraint, we limited to three different ways for a client to establish a communication channel with cloud resources. Client may get connected to the application level or virtual level through the Internet. Either the Internet or a secure VPN connection requires some authentication protocols to prevent unauthorized access to the client's data stored in a cloud service. On successful authorization, a secure communication channel is established between both ends, and it is represented as straight arrow lines in the model (see Fig.3). Datacenter owner or organization may employ their own device management systems as a way to access physical data storage. System developer would develop many secure possible ways to access, share or store data. In this scenario, we superimposed some security patterns to our model way. The act of excluding any or all patterns may still let the system perform its function, but patterns would help an ordinary engineer who has no experience in the field of IT security to get a good understanding of security requirements and ways to implement it. Similarly, security patterns may help a non-technical end user have an idea of what happens in a data breach or data loss without understanding much about the underlying security design. For example, the authenticator enforcer pattern, along with the encrypted storage key pattern, would save sensitive information like passwords, and token ID in an encrypted format, and combinations of more security patterns would make it a very secure transaction. A pattern-based cloud computing design would be very helpful to system designers while developing or maintaining the software. On the other hand, cloud users can avail this in-built strong security feature, which makes both parties benefitting from this design. We proposed a way to implement security patterns in our model. However, there is no specific process to support the evolution or classification of security patterns. This model provides an idea to connect security patterns in a cloud computing environment, but some more research has to be conducted in order to find out more possible patterns, and relationships between those patterns.

VI. Conclusion

Cloud computing provides enormous advantages in data storage and access, where the benefits outnumber the weaknesses. Maintaining security and privacy in clouds became a major challenge and is often viewed as weaknesses that hinder wider acceptance of cloud computing. Recently, security is turning out to be an expected mandatory feature of a cloud computing environment. Only if we could establish security and privacy in clouds, we could continue to benefit from cloud services. In this paper, we have provided an overview of cloud computing and discussed its security challenges. We have also suggested security patterns as a solution to tackle the challenges of cloud security. In our discussions, we have also elaborated on some important non-technical aspects that make the cloud security engineering process very difficult. Therefore, we have introduced a simple model for security patterns for cloud environments and defined the characteristics of the security pattern system.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. (1514568). This work was also supported in part by the National Research Foundation of Korea (No. 2014R1A1A1003707), the ITRC (IITP-2015-H8501-15-1008), and the NIPA (NIPA-2014-H0301-14-1010). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the aforementioned agencies.

References

[1] Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." Journal of Systems and Software 86.9 (2013): 2263-2268.

[2] Jensen, Meiko, et al. "On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.

[3] SO, Kuyoro. "Cloud computing security issues and challenges." International Journal of Computer Networks (2011).

[4] Popovic, Kresimir, and Zeljko Hocenski. "Cloud computing security issues and challenges." MIPRO, 2010 proceedings of the 33rd international convention. IEEE, 2010.

[5] Ramgovind, S., Mariki M. Eloff, and E. Smith. "The management of security in cloud computing." Information Security for South Africa (ISSA), 2010. IEEE, 2010.

[6] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." Services Computing, 2009. SCC'09. IEEE International Conference on. IEEE, 2009.

[7] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems 28.3 (2012): 583-592.

[8] Subashini, S, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications 34.1 (2011): 1-11.

[9] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov. 2010.

[10] Arapinis, Myrto, Sergiu Bursuc, and Mark Ryan. "Privacy supporting cloud computing: Confichair, a case study." Principles of Security and Trust. Springer Berlin Heidelberg, 2012. 89-108.

[11] Nurmi, Daniel, et al. "Eucalyptus: A technical report on an elastic utility computing architecture linking your programs to useful systems." UCSB TECHNICAL REPORT. 2008.

[12] Popa, Raluca Ada, et al. "Cryptdb: protecting confidentiality with encrypted query processing." Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. ACM, 2011.

[13] McIntosh, Michael, and Paula Austel. "XML signature element wrapping attacks and countermeasures." Proceedings of the 2005 workshop on Secure web services. ACM, 2005.

[14] Brodkin, Jon. "Gartner: Seven cloud-computing security risks." (2008).

[15] Whitman, Michael, and Herbert Mattord. Principles of information security. Cengage Learning, 2011.

[16] Mont, Marco Casassa, Siani Pearson, and Pete Bramhall. "Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services." Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on. IEEE, 2003.

[17] https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[18] http://edas.info/doc/

[19] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." National Institute of Standards and Technology 53.6 (2009): 50.

[20] Yoshioka, Nobukazu, Hironori Washizaki, and Katsuhisa Maruyama. "A survey on security patterns." Progress in Informatics 5.5 (2008): 35-47.

[21] Hafiz, Munawar, Paul Adamczyk, and Ralph E. Johnson. "Growing a pattern language (for security)." Proceedings of the ACM international symposium on New ideas, new paradigms, and reflections on programming and software. ACM, 2012.

[22] Heyman, Thomas, et al. "Using security patterns to combine security metrics." Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, 2008.

[23] Fernandez-Buglioni, Eduardo. Security patterns in practice: designing secure architectures using software patterns. John Wiley & Sons, 2013.

.