Cloud Security - A Semantic Approach in End to End Security Compliance

Venkata Naga Satya Surendra Chimakurthi

Sr. Technical Lead, EBA-Ventures-Digital Asset Management (DAM) Solutions, Cognizant Technology Solutions, Dallas, **USA**

Corresponding Contact:
Email: chvnssurendra@gmail.com

ABSTRACT

Many firms are seeing the benefits of moving to the cloud. For the sake of their customers' data, cloud service providers are required by law to maintain the highest levels of data security and privacy. Most cloud service providers employ a patchwork of security and privacy safeguards while industry standards are being created. The upshot is that customers of cloud services are unsure whether or not the security protections supplied by these services are enough to meet their specific security and compliance requirements. In this article, we have discussed the many threats cloud users face and emphasized the compliance frameworks and security processes that should be in place to minimize the risk. To categorize cloud security measures, risks, and compliance requirements, we developed an ontology. We needed to design software to identify the high-level policy rules that must be applied in response to each danger as part of this initiative. Additionally, the program provides a list of cloud service providers that now satisfy specific security requirements. Even if they aren't familiar with the underlying technology, cloud users may utilize our system to build up their security policy and identify compatible providers.

Key words
Cloud computing, cloud security, Security compliance, SaaS

12/31/2017 **Source of Support:** None, **No Conflict of Interest:** Declared

INTRODUCTION

Individual applications, devices, and documents can be used to connect to the cloud by users. However, nothing observable exists within the cloud system, including its internal components, such as its hardware and the operating system that controls the hardware connections. The cloud computing process begins with the user interface shown to each user. This is how users submit their requests, which are subsequently forwarded to the system administration, which locates the required resources and then invokes the proper provisioning services for the system under consideration.

Cloud computing is responsible for the majority of data storage. Data is kept on several servers that a third-party service provider maintains. When a user discovers a virtual server, it looks as though the data is saved in a specific location with a particular name of one specific server, but this is not the case in reality. Its sole purpose is to refer to the virtual space provided by the cloud. It is possible that the user's data will be saved on any one or more of the machines used to form the cloud in reality.

However, while cloud-based solutions are enticing because of the cost savings and ease of provisioning and scalability, most users (Mather et al., 2009) are concerned about the privacy and security of cloud data, which is a significant barrier to cloud adoption. For example, the Cloud Security Alliance (CSA, 2014), the International Organization for Standards (ISO), the National Institute of Standards and Technology (NIST) (Mell & Grance, 2011), and other standards groups have suggested or are developing cloud security standards in recent years. Most cloud computing organizations employ a disorganized collection of security and privacy safeguards. Clients are confused and concerned about what security measures to expect from cloud services and what compliance standards to apply for their firm data stored on the cloud due to this confusion and anxiety. This study makes three substantial contributions.

First and foremost, we conducted a thorough analysis of the potential vulnerabilities that cloud users may be exposed to and the compliance frameworks and security measures that must be in place to limit risk. We looked at security requirements in cloud computing and information technology administration. In addition, we examined the security-related whitepapers available on more than 100 cloud service providers' websites to determine the security protocols they implemented. We then utilized this study to develop an ontology representing cloud security controls, risks, and compliance. This ontology can then be used to extract and store information from standards and cloud providers in W3C-standard semantic web languages, becoming increasingly popular. It allows us to think about it and reason about it while working on the project. Finally, we developed a web-based application that consumer advocacy organizations may use. Given the risks that an organization is exposed to, it advises appropriate cloud security policies and cloud service providers that can support them. This application categorizes the risks that cloud users face and determines which security and compliance policies must be activated in response to each threat, based on the classification. The program also displays a list of existing cloud service providers capable of meeting the security standards.

LITERATURE REVIEW

The cloud security vulnerabilities have been investigated in previous research (Ramgovind et al., 2010; Subashini & Kavitha, 2011; Mather et al., 2009) to understand what they are. The research conducted by Manavalan (2016) on cloud security controls and standards have been primarily focused on the provider end, with a particular emphasis on cloud engineering. Subashini and Kavitha (Subashini & Kavitha, 2011) give a study of the many security threats associated with the cloud computing environment. This research focuses on the security challenges that have arisen due to cloud service delivery paradigms. A risk model for the cloud has also been established by Manavalan & Bynagari (2015); however, it has not been linked to any existing compliance requirements as of yet. . How many cloud providers are applying the cloud security standards in (NIST, 2011) and (Cloud Security Alliance, 2013). They are capable of dealing with possible attacks is an unresolved topic. One that may cause consumers who must choose between different providers to be concerned about the security of their data (Manavalan, 2016). The National Institute of Standards and Technology's cloud computing reference architecture (NIST, 2011; Mell & Grance, 2011) categorizes security and privacy regulations as being under the control of the cloud provider. However, as opposed to this paradigm, the security compliance model is applicable across all roles in the reference design. The security rules employed to secure a cloud environment are the same for all cloud delivery models, regardless of the cloud delivery model. Compliance criteria are applied to these security controls to ensure they are effective. The IT compliance model involves electronic data processing, networks, and information technology infrastructure (Subashini & Kavitha, 2011). In addition, compliance models provide rules and regulations to diverse information technology components to function together smoothly. Organizations frequently use a security control strategy based on these compliance models. Customers and end-users will benefit from transparency in the cloud service model, security controls, and compliance model, which will allow them to achieve reliable cloud data protection (Aslam et al., 2015).

THREATS TO CLOUD SECURITY AND CONTROL MODELS

In order to identify the dangers that cloud users face, we studied the security concerns detailed in publications such as (Cloud Security Alliance, 2013; Subashini & Kavitha, 2011), and others produced by international standards organizations. Cloud security is threatened by -

- Security lapses compromise the privacy and business operations by exposing sensitive data to unauthorized access. Data that cannot be decrypted by an adversary, even if it is taken.
- In the event of a hardware failure or an assault on the system, data loss is possible. This sort of danger may be countered by using data backup procedures.
- Account or service traffic hijacking: harms the user's privacy and security. Personal information, such as bank account numbers, can be stolen by hackers. In order to combat this, anti-phishing and anti-fraud rules should be developed.
- Interaction between users and providers is facilitated via interfaces and APIs that aren't secure. Using APIs, the data should be encrypted before being sent over the network.
- As a result of a "denial of service" attack, legitimate users are unable to access their data. It's possible for an attacker to disable service by changing the encryption key or by slowing it down. Users and cloud providers should work together to devise a system that makes it impossible for attackers to discern trends in communications.
- Data tainted by the actions of "malicious insiders" who have gained access to and control of the company's systems. Legal action should be taken in this case.

- The multi-tenancy feature of cloud services can be misused by attackers to break into other organizations' data. Cloud service providers should take precautions to prevent their customers from gaining access to the data of other users.

- Using the cloud without doing adequate due diligence is a common occurrence among enterprises looking to cut costs. Cloud customers should be educated about cloud technology through awareness activities.

- Vulnerabilities in shared technology: Cloud providers scale their service by sharing the resources. In cloud computing, this sharing technique should be used in all domains and also for monitoring the system.

SECURITY RISKS INVOLVED IN CLOUD COMPUTING

Using cloud computing, we rely on cloud providers to make judgments about our data and platforms in ways that have never been seen before in the history of computing (Subashini & Kavitha, 2011). Furthermore, the apps are executed on the computers of the service provider, and the customers have little to no understanding of the environment in which they operate. As a result, the information is subject to eavesdropping and alteration.

The data stored in the cloud is vulnerable to the following risks:

- Spoofing is a method of gaining access to information by impersonating someone else's identity.
- User data tampering occurs when data entered by a user is modified without the user's permission. Denying the transaction's origin is referred to as "repudiation" (request or response).
- A breach of information security occurs when data is released to unauthorized users without the user's knowledge or consent.
- An attacker attempts to prevent legitimate users from obtaining information or services by launching a denial-of-service (DoS) attack on them.
- Privilege elevation occurs when an attacker is granted authorized permissions that are in addition to those that were first granted. For example, an attacker with a privilege set that has just "read only" rights may be able to raise the set to include both "read" and "write" capabilities.

It is necessary to secure data both while it is in storage and while it is in transit. It is necessary to implement appropriate procedures in order to restrict access to application execution and stored data to just those who are authorized to do so. The amount of security necessary is determined by the deployment methodology, the type of application, the business aim, and the amount of available money (Manavalan & Ganapathy, 2014). Although cloud security must be defined from an operational and governance perspective, it is necessary to handle it from both perspectives. While it is critical to concentrate efforts on traditional security measures such as disaster recovery, data center operations, incident response, application security (including application security, encryption and key management), identity and access management, and virtualization, it is equally important to focus efforts on cloud computing architectural frameworks, risk management, and legal discovery.

INFORMATION SECURITY STANDARDS

Many security standards have emerged in recent years to safeguard the confidentiality, integrity, and availability of data stored in the cloud. The following are some of the most important. To effectively apply security rules in a Cloud environment that will serve as the foundation for your security framework, it is critical that you properly grasp your organization's security policies. In addition, it is critical to select a CSP that provides standards that are relevant to your requirements. Security, system development, financial reporting, IT service delivery, and control environment are all areas where standards may be established.

ISO/IEC 27001 is an audit standard for Information Security Management Systems. Those who claim to have embraced ISO/IEC 27001 can be audited and certified compliant. In total, there are 11 domains and about 130 controls. In addition to security policy, physical and environmental security are included. Regulations for baseline information security and standards for classifying information and information systems were created in 2002 by the Federal Information Security Management Act (FISMA). The European Union's Network and Information Security Agency (ENISA) ENISA's mission is to promote European network and information security. The Institute of Electronics and Electrical Engineers, American National Standards Institute, and National Security Agency also establish standards (NSA).

There are several information security standards and recommendations. Customers might get confused when various CSA have different criteria. The Cloud Security Alliance has established a Cloud Controls Matrix to help users choose the right standard (CCM). The CCM is meant to help cloud clients analyze a cloud provider's overall security risk. It has 13 ISO 270001 and NIST domains. Regardless of the standard the CSA follows, certification assures consumers that data confidentiality, integrity, and availability are protected.

CLOUD COMPUTING SECURITY ISSUE

Cloud Security Framework Layers

It has four layers: virtual machine, cloud storage, cloud data, and virtual network monitor. For the Cloud Storage Layer, a massive virtual storage system is built by combining resources from several cloud service providers. For difficulties, the Virtual Network Monitor Layer integrates hardware and software in virtual machines. However, several parties are interested in creating cloud security standards. On the Cloud Standards web sites, various organizations are developing cloud–related standards. One is the Cloud Security Alliance (CSA). The CSA brings together solution providers, non-profits, and people to debate existing and future best practices for cloud information security. Open Web Application Security Project (OWASP). OWASP keeps a list of cloud-based or software-as-a-service vulnerabilities updated as the threat landscape changes. The Open Grid Forum produces security and infrastructure materials for grid developers and academics.

Cloud Security Components

Transaction management, resource allotment (including operating systems, virtualization), cloud networks, load balancing (which includes databases), memory management (and concurrency control) are only some of the security concerns associated with cloud computing (Manavalan & Bynagari, 2015). Security in a cloud network, for example, should be secure, as it links all of the cloud's services. Load balancing must be done in a secure manner. Cloud computing virtualization raises additional security issues. The mapping of virtual computers to real machines, for example, must be done securely to avoid security breaches. Algorithms for allocating resources and managing memory must be safe (Amin & Manavalan, 2017). Encryption and proper enforcement of data sharing protocols are also part of concurrency control. Data mining techniques may be useful in cloud malware detection.

Cloud Computing Security Issues

Cloud security has several difficulties. The cloud service provider ensures that the consumer does not experience data theft or loss. Because the cloud computing infrastructure is new, its security has not been adequately examined. Thus, a user can infect the cloud by impersonating a genuine user. Thus, all cloud users are affected. Cloud computing security challenges are described below:

- **Data Integrity:** Occasionally, data may contain errors due to human mistake when it is entered into the system. Even during the transmission of the data, errors may occur. Even system failures, such as a disk crash, might result in errors. Viruses in the cloud might potentially cause problems. Thus, a Data Integrity technique is necessary in cloud computing to ensure the integrity of data.
- **Data Loss:** Data loss is a major issue in cloud computing. Sometimes research and development teams communicate sensitive material online, making it exposed to unauthorized access. If a server fails, crashes, or is infected by a virus, the whole system fails, and data loss occurs. Consumers will lose data if the provider shuts due to legal or financial issues. Consumers won't be able to access data since the vendor has stopped down.
- **Data Location:** The location of data saved in the cloud is not always clear to consumers. It's unclear where the data is stored by the vendor. In cloud computing, there is a high degree of data mobility. The data is spread out over the globe. The user can request that the cloud service provider store their data in a certain location, but it needs a contract between the two parties.
- **Data Access Control:** A lack of a secure data access control system might lead to the unauthorized access of sensitive or secret information on occasion. The protection of sensitive data in a cloud environment has emerged as a fundamental concern in a cloud-based infrastructure. The longer data is stored on the cloud, the higher the danger associated with it.
- **Data Theft:** The storage of data in cloud computing is accomplished through the usage of external servers. A vulnerability exists in the data kept on these servers and there is a possibility that it will be stolen.
- **Security issues in provider level:** A cloud is only safe if the vendor provides good security for the customers, which makes it safe for them. The provider should make sure that the customer and the user are safe. Keep the server safe from any outside threats it might come across, too.
- **User level Issues:** When inputting data into the system, the user should take precautions to ensure that the data is not lost or tampered with.
- **Privacy Issues:** In the context of cloud computing, the security of the customer's personal information is extremely crucial. Due to the fact that the majority of the servers are external, the vendor should ensure that they are adequately protected from the operators.

- **Infected Application:** The service provider should have complete access to the server, including all necessary permissions, for the purpose of doing server maintenance and monitoring. The cloud computing services and customers would benefit as a result of this because malevolent users will be prevented from uploading contaminated applications to the cloud.

CLOUD SECURITY AND COMPLIANCE ONTOLOGY

The ideas of cloud security, risks, and compliance controls have been captured in an OWL ontology (Taniya, 2013), which we have built. This ontology is briefly described in this section; however, it is outside the scope of this work and will not be discussed further. The two main classes in the ontology are cloud computing security (which is further subdivided into cloud computing compliance models, cloud computing controls, and threats to cloud security) and cloud computing providers. Cloud computing security is further subdivided into cloud computing compliance models, cloud security controls, and threats to cloud security.

Figure 1 depicts the relationship between the class cloud security compliances and the class security control compliances. We have represented in our ontology the several forms of cloud security compliances that were discussed in Section III. The control elements specified in section III A are subclasses of the Cloud security control class, which includes the control elements stated in section III A. Each cloud security standard has a compliance type that may be implemented. The dangers and their kinds, which are described in depth in Section III, are represented in our ontology. Our recommendation tool's database architecture was influenced by the ontology we used to create it. In Figure 1, you can see the link between Security Controls and Security Compliance classes described by an ontology.

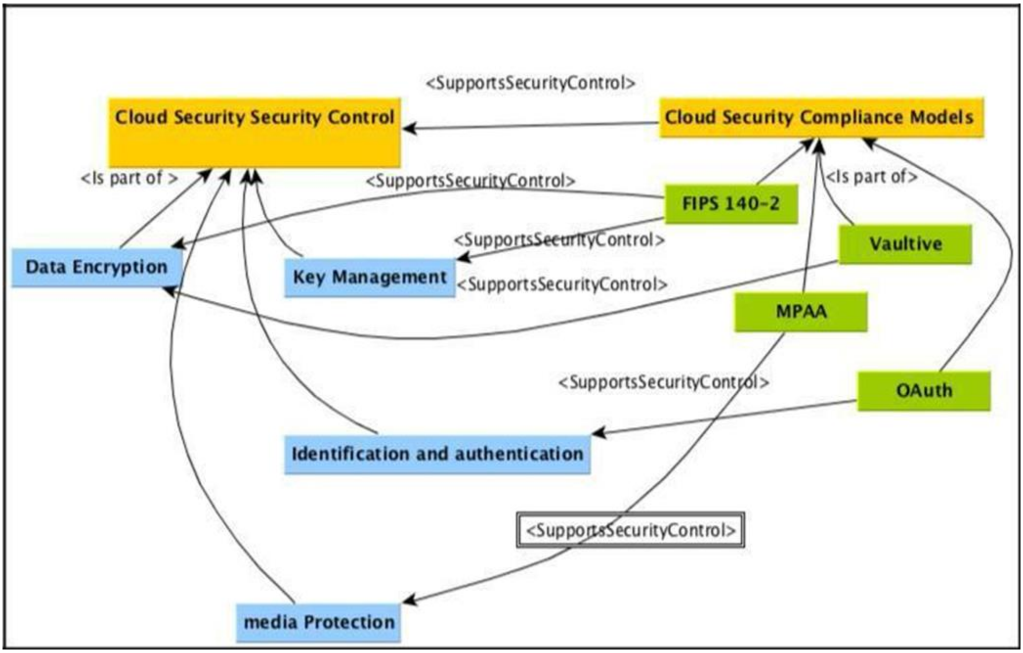
<SupportsSecurityControl>
Cloud Security Security Control
Cloud Security Compliance Models
<Is part of >
<SupportsSecurityControl>
FIPS 140-2
<Is part of>
<SupportsSecurityControl>
Vaultive
Data Encryption
Key Management
<SupportsSecurityControl>
MPAA
<SupportsSecurityControl>
OAuth
Identification and authentication
<SupportsSecurityControl>
media Protection

Figure 1: The ontology: Security Controls and Security Compliance classes are linked

System for Recommendation of Cloud Security Policies

We have created an application that cloud users may use to choose the cloud security and compliance standards that they want to implement within their business. This application is available for download here. This system assists users in identifying cloud-based dangers, as well as the security and compliance approaches that may be used to fight against them. A list of existing cloud service providers who have adopted the standards in their services is also provided by the application.

For this application, we investigated a variety of security compliances, security policies/standards, and risks that might compromise cloud-based security. Following that, we connected these controls, standards, and threats based on characteristics such as a description of security standards, the requirements for standard fulfillment, a description of compliance, and an analysis of risks that influence cloud security. This web-based application was developed with the help of PHP, HTML, and AJAX web technologies, as well as a MySQL database. The database architecture for the application is depicted in Figure 2.

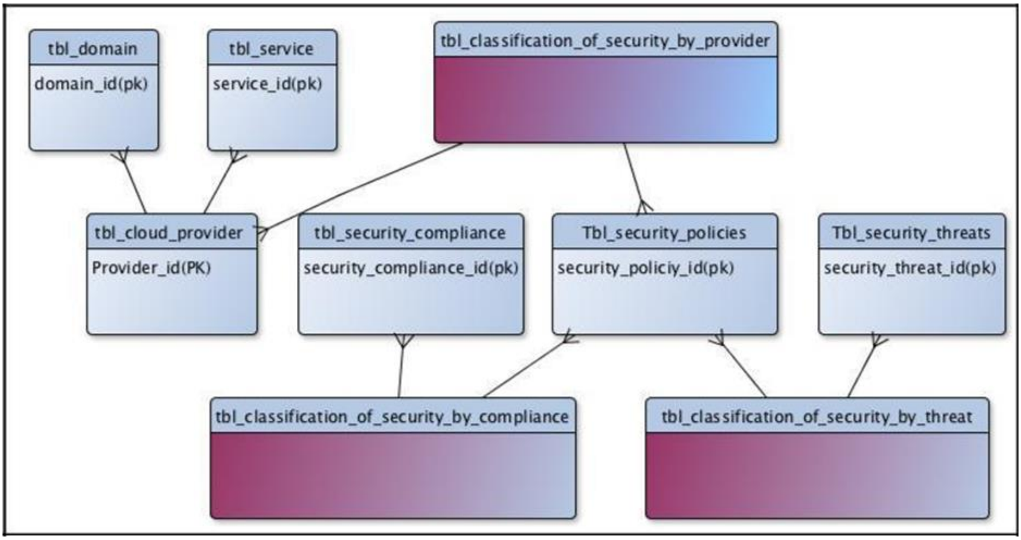

Figure 2: Database architecture for the application

Cloud users may obtain a list of all cloud service providers who satisfy a specific compliance standard by utilizing our application. If customers are unsure about which compliance standard to comply with, they may search for several security controls to find out more information.

Conclusion

People are increasingly turning to cloud computing for their computer needs. In today's cloud-based world, data privacy has become increasingly vital. Scheduled concealment of the data system is a novel strategy for preserving data privacy against attackers who retrospectively access, through legal or other means, a user’s stored data and private decryption keys. In this system, access to the file is granted to the corresponding users of the file only for the period specified, after which the user is no longer able to access the file again. Furthermore, even if a user wants to access a file after the expiry time has passed, he must first get permission from the administrator. The user can only access the file after receiving permission from the administrator. To increase the overall system security, we use the Shamir secret sharing scheme to store private keys for each file. This method is used to store the private keys for each file. As opposed to keeping the keys themselves, the shares generated from the keys are kept. As a result, the planned concealing of data systems aids in the resolution of the data privacy problem.

We have undertaken detailed research to assess the various hazards faced by cloud users and established the compliance models and security measures that need to be in place to mitigate the risk. In this work, we developed an ontology that is semantically rich and can be used to model security risks, cloud security rules, and controls, and describe the provider data in a consistent manner. Customers that are considering moving their data to the cloud but are afraid to do so owing to security concerns, or who are unaware of the security measures, can benefit from an easy-to-use cloud security policy suggestion tool that we have built. Other IT compliance approaches that may be relevant in the cloud paradigm are being investigated further as part of our ongoing work, to determine whether or not they should be included in our cloud security application. We are also building methods to reason over the ontology to better match compliant suppliers.

REFERENCES

Amin, R., & Manavalan, M. (2017). Modeling Long Short-Term Memory in Quantum Optical Experiments. *International Journal of Reciprocal Symmetry and Physical Sciences*, *4*, 6–13. https://doi.org/10.5281/zenodo.5633992

Aslam, B. N., Mishra, R., and Thombare, S. (2015). Enhancement of Cloud Security through Scheduled Hiding of Data. *International Journal of Computer Engineering and Technology (IJCET)*, *6*(3), 24-32

Cloud Security Alliance. (2013). The Notorious Nine: Cloud Computing Top Threats in 2013, p8-p21.

CSA (2014). CSA security Guidance, v3.

Manavalan, M. (2016). Biclustering of Omics Data using Rectified Factor Networks. *International Journal of Reciprocal Symmetry and Physical Sciences*, *3*, 1–10. https://doi.org/10.5281/zenodo.5633990

Manavalan, M., & Bynagari, N. B. (2015). A Single Long Short-Term Memory Network can Predict Rainfall-Runoff at Multiple Timescales. *International Journal of Reciprocal Symmetry and Physical Sciences*, *2*, 1–7. https://doi.org/10.5281/zenodo.5622588

Manavalan, M., & Ganapathy, A. (2014). Reinforcement Learning in Robotics. *Engineering International*, *2*(2), 113-124. https://doi.org/10.18034/ei.v2i2.572

Mather, T., Kumarswamy, S., & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media.

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing*, (Special Publication 800-145).

NIST. (2011). NIST Cloud Computing Reference Architecture.

Ramgovind, S.; Eloff, M.M.; Smith, E., (2010). The management of security in Cloud computing. Information Security for South Africa (ISSA), pp.1,7, 2-4.

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11

Taniya. (2013). Introduction to Cloud Security, *International Journal of Electronics and Communication Engineering & Technology (IJECET)*, *4*(7), 252-260.

--0--