Mugla Journal of Science and Technology

AN ASSESSMENT OF RECENT CLOUD SECURITY MEASURE PROPOSALS IN COMPARISON TO THEIR SUPPORT BY WIDELY USED CLOUD SERVICE PROVIDERS

Mohamad SOUBRA[1*], *Ömer Özgür TANRIÖVER*[2*]

[1]Department of Computer Engineering, Ankara University, 06830, Ankara, Turkey
mhd.m.soubra@gmail.com
[2]Department of Computer Engineering, Ankara University, 06830, Ankara, Turkey
ozgurtanriover@yahoo.com

Received: 30.10.2017, Accepted: 24.11.2017
*Corresponding author
doi: 10.22531/muglajsci.355273

Abstract

In this paper, we aim to present the recent security approaches and solutions proposed for cloud service providers and those provided by widely used cloud service providers. Through a review, recent cloud security mechanisms are discussed with respect to their mode of operation, their structure and the techniques to offer security services. Then five widely used cloud service providers namely Microsoft 365, Cisco WebEx messenger, Force.com, Yammer, Service now are assessed in terms of their security services. The provided information by the assessment may be potentially used by organizations in order to align their security policies with those of cloud service providers.

Keywords: Cloud services, security measures, organizational security policies.

YAYGIN OLARAK KULLANILAN BULUT SERVİS SAĞLAYICILARININ YENİ BULUT GÜVENLİK ÖNLEMİ ÖNERİLERİ AÇISINDAN DEĞERLENDİRİLMESİ

Öz

Bu yazıda, bulut servis sağlayıcıları için önerilen ve yaygın olarak kullanılan bulut servis sağlayıcıları tarafından sağlanan son güvenlik yaklaşımlarını ve çözümlerini sunmayı amaçlıyoruz. Önce, yeni bulut güvenlik mekanizmaları, çalışma tarzları, yapıları ve güvenlik hizmetleri sunma teknikleri özetlenmiştir. Sonra beş yaygın olarak kullanılan bulut servis sağlayıcısı yani Microsoft 365, Cisco WebEx messenger, Force.com, Yammer, Servicenow güvenlik hizmetleri açısından ve yeni güvenlik mekanizmaları desteği açısından değerlendirilmiştir. Sağlanan bilgiler, kuruluşlar tarafından, güvenlik politikalarını bulut servis sağlayıcılarınkilerle uyumlu hale getirmek için kullanılabilir.

Anahtar Kelimeler: Bulut hizmetleri, güvenlik önlemleri, örgütsel güvenlik politikaları.

1. Introduction

The E-Business or Virtual Business services may lead to the creation of "Virtual Enterprises". Internet services are services that are accessed by using the internet and cover a huge spectrum of assets and resources needed by any organization. By utilizing these services, enterprises are described as to have "Service Oriented Architectures" (SOA). Cloud Computing or "On Demand Computing" is an internet based service architecture in which resources and processes are said to be shared with different internet nodes. Through sharing, cloud computing is considered to be the "Green" networking option by which it facilitated the leap towards a multi-platform approach and enterprises have taken the initiative to adopt this new trend. Cloud Computing is tangible through many characteristics like agility, reduction of costs of hardware and software, maintenance aspects, multitenancy, performance, productivity, reliability, scalability, elasticity, and of course security. Some engineers echo that Cloud computing led to under-utilization, waste of IT resources due to resource fragmentation and unequal distribution of workload, others would echo that cloud computing is the solution to mundane security problems [29] [30].

On the other hand, cloud outsourcing services of the investigated providers may cover:

- **Infrastructure as a service (IaaS):** This includes hardware resources like storage, computing power (i.e. CPU and memory) offered as a service to the customers which is based on the load to be distributed upon several machines. This will allow applications to be horizontally scaled. Companies like Amazon [1] for example provides "Simple Storage Service" (S3) for storage, "Elastic Compute Cloud" (EC2) service for computing power, and "Simple Queue Service" (SQS) for network communication for small businesses and individual consumers. HP [2] in another example provides "Flexible Computing Services" (FCS) which is a service that provides computing and storage infrastructure as services for businesses.
- **Software as a service (SaaS):** The service provider provides the customer with application of the product online. As example, this includes Google web-based office applications (word processors, spreadsheets, etc.), Microsoft through online "Customer Relation

Management" (CRM) and "SharePoint", and Adobe through "Adobe Photoshop" and "Adobe Premiere" services on the Web.

- **Platform as a service (PaaS):** This is done through providing facilities to support the entire application development lifecycle, done often through the utilization of web browsers that includes application design, implementation, debugging, testing, deployment, operation and support of rich web applications and services on the Internet. Examples of platforms are Microsoft [6] through "Azure" Services platform and Google [7] through its "App Engine".

Although there exist many service providers with variety of services, one of the biggest challenges for the organizations is to understand and integrate security measures/practices provided by cloud infrastructure/service providers. There seems to be a lack of approach of cloud providers towards standards/practices aspects used to overcome common security problems. These interleaved security aspects are multi-tenancy, information integrity and privacy, vendor lock-on, secure software development, and provider's logs**.** Therefore, we decided to conduct a comparison study with respect to recent security policies/measures proposed in the literature to those provided by the five most widely used cloud service providers. We think that this information can be helpful for both for organizations and service providers in order to be able to benchmark themselves to the respective security measures.

In the rest of the paper we present the recent related work on security approaches in the cloud computing domain. The approaches are discussed with respect to their mode of operation, their structure and the way they offer security services. Four widely used cloud service providers are assessed in terms of their security services. The last part presents the different approaches their implications are further discussed.

2. Literature Review

Our literature research on recent cloud service security measures includes the period 2010 to 2016 that is carried out from a wide range of conference papers and journals included in *IEEE – Xplore, Springer Link* and *Science – Direct.*
A framework for communication of organizational data relying on a two-phase approach is proposed by K Suud. [14]. First phase deals with process of transmitting and storing data securely into the cloud utilizing a MAC (Message Authentication Code) derived from the checksum of any secret key and a128 bit SSL (Secure Socket Layer) encryption scheme. Second phase deals with the retrieval of data from cloud, generation of requests for data access, double authentication using username / password, secret questions, and Service Providers' digital signature verification. The proposed framework hierarchy aims to increase security firmness although it requires many steps to go-through and extra information given by the user.

Jorge Bernal Bernabe et. al [3] proposed a three-modeled semantic-aware access control system to solve multitenancy problems. The first model is the information model that is based on OWL 2 (Ontology Web Language 2) and SWRL (Semantic Web Rule Language) with respect to the CIM (Common Information Model). This framework cope with an access control system. The authorization model based on the definition of authorization statements executed by Role-based access control (RBAC) or Generalized RBAC. The Trust management model which provides a fine grain of trust between tenants. OWL 2 has a lot of advantages by itself, it can be mapped to derive metadata models through RDF (Resource Description Framework) [31]. With the help of RDF, the RBAC framework could be more securely enhanced.

X. Z. X. Zhang et. al [40] proposed a framework that is made up of 7 processes which depends on ISO/IEC 27001, NIST (National Institute of Standards and Technology) risk management guide for information technology systems, and Booz Allen Hamilton information security governance government considerations for the cloud computing environment. The 7 processes are the selection of relevant critical areas, strategy and planning, risk analysis through OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation), risk assessment through COBRA (Console Operator Basic Requirements Assessment), risk mitigation through RTP (Risk Treatment Plans), assessing and monitoring program and risk management review. The system was shown to be durable through its implementation at Yunan University, China. Backing-up ISO/IEC 27001 with COBRA and OCTAVE, the risk management system had also the ability to detect security threats and evaluate them and provide necessary treatment thus, demonstrating the efficiency of such combination.

K. S. Gill et. al [8] proposed a hypervisor managed multi stepped IDPS (Intrusion Detection and prevention System) through utilizing VNI-p (Virtual Network Interface) and a Tracking module. The steps are Virtualization while running two or more operating systems on a single hardware, nesting of Virtual Machines (VMS) in addition to detection and prevention of the attack. The IDPS coped with sudden increase and decrease of traffic which ensured the project efficiency. The utilization of VNI-p as an add-on improved the IDPS's security and this was realized in the tests done.

A. Ahmed et. al [2] proposed the utilization of COBIT (Control Objectives for Information Related Technology). COBIT had the ability to provide customer compliance through 4-eyes authorization, selected authentication methods through passwords, certificates, forensics and contracts through tamper-proof evidence for SLA (service level agreement) contracts, and customizable access control real-time monitoring and auditing capabilities. COBIT easily integrates with and builds on other business and IT frameworks while improving their impact. COBIT is a well-known standard and is quite popular, utilizing COBIT as a standard insures that risk management of security issues is always backed-up by standardizing bodies.

V. Chang et. al [38] proposed a XACML (Extensible Access Control Markup Language) of type "Rescue" triple defense layered CCAF (Cloud Computing Adoption) framework which will ensure to block viruses, Trojans, denial of services attacks and unauthorized access. In addition, through the utilization of OVF (Open Virtual Machine) data will be backed up and retrieved from secure ports. The defense layers are as follows: The 1st layer holds the Access Control and firewall, 2nd layer holds the IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) and the 3rd layer holds the encryption scheme. The system supported high performance and proved to ensure high protection through its implementation at the University of London Computing Center (ULCC). Layering in this schema is thought to be beneficent. Adapting the layer schema helped in modulating the system in which every single layer was responsible of a certain task.

Akbar Khrisna et. al [20] proposed a TOGAF (The Open Group Architecture Framework), PMBOK (Project Management Body Of Knowledge), COSO (Committee Of Sponsoring Organizations of the Treadway Commission) and ITIL (Information Technology Infrastructure Library) COBIT5 framework to solve multitenancy problems through data collection management, risk analysis management, articulating risk management and continuous monitoring. As a result, COBIT5 proved to be reliable when considering risk governance. As mentioned before regarding the utilization of COBIT, COBIT5 is also a popular version of the same standard.

H.-Y. Lee et. al [10] proposed a multi-pronged holistic triple tired Self-Disclosure (self-revealing) framework based on MTCS and ISO27001:2005 standards. The 1st tier host nonbusiness critical applications. The 2nd tier is assigned to data protection and the 3rd tier regulates organizations with specific requirements. As a result, the frameworks showed guidelines to validate controls and protect data which made it build more trust between the users and the service provider thorough the ability establish this trust and build on it. The tier model of the system and the trust build ensures that the systems that can't be trusted are not considered to be secure and vice versa.

Oscar Rebollo et. al [23] proposed a confidential and access controlled ISGCloud which keeps records/logs that enables remote management and allows security monitoring of cloud provider personnel's compliance with security controls. As a result, with respect to the proposed governance criteria, the ISGCloud framework made improvement of nearly 60% after its implementation. Implementing a firm logging system is crucial since attacks could be either direct or indirect thus, logs are very important to identify on-going or up-coming security issues.

M. Almorsy et. al [55] proposed the utilization of the NIST-FISMA (National Institute of Standards and Technology-Federal Information Security Management Act of 2002) tailorable standard covers the management layer, enforcement layer and feedback layer through CPE (Common Platform Enumeration), CWE (Common Weakness Enumeration) and CAPEC (Common Attack Pattern Enumeration and Classification), CVE (Common Vulnerability and Exposure) and CCE (Common Configuration Enumeration). As a result, the standard showed reliability through displaying a catalogue of security control templates when implemented at Swinburne University. Multilayering is very important when building up a solid security system, layers help in organizing data flow and controlling them. This creates more edge when it comes to resolving security issues.

J. P. Veigas et. al [21] proposed a signature and subscription service based Global Mastered IDS (Intrusion Detection Service) framework which compromises signature, subscription and alert modules. The author also proposes an Intrusion Detection Engine (IDE) based local repository responsible for monitoring hosts (nodes) through utilizing cluster controllers and web interfaces. Because rules are stored locally the global subscription rule base, and through the implementation of the framework on an Eucalyptus Cloud, new rules were introduced without modifying existing ones which made it efficient. With the aid of new updated rules, the IDE showed more power in detecting security anomalies. This specifies that importance of rules in IDEs.

Flood, J. et. al [7] proposed a real-time observation and mining based APS (Active Protection System) which produces threat matrix and maps all data flows and catching illegal accessing attempts. The mining process is accompanied by active session spores, defensive agents and honey pots that would secure and monitor the centralized data and the Information payloads. As a result, the author gave a theory of a non-prototype system. Although this schema is only a preposition but it demonstrates how also user-side active programs could be beneficial in enhancing security. Plus, the utilization of the threat matrix is regarded to be of gravity since it maps the data flows thus, security threats syndromes could be noticed and treated.

Rohitash Kumar Banyal et. al [24] proposed a LAMP (Archetypal model of web service solution stacks, named as an acronym of the names of its original four open-source components: the Linux operating system, the Apache HTTP Server, the MySQL relational database management system (RDBMS), and the PHP programming language) low, medium and high authentication level based CAM (Cloud Access Management) system that would use hashed valued arithmetic Captcha Expression, multi-level authentication, mobile phone service as a OOB (out-of-band) secure channel, and secret splitting of authentication Factor. As a result, the proposed framework provided a feasible and efficient solution through the utilization of smart phone which made the system less vulnerable to ubiquitous users. In this schema, the utilization of standards aimed to maximize the security role of the system.

S. Bertram et. al [26] proposed a framework that compromises CORAS risk management process with CS-DST (Cloud security decision support tool), security tokens, and access control services. The authors also suggested the utilization of PBAC (Policy-Based Access Control) which utilizes policy enforcement interceptors, policy decision services, intrusion monitoring tools and service controller for and further modeling security requirements. As a result, the security policy reconfiguration was not time nor address constricted such as to changes in personnel, changes in the execution environment, and crisis situations. A risk management framework aided by a PBAC could be really a fruitful implementation since the risk is assessed through the defined access control policies which basically makes the security system more durable when it comes to exposing security threats and eliminate them.

According the above, systems that provide a sense of security differ in architecture and the way that they take the initiative to resolve security issues. This is due to the fact that companies implementing those systems prioritize their security tasks according to their needs, that is, while companies would require more security measures to be taken on specific levels other companies would deprioritize those implementations since the service they offer utilized in a different level. Security measures that provide simplicity, guarantees operability, insures stability and minimizes the chances of penetration and medaling should be considered. Systems such as IDS/IPS that would be able to filter all the traffic and update its rules to inspect deeper each and every packet have been found popular not only to cloud services providers but also to regular users and programmers. Systems that are able also to display risks and how to prevent them are also a key to insure further stability of the network. In addition, systems that are standard oriented and are maintained by standardizing bodies, that is, they are built on popular and well-known standards are also regarded to be the building blocks of profound security.

3. Benchmarking and Findings

In this section, five of the most utilized services in 2015 will be introduced and represented in Table 1, 2, 3, 4 and 5 respectively. This table illustrates the architectures, standards, methods, algorithm, service type that each service. The table also introduces the security measure(s) and vulnerabilities or drawbacks for each. The services are Microsoft365 [46], Cisco WebEx messenger [56], Force.com [60], Yammer [52] and ServiceNow [50] services. These services are seen to be the most popular and most utilized [18] [19].

To ensure that cloud services give the required security functionality, cloud services have been tailored by the service provider to suit the intended needs. This is why cloud services' security architecture differ from one service provider to the other. As discussed in this paper, some architectures are decomposed into layers that act synchronically to detect, report, and set countermeasures for attacks such as Microsoft 365. Others rely on different types of technology to enhance security like Force.com that utilizes Systrust SAS 70 type II infrastructure to enhance security. The methods may differ but the fact that they are all meant to do the same tasks such as securing data and preventing unwanted user to claim authority of accounts, privileges, etc. bind these systems as siblings. They provide the proper security needed in the favor of continuous maintenance and upgrades. One commonality that binds all the architectures is the utilization of standards for example. While standards are being monitored, and maintained by the bodies, the service providers ensure that their system is in a continuous balance. ServiceNow for example is totally based on the Nation Institute of Standards and Technology (NIST)'s Security Incident Response Application (SIRA) that would highlight infrastructure vulnerabilities. The utilization of encryption schemes was also noticed in architectures such as Yammer and Force.com in which they both relay on TLS/SSL encryption to boost their security.

Table 1: The characteristics of Microsoft 364 services

Service name	Security measures	Security technique\ Algorithm \ Special architecture used within the service	Potential drawbacks \ vulnerabilities
Microsoft 365 services Service Type: -IaaS -PaaS -SaaS	-Access control where a device is enrolled and becomes trusted. Role Based Access Control (RBAC) is also utilized where it controls access to information. In addition, multi-factor authentication is utilized. -Exchange Online Protection (EOP) used for email protection against spams and viruses. EOP is an email filtering service that helps protect costumers from spam and malware, and messaging-policy violations [44]. -Operational Security Assurance (OSA) sued to protect, detect, and respond to security threats. OSA is a framework that incorporates the knowledge that is unique to Microsoft [46]. -A large number of security measures that would ensure that the breach is "under control" on occurrence. Some of the measures utilized are for example live site penetration testing, perimeter vulnerability scanning, etc. -Data Loss Prevention technology which monitors and protects sensitive data. DLP is an insurance that sensitive data doesn't leak outside that corporation's network [37]. -eDescovery is noticed which tends to search for the message or document and hard-delete them. In addition to "90 days" policy in which data is deleted and is un recoverable after 90 days.	-ISO27001/27002 and NIST 800-53 standards are utilized -Four pillar security architecture in which the first regards breach prevention, the second pillar is responsible of breach detection, the third pillar is responsible if respond to breaches and the fourth pillar is responsible of recover form breaches.	-Not all Office 365 features are fully enabled using IPV6 [31]. -Microsoft doesn't provide support for costumer-owned WLAN acceleration and caching devices with office 365 [38] -Microsoft Office 365 utilizes an IDPEmail based SAML 2.0 to deny attackers any data acquisition. SAML is regarded to add complexity to the system plus, it attracts more attackers [47]. -Cross-domain authentication bypass vulnerability was discovered [48].

Table 2: The characteristics of Cisco WebEx services

Service name	Security measures	Security technique\ Algorithm \ Special architecture used within the service	Potential drawbacks \ vulnerabilities
Cisco WebEx messenger services Service type: - IaaS - SaaS	- "Data In Motion" security measures to safeguard data between clients. In addition, it Cisco utilizes "Data At Rest" which is used to secure data stored - Channel encryption for protection against spoofing and SPAM. -Access control is based on "white" and "black" account listing technique. -Firewalls and advanced intrusion detection and prevention system to fortify security. - Files are saved on separate physical disks or isolated using logical unit numbers (LUNs) [57] which is based on the (SCSI) standard [58]. -Tiered backups involve both online (Tier 1) and offline (Tier 2) saves, and data is stored in two geographically dispersed data centers.	-WebEx Messenger utilizes Extensible Messaging and Presence Protocol (XMPP) - Simple Authentication and Security Layer (SASL) and the DIGEST-MD5 mechanism - Security Assertion Markup Language (SAML). -Each server build is based on a minimal installation of the Linux operating system, and hardened based on guidance from Security Technical Implementation Guides (STIGs) published by the National Institute of Standards and Technology (NIST). - 128-bit Secure Socket Layer (SSL) and a 256-bit Advanced Encryption Standard (AES) protection.	- Multiple Cisco products incorporate a version of the OpenSSL package affected by one or more vulnerabilities that could allow an unauthenticated, remote attacker to conduct man-in-the-middle attacks on an SSL/TLS connection [59].

Table 3: The characteristics of Force.com services

Service name	Security measures	Security technique\ Algorithm \ Special architecture used within the service	Potential drawbacks \ vulnerabilities
Force.com Service Type: -IaaS -SaaS	-Stateful packet inspection (SPI) known to dynamic *packet* filtering, is a firewall technology that monitors active connections and is mechanized to know which packets are allowed in the network [41]. -Bastion hosts (special-purpose computers designed to withstand attacks) act as hardened barriers between the perimeter and core firewalls. -Two factor authentication system without the usage of cookies to store confidential user and session information. -Monitoring and termination of idle sessions.	-End-to-end TLS/SSL. -Single sign-on using Security Assertion Markup Language (SAML). -LDAP (Lightweight Directory Access Protocol) service adaptation or authentication using a token instead of a password. -At an infrastructure and network SysTrust SAS 70 Type II is utilized.	-Java 5 based Apex (a proprietary language used in Force.com) is considered to be lagging behind other languages through its lacking of namespaces\packages [42]. -The "force.com IDE", aka force.com eclipse plugin, is incredibly slow [42].

Table 4: The characteristics of Yammer services

Service name	Security measures	Security technique\ Algorithm \ Special architecture used within the service	Potential drawbacks \ vulnerabilities
Yammer Service type -IaaS -SaaS	-Secure development best practices are utilized that integrate security reviews throughout design, prototype and deployment. -All data is classified as confidential and treated as such through the aid of firewalls. -The utilization of hardened Linux servers. Which are patched within 24 hours. -Strong encryption on disk mechanism is adopted and backups are transferred offsite over Secure Socket Shell (SSH) and properly deleted after 6 months. SSH is a network protocol used to access a remote computers and messages transmissions. [52]. -Log in attempts from unrecognized browsers will require users to reconfirm access to their corporate email addresses. -Restricted IP accessing is utilized. -Regex matching system is utilized to alert if thread matching patterns or key words occurs.	-SSL/TLS SAML 1.1/2.0 based SSO.	-Self XSS (Cross-site scripting) vulnerability was detected in which attackers could have injected scripts to [53]. -Another vulnerability is configuration Module in External Networks [54].

Table 5: The characteristics of ServiceNow services

Service name	Security measures	Security technique\ Algorithm \ Special architecture used within the service	Potential drawbacks \ vulnerabilities
ServiceNow Service type -IaaS	-Configuration Management Database (CMDB) which is a database that contains all relevant information about the components, knowns as configuration items (CI), of the information system used in an organization's IT services [49]. -Vulnerability and threat assessment tools, analytics engines, advanced intrusion detection systems platform which triggers CMDB, and Security Operations Security information and event management (SIEM) solutions which provides holistic view of an organization's information technology (IT) security are utilized [49]. -Automation and Orchestration which automate security-run-books and accelerate response times during a security incident. -Automated remediation can be enabled to reduce the load on the system so that it can focus on more sophisticated attacks.	-A National Institute of Standards and Technology (NIST) based Security Incident Response Application (SIRA) is utilized to highlights infrastructure vulnerable to attacks	-Utilizes a Single Tenant Architecture [50]. -Too many categories of items with seemingly arbitrary differences in functionality [51]. -Honing is difficult for the basic user [51].

Regarding the above, five widely used [32] cloud service providers namely Microsoft 365, Cisco WebEx messenger, Force.com, Yammer, Servicenow are assessed in terms of their security services:

1. All the service providers above have core security features which reflects contemporary architectures \ standards and then the security is further enforced \ hardened with other features that insure higher security of sensitive data.
2. S. K. Sood et. al [27] proposal includes a two-level mechanism with utilization of SSL certificates and encryption. Yammer, Force.com and Cisco WebEx messenger services utilize the same discussed concepts in which SSL\TLS is utilized to secure all the connections made and CryptDB mechanism which requires SQL encryption.
3. J. Bernal Bernabe et. al [3] an OWL2 and SWRL (OWL2 based language) based security architecture is proposed. As observed, none of the above services adopts ontology based security techniques.
4. X. Z. X. Zhang et. al [40] discusses an ISO/IEC 27001 standard based security technique and the response workflow is based on the NIST (National Institute of Standards and Technology) risk management guide for information technology systems. Microsoft 365 services basically utilizes the same security standard meanwhile Cisco WebEx Messenger and servicenow services utilizes the response workflow concept.
5. K. S. Gill et. al [8] proposes an Intrusion Detection System (IDPS). Cisco WebEx messenger and servicenow highlights these systems utilizations.
6. A. Ahmed et. al [2] proposes a "4-eyed" security mechanism through COBIT. A. Khrisna et. al [20] also recommends COBIT as a solution the solve security problems in which passwords, certificates, public keys, real monitoring and auditing are considered. Cisco WebEx services security measures cover the above discussed points without the utilization of COBIT.
7. H.-Y. Lee et. al [10] specifies a multi-layered security system. The author also proposed a multi-layered security architecture in which the based on a multi-prolonged approach. Another system is considered by V. Chang et. al [38] in which the system is based on the international standard, ISO27001:2005. O. Rebollo et. al [23] also recommends the usage of a multi-layered security system through the utilization of NIST-FISMA standard. It is realized that Microsoft 365 services abide by a same security architecture in which the security "4 pillar" based system with the adoption of the ISO27001:2005 standard.
8. M. Almorsy et. al [55] recommends a ISGcloud based "four core governance" process. Yammer resembles the discussed security architecture in which data leakage, and low level logical firewalls are put into consideration.
9. J. P. Veigas et. al [21] proposes a system that is based on multi-layers and DE hardening component. Cisco WebEx messenger and Servicenow utilize the same concept of utilizing of IDE while, Microsoft 356 services utilize the aspect of multi-layer architecture security system.
10. Flood, J. et. al [7] discusses a spore based APS system. The technology discussed is quite new and still under discussion.
11. Rohitash Kumar Banyal et. al [24] focuses on the utilization of CAM systems for access control. Microsoft 365 services utilizes Role Based Access Control (RBAC) for services to be accessed.
12. S. Bertram et. al [26] focuses on the implementation ACS and utilizes and intrusion monitoring tool to harden the security system. Microsoft 365 implements a RBAC system in addition Cisco WebEx messenger and Servicenow utilize intrusion detection systems to improve security.

4. Discussion and Conclusion

We have assessed frameworks were found to be the most popular in 2015. The discussed services were Microsoft 365, Cisco WebEx messenger, Force.com, Yammer, service now. while most of these services were found to have commonalities like a multi-layered security architecture, others would acquire other methodologies i.e. access controls and firewalls as their building blocks or additional systems to re-enforce security.

As it can be seen that most of the systems would resemble both Microsoft 365 and Cisco WebEx messenger services architectures therefore, we can derive that the ideal security system to preserve data (sensitive and other of kinds) could be of the form of hybrid systems that would adopt both the concepts of Microsoft 365 and Cisco WebEx messenger services. In other words, systems that ensure not only the sense of security directly to the user i.e. username/password combinations, captchas, etc. but also manage to play a role behind the curtains such as deleting data after 90 days, access control, etc. in addition systems that is more modules-oriented, especially regarding security, are considered to be more adaptable to change of modules, updates, and adding extra features. In this case, systems that resemble the Microsoft 365 systems are most likely to be chosen by companies running cloud services since the system can be manipulated not as a whole but as module-like which makes things for both companies and users much easier.

5. Acknowledgment

This article was presented as an oral presentation at the IMISC2017.

6. References

[1]. A. Apostu, F. Puican, G. Ularu, and G. Suciu, Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud 2 Cloud Computing, pp. 118–123, (2014).

[2]. Ahmed, A. Using COBIT to Manage the Benefits, Risks and Security of Outsourcing Cloud Computing. *COBIT Focus*, *2011*(2), 13–16. (2011).

[3]. Bernal Bernabe, J., Marin Perez, J. M., Alcaraz Calero, J. M., Garcia Clemente, F. J., Martinez Perez, G., & Gomez Skarmeta, A. F. Semantic-aware multi-tenancy authorization system for cloud architectures. *Future Generation Computer Systems*, *32*(1), 154–167, (2014).

[4]. Challenges for IT Based Cloud Computing Governance Yassine BOUNAGUla, Hatim HAFIDDIab, Abdellatif MEZRIOUla aISL Team, STRS Lab, (2010).

[5]. Cloud Security Alliance. Top Threats to Cloud Computing. *Security*, (March), 1–14, (2010).

[6]. F. Huang, H. Li, Z. Yuan and X. Li. An Application Deployment Approach Based on Hybrid Cloud *ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee*

international conference on intelligent data and security (ids), Beijing, 2017, pp. 74-79. (2017).
[7]. Flood, J. & Keane, A. A Proposed Framework for the Active Detection of Security Vulnerabilities in Multi-tenancy Cloud Systems., *in* 'EIDWT', pp. 231-235, (2012).
[8]. Gill, K. S., & Sharma, A. IDPS based Framework for Security in Green Cloud Computing and Comprehensive Review on Existing Frameworks and Security Issues. (2015).
[9]. Grundy, J., & Ibrahim, A. S. Collaboration-Based Cloud Computing Security Management Framework Collaboration-Based Cloud Computing Security Management Framework, (2011).
[10]. H.-Y. Lee and Y.-S. Tao, *Chapter 4 - Multitiered cloud security model*. Elsevier Inc., (2015).
[11]. Cloud computing types http://blog.marconet.com/blog/a-breakdown-of-the-3-types-of-cloud-computing Accessed 1st Nov 2017
[12]. Amazon official site http://www.amazon.com Accessed 1st Nov 2017
[13]. Google engine official site http://www.code.google.com/appengine Accessed 1st Nov 2017
[14]. Hadoop Apache official site http://www.hadoop.apache.org Accessed 1st Nov 2017
[15]. Topics about flexible computing http://www.hp.com/services/flexiblecomputing Accessed 1st Nov 2017
[16]. Big table official site http://www.labs.google.com/papers/bigtable.html Accessed 1st Nov 2017
[17]. Azure official site http://www.microsoft.com/azure/data.mspx Accessed 1st Nov 2017
[18]. Top five services 2016 https://www.skyhighnetworks.com/cloud-security-blog/the-20-totally-most-popular-cloud-services-in-todays-enterprise/ Accessed 1st Nov 2017
[19]. Topics about services architecture https://www.xml.com/pub/a/2001/01/24/rdf.html Accessed 1st Nov 2017
[20]. Khrisna, A. Risk Management Framework With COBIT 5 And Risk Management Framework for Cloud Computing Integration, 103–108, (2014).
[21]. King, N. J., & Raja, V. T. Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law and Security Review*, *28*(3), 308–319, (2012).
[22]. A., Task, J., & Transformation, F. Guide for Applying the Risk Management Framework to Federal Information Systems, *1*, (2016).
[23]. Rebollo, O., Mellado, D., Fernendez-Medina, E., & Mouratidis, H. Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. (2015).
[24]. Rohitash Kumar Banyal, Pragya Jain, and Vijendra Kumar Jain. Multi-factor Authentication Framework for Cloud Computing. Washington, DC, USA, 105-110. (2013).
[25]. Ryan, M. D. Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, *86*(9), 2263–2268. (2013).
[26]. S. Bertram, M. Boniface, M. Surridge, N. Briscombe and M. Hall-May, (2010) On-Demand Dynamic Security for Risk-Based Secure Collaboration in Clouds, pp. 518-525.
[27]. Sood, S. K. A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications*, *35*(6), 1831–1838. (2012).
[28]. V. Chang and M. Ramachandran, "07299312," vol. 9, no. 1, pp. 138–151, (2016).
[29]. Virtualization and Cloud Computing, Security Threats To Evolving Data Centers, Data Center Security, (2011)
[30]. Zhang, X. Z. X., Wuwong, N., Li, H. L. H., & Zhang, X. Z. X. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 1328–1334. (2007).
[31]. Topics about security architectures http://searchnetworking.techtarget.com/definition/stateful-inspection Accessed 1st Nov 2017
[32]. Disadvantages of force.com http://stackoverflow.com/questions/1664503/disadvantages-of-the-force-com-platform Accessed 1st Nov 2017
[33]. Topics about online protection https://technet.microsoft.com/library/exchange-online-protection-service-description.aspx Accessed 1st Nov 2017
[34]. Microsoft 365 service official; site download.microsoft.com/.../Operational-Security-for-Online-Services-Overview.pdf Accessed 1st Nov 2017
[35]. Topics about data loss prevention http://whatis.techtarget.com/definition/data-loss-prevention-DLP Accessed 1st Nov 2017
[36]. Microsoft 365 support site https://support.office.com/en-us/article/IPv6-support-in-Office-365-services-c08786fb-298e-437c-8222-dab7625fc815?ui=en-US&rs=en-US&ad=US&fromAR=1 Accessed 1st Nov 2017
[37]. Disadvantages of Microsoft 365 service https://threatpost.com/office-365-vulnerability-exposed-any-federated-account/117716/ Accessed 1st Nov 2017
[38]. Disadvantages about Microsoft 365 service http://www.securityweek.com/serious-flaw-exposed-microsoft-office-365-accounts Accessed 1st Nov 2017
[39]. Advantages of ServiceNow service http://searchdatacenter.techtarget.com/definition/configuration-management-database Accessed 1st Nov 2017
[40]. ServiceNow architecture http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM Accessed 1st Nov 2017
[41]. Disadvantages of ServiceNow http://seekingalpha.com/article/1111961-after-interviewing-more-industry-insiders-i-am-even-more-bearish-on-servicenow Accessed 1st Nov 2017
[42]. Yammer architecture https://www.trustradius.com/products/servicenow/reviews Accessed 1st Nov 2017
[43]. Disadvantages of Yammer http://www.securityfocus.com/archive/1/530292 Accessed 1st Nov 2017
[44]. Disadvantage of Yammer http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL Accessed 1st Nov 2017
[45]. M. Almorsy, J. Grundy and A. S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework," *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, Washington, DC, pp. 364-371. (2011).

[46]. Cisco WebEx official site https://www.google.com/search?q=vulnerability+of+cisco+webex+messenger Accessed 1st Nov 2017
[47]. Information about Logical Unit Numbers [LIU] http://searchstorage.techtarget.com/definition/SCSI Accessed 1st Nov 2017
[48]. Information about Small System Computer Interface (SCSI) http://searchnetworking.techtarget.com/definition/stateful-inspection Accessed 1st Nov 2017
[49]. Disadvantages of Cisco WebEx messenger service https://www.google.com/search?q=vulnerability+of+cisco+webex+messenger&ie=utf-8&oe=utf-8&client=firefox-b-ab&gfe_rd=cr&ei=TshIV- Accessed 1st Nov 2017
[50]. Force.com architecture https://developer.salesforce.com/page/Multi_Tenant_Architecture Accessed 1st Nov 2017