IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 1, Ser. III (Jan - Feb 2020), PP 13-19
www.iosrjournals.org

Strategies for Securing Cloud Services

OmoyiolaBayoOlushola
School of Information Systems & Technology, Walden University, USA

Abstract: *The security of cloud services has become very necessary due to the huge demand for cloud services because of itsversatile applications. The security factor in cloud computing has been noted to be the most critical factor in cloud as it has the most impact on cloud operations. The strategies for securing cloud computing comprises formal, informal and technical strategies. The strategies include confidentiality, integrity, availability, privacy, compliance, trust, incident response, governance, and security awarenessstrategies. This paper explores the strategies for securing the cloud, analyzes discussions on cloud security and the opportunities, gaps, and future developments of cloud security.*

Keywords*: Security, Cloud, Strategy, Cloud computing, Data, Clients, Information, and Risks*

Date of Submission: 26-12-2019 Date of Acceptance: 31-12-2019

I. Introduction

Cloud computing is developing and turning into a global practice for keeping, sharing, and accessing information with many clients and organizations. At the point when firms decide to implement cloud computing, there is a change in IT practices on identifying with how data is accessed, kept and secured. With the implementation of a modern technology, clients anticipate that business chiefs should ensure confidential information on their network (Nanavati, Colp, Aiello, & Warfield, 2014). It is important for firms to secure their information systems from being compromised, oversee network resources, and develop trust with clients (Sauls, &Gudigantala, 2013). This study is unique and original in the sense that not many research works focus on the security strategies of cloud computing. It will explore the cloud security strategies, and analyze the opportunities, gaps, and challenges of cloud security.

The purpose for the research is to explore strategies for securing cloud computing. In this section, I present the background of problem, strategies for security the cloud, discussion on securing cloud computing, opportunities, gaps and future research and conclusion.

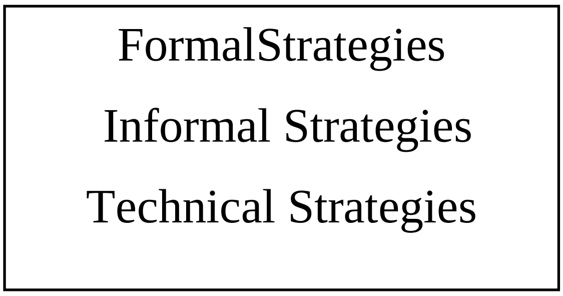
1.1 Background of the Problem

Firms spent a lot of money to improve the security of their cloud infrastructure (Nanavati et al., 2014). The usage of cloud computing by Information Technology professionals to meet business needs is becoming more common because of the good benefit of storing data in the cloud and accessing it whenever needed. At the point when organizations put resources into their Information Technology department, they see an increment in the firm's worth (Avram, 2014). Therefore cost plays a key role. Even when it comes to security. It is always the function of cloud service providers to mitigate the security risks of the cloud and increase the reliability of its infrastructure so as to foster the relationship between them and their clients (Nanavati et al., 2014).

Cloud computing has several benefits but it also has security challenges which includes data breaches and data loss. Several researchers have written on cloud security, its challenges and security strategies and some of them hold different views. This paper contains analysis of the security challenges of the cloud and security strategies for cloud computing.

II. Security Strategies for Cloud Computing

Strategies for securing cloud computing comprise of formal, informal and technical strategies (Ahmed & Hossain, 2014; Chang&Ramachandran, 2015). The strategies are based on the Routine Activities Theoryas seen in*Fig. 1* below.The formal strategies include compliance strategies (with policies and regulations), governance strategies and incident response strategies (Silbey, 2013).The informal strategies include the strategy of cloud security education, training, and awareness, so as to develop a mature security risk culture (Lowry and Moody, 2014). While the technical strategies include strategies such as confidentiality, integrity, availability, privacy, and trust strategies.



FormalStrategies

Informal Strategies

Technical Strategies

Figure 1.Security Strategies based on Routine Activities Theory

2.1. Formal Strategies

The first set of strategies are formal strategies. These include compliance strategies (with policies and regulations), governance strategies and incident response strategies (Silbey, 2013).

2.1.1.Compliance strategy. Compliance is another security strategy for securing cloud computing. It is the second most critical factor affecting cloud computing adoption (Rao &Selvamani, 2015). Seventeen percent (17%) of Information Technology architects opined that regulatory compliance is one of the top sources of worry when considering cloud adoption (Tang, & Liu, 2015). When a company is compliant, their data would be protected, and the services of the company would be in alignment with industry regulations. But when there is no alignment with laws, policies and regulations, there may be legal issues (Dove, Joly, Tassé, Burton, Chisholm, Fortier, & Kent, 2014). Compliance strategy can affect perceived ease of use or, perceived usefulness to select cloud computing. With the development of laws and policies and regulations for cloud computing, there should be compliance which would have a direct impact. Some known regulations include Family Educational Rights and Privacy Act, Electronic Communications Privacy Act, and Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act, and Gramm-Leach-Bliley Act (Srinivasan, 2013).

2.1.2.The Strategy of Cloud Security Governance. The strategy of cloud security governance is another strategy for cloud security. With cloud security governance, policies can be developed and applied to oversee cloud computing services, and fulfill security and business objectives (Hung, Hwang, & Liu, 2013). Cloud security governance gives direction as regards data security and cloud. It helps to secure data wherever it may be located and also secure the cloud (Hung et al., 2013). It would also include cloud security policies, measurement and system management (Sareen, 2013).

2.1.3.Incident Response Strategy. Incident response strategy is another security strategy for securing the cloud. The cloud requires such a strategy for the monitoring of the tools, processes, and programs in the cloud system and for quick reporting, root-cause identification, and incident resolution responses when there are incidents. Incident response has been one of the challenges of data security (Rao &Selvamani, 2015). As a result of the architectural design of some cloud systems, such as multi-tenancy and high scalability, incident response could pose challenges to doing digital forensics and finding the attack vectors (Ghilic-Micu, Stoica, &Uscatu, 2014). Kalloniatis, Mouratidis, Vassilis, Islam, Gritzalis, &Kavakli (2014) opined that there should be holistic forensic framework for the incidents detection and incident response.

2.2. Informal Strategies

The second set of strategies are informal strategies. These include the strategy of cloud security education, training, and awareness, so as to develop a mature security risk culture (Lowry& Moody, 2014).

2.2.1.The Strategy of Cloud Security Awareness. The strategy of cloud security education training and awareness is one of cloud security strategies. It is necessary to educate the cloud professional because any mistake can have a major impact on the job of the professional and also on the stored data (Donald, Oli, &Arockiam, 2013). The mistake could lead to a data breach and cause reputational risks for the organization. Security awareness is a good security measure that can prevent the occurrence of internal and external security risks. The security awareness should also be backed with action (Stanciu, &Tinca, 2016).

2.3. Technical Strategies

The third and final set of strategies are the technical strategies. These include strategies such as confidentiality, integrity, availability, privacy, and trust strategies. These includes the principles of authentication, authorization, auditing, encryption, password management, identity management, and access management etc.

2.3.1. Confidentiality strategy. Confidentiality is one of the CIA triad. It is also one of the security strategies for securing the cloud. When secured data and systems are only accessed by authorized users, there is confidentiality (Ranjith, Vijayachandra, Sagarika, &Prathusha, 2015; Zissis &Lekkas, 2012). Confidentiality strategy may affect perceived ease of use or, perceived usefulness to select cloud computing. Measures such as access control, least privilege, encryption, authorization, auditing and authentication, identity and access management, password management etc. are measures that ensure confidentiality. Customers also need a guarantee that confidential data is not being accessed or used illegally by anyone including the cloud service provider (Rong, Nguyen, &Jaatun, 2013; Ranjith, Vijayachandra, Sagarika, &Prathusha, 2015; Stoetzer, 2016).

2.3.2. Integrity strategy. Integrity is another strategy from the CIA triad. It is also a security strategy for cloud computing. When data is not modified and it is kept away from unauthorized users, the authentic data is said to have integrity (Zissis &Lekkas, 2012). Integrity strategies such as data signing, whole file checking, encryption of data resting and inflight, and implementation of a software integrity check can be used to secure data. Data integrity remains one of the most important factors affecting cloud computing adoption (Oliveira, Thomas, &Espadanal, 2014).

2.3.3.Availability strategy. Availability is another strategy from the CIA triad which is the bedrock of information security and it is also one of the security strategies for securing the cloud. It is one of the challenges of data security (Rao &Selvamanu, 2015). Twenty nine percent (29%) of IT leaders view availability as a key factor affecting cloud computing adoption (Tang, & Liu, 2015). A service level agreement from the cloud service provider can help solve the problem of availability of service with promise of service uptime and reliable service ((Dhasarathan, Thirumal, &Ponnurangam, 2017). Availability can affect perceived ease of use or, perceived usefulness to select cloud computing. Availability ensures business continuity or continuous availability of data and services (Phaphoom, Wang, Samuel, Helmer, &Abrahamsson,2015).

2.3.4.Trust strategy. Trust is also one of the security strategies for securing the cloud. A trust strategy can affect perceived ease of use or, perceived usefulness to select cloud computing. Trust can be established when there is good relationship between the cloud service provider and their clients. A service level agreement for example can serve as a contractual agreement between them. Trust is an important determinant influencing the selection of cloud computing (Ali, Soar, & Yong, 2016). Private clouds win more trust than public clouds because public clouds are faced with external and internal threats (Wei, Ganjali, BeomHeyn, Sukwon, & Lie, 2015). When there is trust, there is security and there is availability of data. And when there is security and availability of data, there is trust.

2.3.4. Privacy strategy. Privacy is one of the security strategies for securing the data in the cloud. Privacy strategy can affect perceived ease of use or, perceived usefulness to select cloud computing. Privacy is the most critical factor affecting cloud adoption (Rao &Selvamani, 2015). Forty nine percent (49%) of Information Technology architects opined that privacy is a top source of worry when considering cloud adoption (Tang, & Liu, 2015). Firms and individuals take data privacy seriously because lack of it can cause data loss, financial loss and reputational risks (Ghorbel, Ghorbel, &Jmaiel, 2017).

III. Discussion On Securing Cloud Computing

Many researchers have published works on securing strategies on cloud computing. Ali, Khan, &Vasilakos (2015) did a study on security in cloud computing, focusing on the chances and problems. The trio analyzed security issues such as mobile application security, end-user privacy, authentication, and data security. The researchers indicated that the distributed computing indicates, amazing possibilities to offer savvy, simple to manage, flexible, and ground-breaking assets over the Internet. The cloud computing enhances the capacities of the equipment assets by ideal and shared utilization. The aforementioned shows support for the companies and end-users to transfer their services and applications to the cloud. Indeed, even the important framework, for instance, generation of power and plants for distribution are being relocated to the distributed computing worldview. In any case, the administrations gave by external cloud specialist co-ops include extra security dangers. The transfer of customer's assets (information, applications, and so on.) out of the authoritative control in a mutual domain where different clients are arranged increases the risks. The authors also analyzed the open issues and future developments on cloud computing which has been documented in the next section (Ali, Khan, &Vasilakos, 2015). Brandas, Megan, &Didraga (2015) did a research on global perspectives on Accounting Information Systems (AIS), with a focus on the Mobile and cloud approach. With regards to versatile and cloud innovation advancement, an ever increasing number of organizations receive such advances as foundation support for their exercises. The trio conducted a study on the fundamental zones of effect in utilizing cloud and versatile advances on AIS. Some research works have studied the positive job of utilizing cloud and portable advancements in business improvement. They opined that the advancements give adaptability, versatility and decreased support costs. They believe that, from a global perspective, AIS improvement utilizing cloud and versatile advances will prompt a revamping of the business engineering with noteworthy effect on business technique (Brandas, Megan, &Didraga, 2015).

Elhaida, &Frueh (2015) did a study on the protection of electronic mental health communication and management of records in this present time. The duo presented cloud storage as one of the means of backup for the health system. Cloud backup is very important so as to ensure continuous availability of patient records and so as to avoid a HIPAA compliance issue and lack of continuous care. The researchers presented common security concerns related with utilizing innovation in clinical administrations or research. The authors offer down to earth, simple to-utilize programming application answers for clinicians and analysts to verify quiet correspondence and records. The authors discussed issues as utilizing encoded remote systems, secure email, scrambled informing and videoconferencing, protection on interpersonal organizations, and others (Elhaida &Frueh, 2015). Smith (2016) opined that some hackers hack into companies' private information through cloud service providers. He indicated that any attack that involves penetration to a firm's internal network is a material cyber-attack. He opined that an attack may not be material from a monetary point of view, yet it is material from a cyber security perspective (Smith, 2016). Sookhak, Gani, Khan, &Buyya (2015) did a study on dynamic remote data auditing for protecting big data storage and for authenticating the integrity of the data kept in the cloud. They are likewise not material to huge information stockpiling in light of the high computational overhead on the reviewer. The authors came up with an effective remote data auditing strategy for protecting big data storage in cloud computing using an algrebraic signature (and depending on logarithmic mark properties) and for a distributed storage framework that causes least computational and correspondence costs (Sookhak, Gani, Khan, &Buyya, 2015). Soomro, Shah, & Ahmed (2016) studied security issues in cloud computing and how it relates to management. They opined that cloud computing has its own challenges for managers. Though it saves costs, it has a number of legal, ethical and security challenges. The trio opined that data security is the main problem with cloud computing as it decreases the development of cloud computing. Tankard (2015)conducted a study on data classification, the bedrock of information security. He opined that information security is turning into a perpetually squeezing concern and a lot is on the line for companies as the loss of any delicate recognizable data identified with clients can cause monetary, aggressive, brand and reputational harm (Tankard, 2015). Thompson, Ravindran, & Nicosia (2015) conducted a study on knowledge gained on data governancefrom a public sector application audit. Public offices routinely keep huge data about people in the network. The trio stressed the importance of data protection. The authors also opined the communal expectation that there would be standards, practices and procedures in relation to data access, privacy, security and disposal with overarching data governance in place (Thompson, Ravindran, & Nicosia, 2015). Ab Rahman, & Choo (2015) did a survey study on information security event management in the cloud. The authors showed that Incident taking care of strategy is the main strategy to reduce risks related to disclosure, integrity attacks and denial of service attacks against organization assets, just as limiting loss especially as organizations move to the cloud. The researchers surveyed existing incident taking care of and advanced forensic resource having the points of adding to the gaps in understanding of taking care of incidents in the cloud environment. The authors later proposed a calculated cloud incident management model that unites incident handling, the Capability Maturity Model and advanced audit for handling risk events for organizations utilizing cloud services (Ab Rahman & Cho, 2015). Chang, & Ramachandran (2015) conducted a quantitative study on implementing security of data using the Cloud Computing Adoption Framework (CCAF). The authors demonstrated that providing data security at real-time of data in the tune of petabytes is significant for cloud and grid computing. The researchers demonstrated that an ongoing overview on security of cloud expresses that the protection of the data of the user has the most elevated need just as concern. They proposed this is only attainable with a methodology that can be adoptable and that is systematic and well-structured. Therefore, they built up the Cloud Computing Adoption Framework specially made for protecting data in the cloud. The authors showed that security in many layers can ensure that data in real-time is secure and it comprises three security levels: access control and firewall; management of identity and prevention of intrusion; and encryption that is convergent (Chang, & Ramachandran, 2015). Chang, Ramachandran, Yao, Kuo, & Li (2016)suggested that when utilizing the versatility as a genuine model for big business cloud security, every single resilient trademark ought to be mixed to deliver more noteworthy effects. The authors opined that Cloud Computing Adoption Framework (CCAF) is a design model that mixes software strength, administration parts and rules and gives true case studies to create more prominent effects to the firms embracing security and cloud computing. With CCAF, there is alignment in business and gives dexterity, productivity and unification for business focused edge. The authors presented the analysis and decided that the utilization of CCAF can enhance security for big business cloud computing (Chang, Ramachandran, Yao, Kuo, & Li, 2016). Kazim, & Ying (2015) conducted a survey study on high level security risks in cloud and grid computing. The researchers proposed that cloud computing empowers the usage of resources in a shared capacity, for example, network, storage, software, and applications through internet. The creators demonstrated that cloud end-users can rent various resources as indicated by their necessities, and receive cash just for the services they use. And that in spite of all the merits of cloud there are numerous security challenges identified with virtualization, hardware, network, information and specialist co-ops that go about as a huge boundary in the appropriation of cloud in the IT sector. The creators reviewed the high-level security challenges identified with cloud computing. For every one of these security risks they portrayed how it very well may be utilized to abuse cloud parts and its impact on cloud substances, for example, users, and providers and the services that should be done to avert these risks. The creators proposed that these solutions incorporate the security procedures from resources just as the best security rehearses that would be trailed by cloud managers (Kazim, & Ying, 2015). Kote, Raja, & Raju (2015) conducted a study on cloud data security challenges and its solutions. The researchers suggested that distributed cloud computing is rapidly increasing innovations linked with utility computing, grid computing, and distributed systems. Cloud service suppliers, for example, Google, Microsoft, IBM, Amazon give their clients the privilege of developing their solutions in cloud condition and to access them from anywhere. The authors indicate that cloud information are managed and get to a remote server with the aid of services given by cloud administration suppliers. The researchers suggested that giving security is an important stress as the data is sent to the remote server over the internet. The authors suggested that before doing Cloud Computing in a firm, security problem could be watched out for. The researchers featured information security related problems in cloud condition and solution. The authors rapidly check problems in distributed computing security. The researchers indicated that the way that data is sent to the cloud service supplier is perceived as the inside logical problems that leaves distributed computing protection from various themes in executing protection. (Kote, Raja, & Raju, 2015). Krishna, Kiran, Murali, & Reddy (2016) conducted a study on Security challenges in service model of cloud. The authors opined that providers and clients; availability, authenticity, integrity, privacy and confidentiality are critical issues. The researchers indicated that the security of PaaS clouds is taken from numerous views like control of access, privacy and service coherence while ensuring the service supplier and the clients (Krishna, Kiran, Murali, & Reddy, 2016). Rafeeq, & Kumar (2015) conducted a study on the available and safe cloud data storing and de duplication. The authors opined that privacy and security are major problems of the public cloud. The authors suggested that so as to solve the security challenges, there was a reliable proposal and implementation of Open Stack Swift, another client-side de-duplication scheme for safely sharing and keeping outsourced data through the public cloud. The authors suggested that security issues, requirements and challenges that service providers encounter during cloud building. The researchers indicate that the proposal has two-fold. Better confidentiality towards unauthorized users, and integration of access rights in metadata file. This indicates each client computing according to data key to encode the data that he wants to keep in the cloud (Rafeeq, & Kumar, 2015). Rao, &Selvamani (2015) conducted a study on security of data problems and its cloud computing solutions. They also discussed development of future solid standards for cloud computing security. The authors indicated that provision of a protected data access in the cloud, advanced coding methods can be utilized for keeping and recovering data from the cloud. And that legitimate key management methods can be utilized to control access to the cloud such that only authorized persons can access the data (Rao, &Selvamani, 2015).Roy, Sarkar, Ganesan, & Goel (2015) conducted a study on securing the cloud, from the view point of a service based firm. The authors suggested that in cloud, the core mechanism of security is in virtualization. .i.e. the implementation of commands at various levels of privilege. Security is the main root cause of such VM crashes. This involves changing the cloud storage, hypervisor and images of VMs utilized rarely, and remote cloud client utilized by the client and risk from attackers. Though utilizing protected infrastructures such as private clouds reduced many of these security challenges, most cloud clients utilize lower costs options like private clouds, thus an intensive analysis of all realized security problems is relevant. Consequently the authors analyzed progressing research in cloud security arranged by the attack scenarios abused most regularly in cloud. The authors investigated scenarios of attacks that needs protecting the hypervisor, misusing co-residency of VMs, management of VM image, reducing insider risks, protecting storing in clouds, abuse of lightweight SAAS users, and ensuring propagation of cloud data. The authors discusses organizational security suites in clouds (Roy, Sarkar, Ganesan, & Goel, 2015). Tang & Liu (2015) opined that the adoption of SaaS has its own challenging security risks. The researchers suggested that transferring a firm's sensitive data to providers enlarges and makes complex the risk landscape in which the firm works. The authors featured the ramifications and importance of a structured choice of a provider in meeting the necessary security strength based on the firm's specific security architecture. The researchers proposed a holistic model, called Function Auditability, Governability and Interoperability (FAGI), as a methodology to enable a cloud user to choose and use a good provider through four main choices: Choosing a secured cloud that has good security roles; Selecting an auditable cloud through tests; Selecting out a manageable cloud that offers the necessary transparency; Going for a cloud that offers the needed portability (Tang, & Liu, 2015).

IV. Opportunities, Gaps and Future Research

Ali, Khan, &Vasilakos (2015) opined that there are opportunities and open issues such as multi-tenancy, virtualization, multi tenancy, shared resource pool, and privacy and security issues in cloud computing. The authors suggested that cloud and portable innovation selection require a thorough examination of information and application security because Accounting Information System process and store a progression of delicate and classified information (Brandas, Megan, &Didraga, 2015). Soomro, Shah, & Ahmed (2016) opined that cloud-based computing has a number of legal, ethical and security challenges. The trio opined that data security is the main problem with cloud computing as it decreases the growth of cloud-based computing. Krishna, Kiran, Murali, & Reddy (2016) identified the following as the security challenges of cloud computing: invasion by clients, Shared Technology Vulnerabilities, Failures in Provider Security, Availability and

Reliability problems, Combining Provider and Customer Security Systems, Legal and Regulatory challenges, Application Programming Interfaces that are not secure, Perimeter Security Model Broken, Data Leakage or loss, Insiders that are malicious, Unknown Risk Profile, and Account, Traffic Hijacking & Service. Rao &Selvamani (2015) highlighted the data security challenges as data breaches, confidentiality attacks, integrity attacks, and availability attacks, datacenter operation challenges, storage attacks, segregation attacks, access risks, locality attacks, data loss and data leakage. They also offered solutions such as intrusion prevention systems, integrity check, encryption, access control, authentication, and attribute based policies to secure cloud computing (Rao, &Selvamani, 2015). Soomro, Shah, & Ahmed (2016) opined that the management's decisions regarding cloud-based activities are technical and that the managers face challenges which include regulatory implications, information security cultural changes, information security audit implications, ethical and legal problem, information audit, information security control, many other business management challenges and a need to know business challenges affecting cloud computing.

Works of the future to combine security and auditing tool to ensure policy agreement among various involved entities are urgently required (Ali, Khan, &Vasilakos, 2015).

Sookhak, Gani, Khan, &Buyya (2015) opined that future work would concentrate on extending method for auditing the integrity of large archival files in distributed cloud storage systems. Ab Rahman & Cho (2015) discussed future works that would include both real world data and simulated data in a private cloud computing environment to decide the utility of the conceptual model. The duo also discussed on future works like a collaborative and international cloud incident management platform with the objectives of sharing information between many stakeholders that are geographically dispersed and implementing real-time incident handling and reaction to malicious cyber activities in real-time. The authors also wanted a consistent definition for cybersecurity incident for the future (Ab Rahman & Cho, 2015). Chang, & Ramachandran (2015) opined that cloud computing adoption framework would be increasingly successful when joined with Business Process Model and Notation simulation to assess security and Penetration test results.

V. Conclusion

Cloud computing has been beneficial for many firms for access and availability purposes. However, attackers who hack cloud services have given clients, some security concerns. The study explored strategies utilized by IT leaders to secure data on the cloud. Formal, Informal and Technical Strategies for securing cloud services likeconfidentiality, integrity, availability, privacy, compliance, trust, incident response, security awareness and governance were analyzed. Opportunities, gaps and future works were also discussed. Published works on security strategies of cloud computing were also analyzed. The findings of this study may contribute to social change by reducing clients' concerns with respect to the protection of the data being hosted inside the cloud. It may also contribute to social change by improved confidentiality of data, reduction in the occurrence of breaches, enhanced integrity of personal information, continuous availability of cloud services and the security of data through improved cybersecurity compliance and awareness.

References

[1]. Ab Rahman, N. H., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security, 49*, 45–69.doi:10.1016/j.cose.2014.11.006.

[2]. Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications (IJNSA), 6*, 25–36. doi:10.5121/ijnsa.2014.6103.

[3]. Ali, M., Khan, S. U., &Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305,* 357–383. doi:10.1016/j.ins.2015.01.025.

[4]. Ali, O., Soar, J., & Yong, J. (2016). An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments. *Journal of Information Security and Applications, 27*, 19-34. doi:10.1016/j.jisa.2015.11.006.

[5]. Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, 12, 529-534. doi:10.1016/j.protcy.2013.12.525.

[6]. Buyya, R., Vecchiola, C., &Selvi, S. (2013). Mastering cloud computing: Foundations and applications programming. Waltham, MA: Elsevier.

[7]. Brandas, C., Megan, O., &Didraga, O. (2015). Global perspectives on accounting information systems: Mobile and cloud approach. *Procedia Economics andFinance, 20,* 88–93. doi:10.1016/s2212-5671(15)00051-9

[8]. Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing, 9*(1). 138-151. doi:10.1109/tsc.2015.2491281

[9]. Chang, V., Ramachandran, M., Yao, Y., Kuo, Y., & Li, C. (2016). A resiliency framework for an enterprise cloud. *International Journal of InformationManagement, 36,* 155–166. doi:10.1016/j.ijinfomgt.2015.09.008.

[10]. Dawson, P. (2015). Five ways to hack and cheat with bring-your-own-device electronicexaminations. *British Journal of Educational Technology, 47*, 592–600.doi:10.1111/bjet.12246.

[11]. Dhasarathan, C., Thirumal, V., &Ponnurangam, D. (2017). A secure data privacy preservation for on-demand cloud service. *Journal of King Saud University -Engineering Sciences, 29(2),* 144-150. doi:10.1016/j.jksues.2015.12.002.

[12]. Donald, A. C., Oli, S. A., &Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. *International Journal of Electronics and InformationTechnology (IJEIT), ISSN, 3*(1), 2277-3754.

[13]. Dove, E. S., Joly, Y., Tassé, A. M., Burton, P., Chisholm, R., Fortier, I & Kent, A. (2014). Genomic cloud computing: legal and ethical points to consider. *EuropeanJournal of Human Genetics*. *23,* 1271–1278. doi:10.1038/ejhg.2014.196

[14]. Elhaida, J. D., &Frueh, B. C. (2015). Security of electronic mental health communication and record-keeping in the digital age. *The Journal of ClinicalPsychiatry*, *77*(2), 262-268. doi:10.4088/jcp.14r09506

[15]. Ghilic-Micu, B., Stoica, M., &Uscatu, C. R. (2014). Cloud computing and agile organization development. *Informatica Economica, 18,* 5–13. doi:10.12948/issn14531305/18.4.2014.01

[16]. Ghorbel, A., Ghorbel, M., &Jmaiel, M. (2017). Privacy in cloud computing environments: A survey and research challenges. *Journal of Supercomputing*, *73*(6), 2763-2800. doi:10.1007/s11227-016-1953-y

[17]. Hung, C. N., Hwang, M. D., & Liu, Y. C. (2013). Show the way to information security governance for universities in taiwan. *Applied Mechanics and Materials*, *278-280*, 2199. doi:10.4028/www.scientific.net/amm.278-280.2199

[18]. Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., &Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces, 36,* 759–775. doi:10.1016/j.csi.2013.12.010

[19]. Kazim, M., & Ying, S. (2015). A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications, 6 (3), 109-113*. doi:10.14569/ijacsa.2015.060316

[20]. Kote, A., Raja, P. V. K., & Raju, M. V. (2015). Cloud data security challenges and its solutions. *International Journal of Computer & Communication EngineeringResearch*, *3*(5), 89-92.

[21]. Krishna, B. H., Kiran, S., Murali, G., & Reddy, R. P. (2016). Security issues in service model of cloud security environment. *Procedia Computer Science*, *87*, 246-251. doi:10.1016/j.procs.2016.05.156.

[22]. Lowry, P. B., & Moody, G. D. (2014). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, *25*, 433–463. doi:10.1111/isj.12043

[23]. Nanavati, M., Colp, P., Aiello, B., & Warfield, A. (2014). Cloud security: A gathering storm. *Communications of the ACM*, *57*(5), 70–79.

[24]. Oliveira, T., Thomas, M., &Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, *51*(5), 497-510. doi:10.1016/j.im.2014.03.006

[25]. Phaphoom, N., Wang, X., Samuel, S., Helmer, S., &Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems & Software, 103*, 167-181. doi:10.1016/j.jss.2015.02.002.

[26]. Pyrooz, D. C., Decker, S. H., & Moule Jr, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*, 471– 499. doi:10.1080/07418825.2013.778326

[27]. Rafeeq, M. D., & Kumar, C. S. (2015). Reliable secure data storage in the cloud environments and de duplication. *International Journal of Computer Science andEngineering*, *3,* 1086–1091.

[28]. Ranjith, G., Vijayachandra, J., Sagarika, P., &Prathusha, B. (2015). Intelligence based authentication – Authorization and auditing for secured data storage. *InternationalJournal of Advances in Engineering & Technology, 8*, 628-636.

[29]. Rao, R. V., &Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*, 204–209. doi:10.1016/j.procs.2015.04.171

[30]. Roy, A., Sarkar, S., Ganesan, R., & Goel, G. (2015). Secure the cloud: From the perspective of a service-oriented organization. *ACM Computing Surveys (CSUR)*, *47(*3*),* 1-30. doi:10.1145/2693841

[31]. Sareen, P. (2013). Cloud computing: types, architecture, applications, concerns, virtualization and role of it governance in cloud. *International Journal ofAdvanced Research in Computer Science and Software Engineering*, *3(3)*, 533-538.

[32]. Sauls, J., &Gudigantala, N. (2013). Preparing information systems (IS) graduates to meet the challenges of global IT security: *Journal of Information Systems Education*, *24*, 71–73.

[33]. Silbey, S. S. (2013). Organizational challenges to regulatory enforcement and compliance a new common sense about regulation. *The Annals of the American Academy ofPolitical and Social Science*, *649*, 6–20. doi:10.1177/0002716213493066

[34]. Smith, G. S. (2016). Evaluating materiality in cybercrime footnotes. *Journal ofCorporate Accounting and Finance, 27*, 77–87. doi:10.1002/jcaf.v27.2

[35]. Sookhak, M., Gani, A., Khan, M. K., &Buyya, R. (2015). Dynamic remote data auditing for securing big data storage in cloud computing. *Information Sciences*, *380,* 101-116, doi:10.1016/j.ins.2015.09.004.

[36]. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal ofInformation Management*, *36*, 215–225. doi:10.1016/j.ijinfomgt.2015.11.009.

[37]. Stanciu, V., &Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting & ManagementInformation Systems*, *15,* 112-130.

[38]. Stoetzer, O. R. (2016). You are your password: IT and public safety personnel's views of biometrics as identity and access management on college campuses (Order No. 10130912).

[39]. Srinivasan, S. (2013). Is security realistic in cloud computing? *Journal of InternationalTechnology and Information Management, 22,* 47-66.

[40]. Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security*, *50,* 60–73. doi:10.1016/j.cose.2015.02.001

[41]. Tankard, C. (2015). Feature: Data classification – the foundation of information security.*Network Security*, *2015,* 8–11. doi:10.1016/S1353-4858(15)30038-6

[42]. Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *GovernmentInformation Quarterly*, *32,* 316–322. doi:10.1016/j.giq.2015.05.001

[43]. Thornham, H., & Cruz, E. G. (2018). Not just a number? NEETs, data, and data logical systems. *Information, Communication & Society, 21*(2), 306-321. doi:10.1080/1369118X.2017.1279204.

[44]. Wei, H., Ganjali, A., BeomHeyn, K., Sukwon, O., & Lie, D. (2015). The state of public infrastructure-as-a-service cloud security. *ACM Computing Surveys*, *47*(4), 68:1-68:31. doi:10.1145/2767181

[45]. Zissis, D., &Lekkas, D. (2012). Addressing cloud computing security issues. *FutureGeneration Computer Systems*, *28*(3), 583-592. doi:10.1016/j.future.2010.12.006