International Journal of Research Findings in Engineering, Science and Technology | IJRFEST
p-ISSN: 2315-8417 | e-ISSN: 2489-0138
Volume 5, Number 1 May, 2023

A Survey of Security and Privacy Compliance in SAAS Business Applications: Challenges, Issues and Approaches to Compliance

Hammajam Ahmed Adamu
Department of Information Technology,
Modibbo Adama University, Yola Adamawa State

Article DOI: 10.48028/iiprds/ijrfest.v5.i1.07

Abstract

Benefits of Software as a Service (SaaS) applications such as low cost and scalability are motivating factors for businesses to adopt them. Government and industry bodies have implemented several regulations and standards to ensure effective security of SaaS applications and the entire cloud model; for example, the European Union requires every type of organisations to comply with the General Data Privacy Regulation when handling personal data of EU citizens. However, ensuring compliance with these regulations and standards by SaaS application service providers continue to remain a hurdle. Organisations have continued to question their compliance to these regulations for the security and privacy of their data. In this paper, we surveyed on related works on compliance, security and privacy in SaaS applications. We presented the challenges and issues of compliance and current approaches to overcome them. Finally, we concluded that there is a need for a compliance framework for SaaS applications.

Keywords: *Software as a service, Cloud, Compliance, Security and privacy, Regulations, and Standards*

Corresponding Author: **Hammajam Ahmed Adamu**

Background to the Study

SaaS applications and the cloud represents a significant shift in technology and a unique opportunity for the Nigerian oil and gas industry to become more efficient, agile, and much more profitable. However, what is the concept of cloud computing? According to [1] defines Cloud computing as a "computing model for enabling ubiquitous, convenient network access that is on-demand to a pool of shared computing resources and services that can be that are configurable and rapidly provisioned with minimal service provider interaction. According to [2], Cloud Computing has the following specific characteristics, resource pooling, broad network access, rapid elasticity, measured service and has three service models like namely Software as a Service (SaaS), Platform as a Service (PaaS), Infrastcurue as a Service (IaaS) and four deployment models. In this work, we focused on the Software-as-a-service model. The Software as a service (SaaS) delivery model is a situation where a full application is managed and hosted by the provider with users or customers consuming it over an internet connection using a web browser [1]. This has led to an strong interest in SaaS applications to [3], with revenues expected to reach about $85.1 billion in 2019. Software as a service applications provide additional benefits to businesses and organisations as incentives for adoption [4].

Despite these advantages of SaaS, issues of compliance, security and privacy challenges still exist in SaaS applications. There are much research works considering these issues, but we are purely concerned with security and privacy compliance issues in SaaS applications, and to the best of our knowledge, there are relatively few works dealing with the issues of compliance, security and privacy in SaaS applications. What then is security and privacy compliance within the context of SaaS applications? How is compliance assured or verified within the SaaS model of cloud computing given the fact that security and compliance are the responsibility of the application service provider?

Compliance means enforcing rules that implement the policies as provided in regulations and standards. According to [5], compliance is one of the most critical requirements for many software systems, including the cloud. Compliance with regulations such as the GDPR [6] and NDPR [7], is required by governmental bodies like the EU and the Nigerian government. These regulations are mandatory, while industry standards are suggestions. For example, ISO [8] is not mandatory. Security and privacy compliance in the Software as a service model is a shared responsibility among stakeholders [2]; this shared responsibility includes stakeholders such as the service providers and customers or users. However, these days' security and privacy compliance generally indicate the compliance with governmental regulations or industry accepted security standards such as National Institute of Standards and Technology [9] International Standard Organisation 270001 [8] with noncompliance resulting in penalty fees.

Regulations are rules meant to carry out a specific piece of legislation; they are made and maintained by an authority [10] and implemented with the sole intent of protecting the customer's privacy and security such as the GDPR, NDPR and HIPAA. These regulations are unique to their purposes and countries of origin, but according to [11] in many cases, they are similar and designed to achieve local needs. In this research work, we consider the GDPR,

NDPR. These regulations are usually textually crafted for the legal community and are subject to legal and ambiguous interpretations further compounding the challenges of compliance and the verification of compliance. We scrutinized several regulations and standards with impact on our focused area of research.

Standards, on the other hand, are published by organised bodies known as standards defining organisations (SDO's) [11]. Such organisations have a wide variety of internal processes and membership rules, which range from entirely open access to closed formal representation that can in some cases require the approval of national governments and international coordinating bodies [12]. An example is the Cloud Security Alliance [2], which is a non-profit organisation trying to promote security assurance in the cloud. Standards are a means to achieving interoperability and compliance. There is then a need for checking compliance to security and privacy to assist organisations in the verification of compliance when they implement or adopt software as a service into their operations. However, we have found that there is a lack of a compliance framework or compliance tool for SaaS implementations, especially in the Oil and gas industry.

Compliance automation [6], or automated compliance is a software application and technology used to simplify compliance procedures. Security specialists have generated security compliance or auditing of information manually. This involves manual data collection and assessment, which is slow and expensive. To achieve compliance, Reference [13] identified SaaS security and privacy issues and challenges. Reference [11] identified security features that are common for International Standard Organisation [8], Health Information PAA [14], and PCI DSS [6] Reference [15] discussed the CCM. They concluded that implementing compliance guidelines for CCM regulation could cover compliance for security and privacy in SaaS applications. Reference [16] developed a methodology for mapping cloud controls to key industry frameworks like NIST [1], to reduce compliance fatigue and challenges in the cloud services, including SaaS applications. This is necessary as organisations use independent third-party certifying agencies and manual processes to assure compliance, security, and privacy. However, despite the importance of security and privacy and its compliance in SaaS applications, as argued above, there are not many specific surveys on security and privacy compliance in SaaS applications. Therefore, the contribution of this paper is to identify and review papers on security and privacy compliance in SaaS applications. We surveyed some security and privacy compliance efforts. We also discussed the issues raised and provided a guide on how security and privacy compliance in SaaS applications can be addressed.

Section 2 describes some background about regulations, standards, frameworks, and compliance within the context of SaaS applications. We surveyed several security issues in Section 3; we went on to survey compliance issues in Section 4. In Section 5, we discussed current security and privacy compliance approaches. Section 6 summarises compliance, security and issues and provided recommendations and end with some conclusions and future research directions in Section 7.

Background
In this section, we describe the background of cloud computing, software-as-a-service (SaaS), regulations, standards, and compliance framework.

Regulations
Here, we summarise below some of the relevant regulations currently in force and with impact on Software-as-a-Service. These regulations have different jurisdictions, but they do have a significant global impact on organisations.

The Nigerian Data Protection Regulation
The Nigerian data protection regulation (2019) [7] came into effect in April of this year. The objective of the regulation is the safeguard the rights of natural persons to data privacy, the conduct of safe of transactions involving the exchange of personal data, and the prevention of the manipulation of personal data.

General Data Protection Regulation
The GDPR aims to protect all EU citizens from privacy and data breaches in an increasingly data-driven world. It is arguably the most significant change as the GDPR applies to all companies processing the personal data of European data subjects, regardless of where the company's operational location. This is not the case previously; territorial applicability of the directive was ambiguous and referred to the data process in the context of an establishment. Organisations can be fined up to 4% of annual global turnover under the GDPR, [6]. Examples of SaaS applications like human resource applications and sales applications collect personal data and personally identifiable information, which will require compliance with GDPR. Failure of SaaS application providers or users to ensure compliance may lead to penalties as stipulated in the regulation.

Sarbanes-Oxley Act (Sox)
The Sarbanes-Oxley Act (SOX) came into force in July 2002; all U.S. corporations are required to be [17] SOX compliant The Sarbanes-Oxley Act (SOX) establishes standards for all US publicly traded companies the public from accounting errors and fraudulent practices. If these companies or organisations use SaaS applications, which will have their data stored externally, they will require a mechanism for assurance that their data is secure. Thus, reinforcing the need for compliance verification tools.

Health Insurance Portability and Accountability Act
Under the HIPAA regulation, all Healthcare organisations in the US are required to comply with the (HIPAA). The objective of HIPAA is to ensure the security and privacy of health data [18]. The impact of HIPAA on SaaS applications is widespread, and many SaaS solutions have been developed with a focus on the areas of adult care, assisted living and general healthcare delivery such as the NHS. These solutions will have to comply with the HIPAA to protect and guarantees the privacy of an individual's health data.

Standards

ISO/IEC 27000

Information technology (IT) controls are reusable system requirements that IT managers, use to demonstrate compliance with international standards, such as ISO 27000 standard [8]. These controls are reusable; they tend to cover best practices independently from what specific government laws may require.These standards are used in service sectors such as healthcare, finance, retail, communication, energy, education, and government agencies. The ISO 27001 certification demonstrates that SaaS applications service providers have an array of the full spectrum of security best practices in place.

Payment Card Industry /Data Security Standard

The United Kingdom cards association describes the PCI DSS as the worldwide Payment Card Industry Data Security Standard. This was set up to help businesses process card payments securely and reduce card fraud [6]. The policy guideline is designed for organisations handling consumer's payment card data. The policy is available only in textual format and requires significant manual effort to ensure their compliance. The PCI DSS has a significant impact on SaaS applications in with applications, particularly in the areas of retail and payment services.

Frameworks

Control Objectives for Information and Related Technology

Information Technology Governance, IT Governance or ICT Governance, is a subset discipline of Corporate Governance. It is a standard that provides IT governance and control. It attempts to ensure the integrity of information and information systems by providing technical guidelines for compliance, governance, audit, and risk management [17]

Cloud Control Matrix

According to [2], the cloud control matrix (CCM) serves as a tool to help meet security and privacy compliance requirements. It achieves that by listing cloud security controls and maps them to multiple standards. The matrix can also be used to document security responsibilities. These regulations and standards are used in different sectors such as retail, healthcare, oil and gas, finance and government agencies. The Cloud Control matrix allows for the organisation of requirements of regulations, standards, and relevant industry best practices into controls and controls domain mapped to achieve security and privacy compliance as in the works of [11]

Survey of Security and Privacy issues in SAAS Applications

Research has shown that security and privacy challenges are likely explanations for why organisations are slow in the adoption of SaaS applications [4]. These challenges include data security, network security, data locality or localization, data integrity, data segregation data access, authentication and authorization, data confidentiality, web application security, data breaches, virtualization vulnerability, availability, backup, identity management and sign-on process.

Standardisation, Interoperability and Availability

Majda et al. [19] define Interoperability as a property of a consumer system, whose interfaces are completely understood, to work with another Cloud provider, present or future, with restricted access. Currently, there is no standard interfacing with a Cloud or SaaS application provider, and each provider has its own API's they argued.

They also went on to discuss the availability of data. They argued that it is the responsibility of SaaS service providers to guarantee the availability of data without any interruption. Availability is described as the property of a system being accessible upon demand by an authorised entity. This is enabled by technologies, such as service-oriented architectures (SOA), virtual machines, and other cloud infrastructure, contribute to this trend.

Authentication, Authorisation

As SaaS applications services are hosted outside of the corporate firewall, they are beset with challenges relating to authentication and authorisation issues. These issues raise questions like who should access what resource, when and how and also for how long. Hafizul et al. [20], in their study, have identified some authentication challenges and proposed an enhanced remote user authentication scheme that uses elliptic curve cryptography and identity-based cryptosystem with three-way challenge-response handshake technique. Other authentication solutions include Security Assertions Markup Languages Identity solutions.

Data Security and Backup

Rajeswari et al. [21] in their study described the critical challenges of data security of the cloud-computing era. They argued that the appropriateness and privacy of data stored in the cloud might be compromised due to limited security mechanisms provided to the data owners. They surveyed and analysed each category and compared the strength and weaknesses of each approach. They described data security as one of the significant impediments to SaaS adoption. They went on to survey some different security risks that pose a threat to the cloud and the unique security issues that have emanated due to the nature of service delivery models such as the software as a service.

Data Access, Location, and Segregation Issues

Barona et al. [22] in their study surveyed different security issues and threats, which incorporate data breach, unreliable connectivity, sharing of resources, data accessibility and inside attacks. They asserted that a breach of security might lead to the accidental or unlawful destruction or access to, personal data. They examined primary security threats and data breach issues that are right now exploring to SaaS applications and other cloud models. They further investigated other security issues in SaaS applications such as locality of data, and data segregation.

They argued that the location of data is one of the significant challenges of the software as a service this is because SaaS applications data and the application itself are hosted on the service provider's infrastructure leading to several security challenges. Recently, intergovernmental organisations like the European Union implemented the GDPR requiring

the location of personal data of EU citizens to be hosted within the borders of the EU. This presents a significant compliance challenge to SaaS application providers, users and governments.

They went on to describe data segregation in the context of SaaS applications as a situation where the data of different users will be hosted on the same data infrastructure. They went on to emphasise that, the data of one user, should not affect the data conditions the data of other users of the same application in a multitenant environment. This results in maximum utilisation of hardware resources. In order to avoid both unintended and malicious access to other user's data, SaaS application service providers should ensure separate segregation of data.

Data Confidentiality and Integrity Issue

Data confidentiality and integrity are critical elements in any system. Tiwari et al. [23] in their review described confidentiality, security and privacy as a significant issue for users of SaaS applications due to their dependence on the service provider. They further argued that the SaaS service model provides many features, but adequate security remains a challenge, they went on to describe existing solutions and propose several SaaS security vulnerabilities in the areas of confidentiality, privacy, and security threats. To this effect, they discussed the need for data encryption before it is outsourced. This is to ensure that only encrypted data is transferred to the service provider platform. However, they further discussed that the user or client should be responsible for handling the access control policy, encrypting the data, decrypting it.

Virtualisation, Encryption and Network Security

According to [24], virtualisation is a conceptual process of extracting computing resources and operating system from the hardware on which they are deployed. The Virtual machine and the Virtual Machine Manager are referred to as the components that make up the concept of virtualisation. They are usually represented as an image. According to Reference in their survey, there are many advantages of SaaS as a component of cloud computing. As Virtual Machines (VM's) are hosted on the same physical server, resources are shared by the VMs belonging to multiple users. Thus, providing a situation where VM's hosting SaaS applications can be exploited to gain access over other user's data or deny service. They went on to propose constructive security measures that can be deployed to avoid such attacks

According to [13], the network is a medium to access SaaS services from a cloud system. SaaS service providers must implement strict regulation for data protection from any manipulation, theft and unauthorised access of data.

Survey of Compliance Issues in the SAAS Applications

Compliance typically involves complying or adhering to industry standards, and regulations or laws [5]. For effective service provisioning, Service Level Agreements are used to guarantee the rights of a user, and the obligations of the service provider [25]. SLA's are therefore used in the measurement of service levels provided by the service provider such as availability, response time, Quality of Service, downtime, security and location of data are

part of the SLA [25]. However, challenges of verifying security and privacy compliance remains a significant impediment to SaaS applications adoption [18]. It is against this backdrop that governments and industry enforced several laws and regulations regarding the administration and compliance to security and privacy of data, especially in SaaS applications.

As earlier stated, that in the SaaS model, the client or user depends on the SaaS provider for security [2]. Therefore, based on the principles of shared responsibility, the provider is responsible for keeping multiple users' away from seeing each other's data in a multi-tenant environment. Therefore it becomes difficult for the user to ensure that the right security measures have been implemented and it is difficult to get the assurance that the application will be available when needed.

Regulations, Standards and Law that are used in information technology are different across different countries. This is the case with cloud computing and software as a service. These laws, such as the GDPR [6] and the SOX, are used to govern the use of personal data and storage of data. Correspondingly, adhering to these laws and regulations are required, and failure to adhere attracts a penalty. Thus, becoming a challenge to both the service provider and user. Reference [1], contended that understanding and enforcing regulations are a significant challenge in cloud computing and software as a service. The contributors analysed the challenges of data location, loss of control, and transparency in public compliance. They did not provide means or details on how to enforce these regulations required for security and privacy compliance by automated means. As we explained earlier, organisations enforce these regulations by using manual means and third-party auditing or compliance processes.

Reference [26] conducted a comprehensive study to review the potential threats faced by cloud consumers and have determined the compliance models and security controls that should be in place to manage the risk. They went on developed an ontology describing the cloud security controls, threats and compliances. They developed an application that classifies the security threats faced by cloud users and automatically determines the high-level security and compliance policy controls that must be activated for each threat. Reference [27] analysed the top seven threats and their possible impact on compliance in the cloud by mapping threats to applicable regulations. This mapping was used as a reference for the evaluation of compliance. However, the paper lacks explicit mappings between compliance and security and privacy challenges.

Current Approaches to Security and Privacy Compliance in SAAS

There are different approaches to ensure security and privacy compliance in SaaS. SaaS application service providers such as Amazon, Microsoft, and others claim compliance for HIPAA [18], PCI [6] SOX [17], and GDPR [6]. This is achieved using their proprieties and systems. This sometimes presents an interoperability problem to users of SaaS applications. Another widespread approach in the industry for achieving security and privacy compliance in SaaS applications is the service level agreement. Reference [28] stated that Service level agreements (SLAs) are used to define the quality of the provided services. To support their

argument, they went developed a framework of steps to verify and assure the SLA compliance of Web Services offered across several Cloud providers the framework targets the evaluation of the QoS of the SaaS Web Services.

The last approach to security and privacy compliance we considered in this work is the automation of regulations and standards for effective compliance. Reference [29] developed an approach that enables cloud-computing clients to verify health regulatory compliance claimed by cloud computing providers. The approach allows clients of cloud computing to check automatically how the cloud provider meets regulatory compliance, such as HIPAA legislation for their health records. Reference [30] discussed the advantages of automating information security policies for expressing the high-level objectives of security compliance of enterprise SaaS applications and presented a novel idea of checking compliance from the log records. Compliance in the cloud is based on the concept of shared responsibility among service providers and consumers [2]. This responsibility is different across the different cloud computing models. For the sake of this research work, we considered what shared responsibility mean in the context of the SaaS model. Here, consumers are responsible for securing data, while service providers are responsible for securing services. In general, the lack of full control and transparency creates compliance challenges in the cloud. In summary, most service providers have published compliance designs, and implementations based on their proprietary cloud platforms, infrastructures, and products. The available offerings are vendor specific or do not follow standard models, patterns or architectures as a result; therefore, challenging to examine the level and scope of compliance.

Summary of Security and Privacy Compliance Issues and Recommendations
Security and Privacy Challenges
SaaS applications like all IT platforms are subjected to a variety of security and privacy challenges. This is also compounded by the nature of security and privacy responsibilities of service providers and users as the client or user depends on the SaaS provider for security. Therefore it becomes difficult for the user to ensure that the right security and privacy measures have been implemented proposed how SaaS vendors must ensure that critical aspects are covered across layers in order to ensure the security of data. Other issues such as Standardization and Interoperability authentication and authorisation; The locality of data., Multitenancy and data segregation data access, data availability data confidentiality for ensuring data integrity in the cloud and SaaS applications, network security issues, and virtualisation and encryption, which are major security and privacy challenges were analysed.

In general, compliance involves adherence to established standards, regulations or laws. The prevailing situation is; cloud service providers or SaaS application providers guarantee compliance to these regulations via service level agreements. Nonetheless, users and organisations still need to be ultimately responsible for assuring their data security and integrity based on the principle of shared responsibility [2]. Some of the compliance challenges discussed earlier are Regulations and laws. The regulations and laws have different jurisdictions but broader implications such as the GDPR and NDPR. Nonetheless, these challenges to compliance regulations, standards and laws continue to remain concerns for the security and privacy of SaaS applications.

Regulations Complexity
Regulations are drafted usually by legal professionals and challenging to interpret by people outside the legal profession [18]. There are situations where the regulations are not consistent and with different jurisdictions. Significant effort has been made by some researchers to simplify these regulations using citation graphs, reference architectures and policy languages.

To help harmonise these standards and regulations, the cloud security alliance developed a framework [2] that took into account all standards since 2006 and coming up with a matrix called the Cloud Control Matrix [11], mapping the existing frameworks through a list of detailed cloud assurance controls. This bridged the gap between industry and government standards by offering a framework of consolidated standards. There still several efforts aimed at improving the assessments of security and privacy in SaaS applications and the cloud.

Lack of Control, Sovereignty and Jurisdiction
The cloud provides minimal and inflexible means for customers to control their data, for example, customers cannot comply with laws requiring data to be kept in the originating jurisdiction, nor control sharing of data with third parties. This lack of control can hinder SaaS adoption for data that falls under regulations. Policy languages have been proposed on how SaaS applications can be enriched with policy language support to empower customers or users have control over cloud data.

Overlapping Standards
Regulations as promulgated by governments, governmental bodies, agencies and industry associations often overlap and create more challenges of compliance to organisations. These regulations such as GDPR, NDPR, HIPAA, SOX, PCI DSS tend to have similar provisions but with different purposes and enforcement authorities. To help address the challenges of compliance with various regulations, [2] have designed the cloud control matrix to help map the provisions of these regulations and standards for ease of the compliance process.

Conclusions and Future Directions
In this survey, we critically analysed the existing literature on security and privacy compliance by exploring relevant publications and several approaches to security and privacy compliance in SaaS applications. We have also discussed the complexities of regulations and standards and discussed situations where they overlap; we have also discussed several efforts aimed at harmonising and mapping of several regulations into controls for ease of compliance by industry bodies. A handful of security and privacy compliance challenges can be addressed using standard compliance models, architectures and best practices to regulations and standards [18]. Additionally, there have been a handful of attempts at tackling these challenges to security and privacy compliance in the context of SaaS applications. However, to the best of our knowledge, there has been no attempt to automate specific controls mapped to regulations and standards based on the Cloud Control Matrix controls specifically for the retail sector of the oil and gas industry. This kind of compliance approach, we believe could improve security and privacy compliance of SaaS applications and the overall quality and adoption of the rate of SaaS applications within the industry.

Our proposed SaaS security and privacy compliance framework will be able to help users and organisations verify compliance using the API's of the SaaS application service providers. The framework will focus on the oil and gas industry requirements and will be cloud-based. The framework will be developed using a combination of intelligent cloud-based tools and a policy language that can dynamically collect data from the SaaS application service provider's API. The proposed security and privacy compliance framework will help to deepen the adoption of SaaS business application in the retail sector of the oil and gas industry. Furthermore, the framework will further increase the trust in the Security and privacy measures of SaaS applications and Cloud Service Providers.

The proposed SaaS security and privacy compliance framework differ in many ways with existing automated frameworks as it seeks to automate compliance to security and privacy controls using the cloud control matrix with a specific focus on the retail sector of the oil and gas industry using a security and privacy policy language. This will contribute modestly to the development of the oil and gas industry. This work further provides a new methodology that will allow researchers and designers to study security and privacy in cloud computing in the context of SaaS with improved efficiency for compliance in security and privacy assurance, in an enterprise context like retailing, in the Nigerian Oil and gas industry.

Acknowledgement
This paper has received funding from the Petroleum Technology Development Fund of the Federal Republic of Nigeria. The authors would like to further thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. They are also grateful to Dr Daniel Fitton for his valuable guidance.

References

[1] (2011). *NIST Security and Privacy Guide in Cloud Computing*, Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

[2] CSA, Security guidance guidance v4.0," Cloud Security Alliance, 2017.

[3] (2018). *Gartner forecasts worldwide public cloud revenue to Grow 17.3 Percent in 2019*, Available: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.

[4] Harikrishna, P. & Amuthan, A., "A survey of testing as a service in cloud computing," in *2016 International Conference on Computer Communication and Informatics (ICCCI),* 2016, pp. 1-5.

[5] Massey, A. K. *et al*, "Assessing the accuracy of legal implementation readiness decisions," in *2011 IEEE 19th International Requirements Engineering Conference,* 2011, 207-216.

[6] Elluri, L., Nagar, A. & Joshi, K. P., (2018). An integrated knowledge graph to automate GDPR and PCI DSS compliance," in *2018 IEEE International Conference on Big Data (Big Data),* 1266-1271.

[7] (2019). *The Nigerian data protection regulation, 2019*. Available: https://nitda.gov.ng/wp-content/.../Nigeria%20Data%20Protection%20Regulation.pdf.

[8] (2019). *ISO 27001, the international information security standard*, Available: https://www.itgovernance.co.uk/iso27001.

[9] National Institute of Standard and Technology -USA, (2011). *The NIST definition of cloud computing*,"

[10] Kshetri, N. & Murugesan, S., (2013). Cloud computing and EU data privacy regulations," *Computer*46, *(3),* 86-89,

[11] Giulio,C. D. *et al*, "Cloud standards in comparison: Are new security frameworks improving cloud security?" in *2017 IEEE 10th International Conference on Cloud Computing (CLOUD),* 2017, 50-57.

[12] Murugesan, S. & Bojanova, I., (2016). Community clouds," in *Encyclopedia of Cloud Computing* Anonymous Wiley-IEEE Press,744.

[13] Chouhan, P. K., Yao, F. & Sezer, S. (2015). Software as a service: Understanding security issues," in *Science and Information Conference (SAI),* 162-170.

[14] (). *Health Information Privacy*.

[15] Sultan, W. A. A, (2016). *Data security, privacy*, Availability and Integrity in Cloud Computing: Issues and Current Solution, 7*(4),* 485-498,

[16] (2018). *Methodology for the mapping of the cloud controls matrix*. Available: https://blog.cloudsecurityalliance.org/2018/07/09/methodology-for-mapping-the-cloud-controls-matrix/.

[17] Kim, N. *et al*, "SOX act and IT security governance, (*2008) International Symposium on Ubiquitous Multimedia Computing,* 218-221.

[18] Yimam, D. & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing, *Journal of Internet Services and Applications,* 7, *(1),*5, May.

[19] E. Majda & E. Ahmed (2015). Using cloud SaaS to ensure interoperability and standardization in heterogeneous cloud-based environment," in *2015 5th World Congress on Information and Communication Technologies (WICT),* 29-34.

[20] Islam, S. H. & Biswas, G. P. (2011). A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, *Journal of Systems and Software,* 84, *(11),* 1892-1898. DOI: https://doi.org/10.1016/j.jss.2011.06.061.

[21] Rajeswari, S. & Kalaiselvi, R., (2017). Survey of data and storage security in cloud computing," in *2017 IEEE International Conference on Circuits and Systems (ICCS),* 76-81.

[22] Barona, R. & Anita, E. A. M., (2017). A survey on data breach challenges in cloud computing security: Issues and threats, *International Conference on Circuit, Power and Computing Technologies (ICCPCT),* 1-8.

[23] Tiwari, P. K. & Joshi, S., (2014). A review of data security and privacy issues over SaaS," in *2014 IEEE International Conference on Computational Intelligence and Computing Research,* , pp. 1-6.

[24] Singh, A. & Chatterjee, K. (2017). Cloud security issues and challenges: A survey, *Journal of Network and Computer Applications,* 79, 88-115, DOI: https://doi.org/10.1016/j.jnca.2016.11.027.

[25] Trapero R. *et al*, (2017). A novel approach to manage cloud security SLA incidents, *Future Generation Computer Systems,* 72, 193-205. DOI: https://doi.org/10.1016/j.future.2016.06.004.

[26] Hendre, A. & Joshi, K. P. (2015). A semantic approach to cloud security and compliance," in *2015 IEEE 8th International Conference on Cloud Computing,* 1081-1084.

[27] Mirković, O. (2008). Security - How to Measure Compliance,".

[28] Ibrahim, A. A. Z. A., Varrette, S. & Bouvry, P. (2018). On verifying and assuring the cloud SLA by evaluating the performance of SaaS web services across multi-cloud providers," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W),* 69-70.

[29] Khan, K. M. & Yun, B. (2013). Automatic verification of health regulatory compliance in cloud computing," in *2013 IEEE 15th International Conference on E-Health Networking, Applications and Services (Healthcom 2013),* 719-721.

[30] Mandal, D. & Mazumdar, C. (2018). Automating information security policy compliance checking," in *2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT),* 1-4.