A survey on resolving security issues in SaaS through software defined networks

Gopal K. Shyam*

School of Computing and Information Technology,
REVA University,
Bengaluru 560064, Karnataka, India
Email: gopalkrishnashyam@reva.edu.in
*Corresponding author

Reddy Sai Sindhu Theja

School of Computing and Information Technology,
REVA University,
Bengaluru 560064, Karnataka, India
and
Department of Computer Science and Engineering (CSE),
Sreenidhi Institute of Science and Technology (SNIST),
Ghatkesar, Hyderabad 501301, Telangana, India
Email: thejasindhu@gmail.com

Abstract: The key ingredient in the success of Software-as-a-Service (SaaS) is based upon the client's satisfaction. Sensitive data acquired from the organisations are processed by the SaaS applications and stored at the SaaS provider end. All data flow over the network needs to be secured to avoid leakage of sensitive data. However, upon preliminary investigation, security is found to be the foremost issue that hampers the growth of confidence in the entrepreneurs for data deployment. This paper mainly focuses on different security issues in SaaS. Further, we analyse the security issues derived from the use of Software Defined Networking (SDN) and elaborate on how it helps to improve security in SaaS. Additionally, comparisons between current solutions and SDN solutions are made. Hence, this work aims at giving new directions to the researchers, specifically in the domain of SaaS, in understanding security issues and planning possible countermeasures.

Keywords: software-as-a-service; security issues; attacks; software defined networking.

Reference to this paper should be made as follows: Shyam, G.K. and Theja, R.S.S. (2021) 'A survey on resolving security issues in SaaS through software defined networks', *Int. J. Grid and Utility Computing*, Vol. 12, No. 1, pp.1–14.

Biographical notes: Gopal K. Shyam is a Professor in School of Computing and IT at REVA university. He has received his BE, MTech and PhD degrees in Computer Science and Engineering from VTU, Belagavi. He has handled several subjects for UG/PG Students like Algorithms, Computer Networks, web programming, Advanced Computer architecture, Information security, Computer Concepts and C Programming. His research interest includes cloud computing, grid computing, high performance computing etc. He has published about 10 papers in highly reputed National/International Conferences like IEEE, Elsevier etc. and 5 papers in Journals with high impact factor like *JNCA* and *IJCC*.

Reddy Sai Sindhu Theja received her BTech degree from MRR Institute of Science and Technology, JNTU Hyderabad and MTech degree from KL University, Vijayawada and pursuing PhD degree under the guidance of Dr. Gopal K. Shyam at REVA University, School of Computing & IT Bangaluru, India. Her research interests include cloud computing, machine learning etc. She is working as an Assistant Professor at Sreenidhi Institute of Science and Technology, Hyderabad, India. She has handled several subjects for UG/PG students like Database Management Systems, Mathematical foundations of Computer Science, Object Oriented programming through Java, Software Project Management, Real-Time Operating Systems and Cloud Computing.

1 Introduction

Cloud is a kind of large-scale distributed economy-driven computing model which has turned into today's most prominent research area due to its ability to trim down the costs related to computing (Kaur and Singh, 2015; Weihua and Shibing, 2013). It provides three service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service and (PaaS), and Software-as-a-Service (SaaS) which offer infrastructure resources, application platform, and software services, respectively. SaaS has received noteworthy responsiveness as it deals with applications that run on top of a PaaS, which in turn runs on top of IaaS (Tsai et al., 2014; Subashini and Kavitha, 2011). So, there is a chance of features inherited by SaaS from PaaS and IaaS, and risks too. Owing the several advantages of cloud like less management burden, no maintenance, easy access, and flexibility, it is becoming a popular platform for SaaS. The main initiative of this work is to provide security for SaaS customers (Rath et al., 2019). SaaS applications are usually under the control of end-users, which offers an increased level of security and control functionality (Aime et al., 2011).

The upgrades made by SaaS providers are readily available to their customers instead of buying and installing them. The SaaS paradigm provides two types of connectivity to the end-users. They are web-based connectivity and Application Programming Interface (API) (Deshpande et al., 2018). In spite of all the excitement surrounding the SaaS, enterprise customers are still unwilling to set up their business in it due to lack of security. The SaaS community is in a great need for best security practices, to help in designing and developing secure SaaS application. Moreover, the focus on security aspect is restricted to some specific areas like how to eliminate cyber attacks and how to develop secure code, but does not cover many aspects such as compliance regulations, governance and privacy (Rath et al., 2019).

Customers and providers are the two different actors in SaaS, in which single or multiple customers use the services offered by the service provider. For example, organisations with different employees access the software with divergent privileges. Even though SaaS is a massive piece of software to the user, in reality, it can be put into practice with multi-provider architecture (Song et al., 2019). The provider can make use of resources from other parties like getting hardware resources from third parties, or provider can host resources with their own data centre. This kind of multi-tenant architecture of SaaS leads to security issues like Denial of Service (DoS) attacks, Quality of Service (QoS), Multi-step attack, Insider attack, etc.

SaaS services are offered by providers who may use third-party (sub-provider) services as a part of their supply chain. Tenants make an agreement with the provider to get a cloud service, which they use to host applications and services for their users. Therefore, in relation to the security of SaaS service, the following relationships must be considered which leads to threats: (i) the communication between the customer and the provider, (ii) the cross communications among various customers of the same vendor, (iii) communications among the SaaS provider and sub-providers, and (iv) third-party invaders targeting any component of the SaaS service. Third-party invaders are the attackers who will attack the system and make the resources unavailable for the users. Data flows usually equivalent to these relationships. The Cloud Service Provider (CSP) has maximum control over the SaaS and therefore customer has minimum control over security, as the executing platform lies outside the network of the user (Anjana and Singh, 2019).

As the SaaS adoption rate increases, many critical issues arise with respect to security (Elsayed and Zulkernine, 2019) should be addressed. From the provider's point of view, how is it possible for a provider to protect the security of SaaS application from the unauthorised customer requirements. From the customer's point of view, how is it possible for a customer to check the integrity and confidentiality of their information that run through a SaaS application and how can he trust the security of such application which is hosted by third parties.

The existing research focuses on addressing the security for non-dynamic situations such as: (i) the provider not being able to communicate with all the neighbours due to the failures or the time constraints, (ii) the service may not be accessible in situations where communication is unavailable or very expensive, (iii) the resources that are available may join the network and leave unexpectedly leading to various complexities, (iv) non-usage of previously recorded data to improve the decision of prospective data to be sent. This has now turned as a bottleneck for cloud operators in scaling their networks. There is a need to address the security concerns dynamically, and the SDN makes it possible to address the dynamic network management concerns that provide possible management to the entire network through granular network control, intelligent orchestration and provisioning (Ketel, 2018).

SDN has emerged from the service focused requirements. SDN is a network paradigm where the decoupled data and control planes allow the abstracted network infrastructure for applications as well as services (Lai et al., 2016). It provides a centralised controller through which the network is centrally managed and facilitates automated network management. This feature helps the administrators to quickly adapt the network resources and network-wide traffic resources, which are adjusted dynamically to meet the changing needs in SaaS (Sivaraman et al., 2013). For instance, bandwidth can be allocated at runtime into the data plane from the application (Sezer et al., 2013). The most up to date progress in high performance switching of SDN could potentially be a striking resolution for the network level issues in cloud (Park et al., 2019). This paves the way for power management, network-wide access control, home networking, etc through SDN.

All the enterprises and operators are turning to SDN because of its programmable networks, intelligence and control centralised, network interaction through APIs, vendor neutral architectures. SDN is designed to work with complex networks and makes them effortlessly manageable and is centrally run. Therefore, it does not matter how complex the network is (https://www.ciena.com/insights/why/Why-SDN.htmlbusinness). Also, the network programmability in SDN makes the network aware of the applications. SDN provides a fast, effective, and a consistent centralised point of control to give out security decisions and policy updates, and can automate user access control (Oktian

et al., 2018), which would enable the use of resources in time, and for this reason, SDN is used as a reasonable direction in this paper.

Our work has the following contributions: (i) categorising the security issues of SaaS into multiple levels (ii) mapping of security issues and their respective attacks regarding SaaS (iii) SDN in SaaS security handling (iv) comparative analysis of SDN and non-SDN in handling security.

This paper constitutes the following sections. Section 2 includes security issues of the SaaS layer. Section 3 consists of a comparison of existing solutions with non-SDN techniques and SDN techniques, and the efficiency is estimated. Section 4 contains the challenges of SDN. Section 5 covers the conclusion and throws light on future work.

2 Security issues in SaaS delivery model

SaaS has received noteworthy responses in the recent times as one amongst the foremost components of cloud computing. SaaS flushes out the complexities of software procurement procedure in the direction of charging services as an alternative to procurement and their basic infrastructure. As an outcome, tenants can accumulate infrastructure expenses, software permits, system administration, and development staff. Residents can toggle towards a choice of various service providers.

The SaaS paradigm allows service vendors to aim at small and average enterprise markets by exposing them to a software adoption cost model with a reasonable budget (Almorsy et al., 2014). But in SaaS, for proper security measures, the customer has to depend on the provider. The provider ought to do the job to maintain various customers from considering each other's data. Consequently, this turns out challenging to the customer to guarantee the exact security measures and to acquire the assurance that the application will offer when required.

Some of the level-wise security issues which reflect the crucial elements of SaaS application improvement and utilisation process are discussed in Table 1. SaaS allows providing software as a service to the users through internet. At this instance, security must be provided in order to maintain true customer relationship management. The probability of the occurrence of security issues at different levels are application level, data security level, deployment level, network level, virtualisation level and cyber security level. Attack vector is a means through which an attacker gains access to a network to penetrate the target system. The attack vectors that fall under the category of each level of security issues are provided. Subsequently different types of attacks associated with attack vectors and possible solutions are given based on the existing works.

Table 1 Level-wise security issues of SaaS

Security issues	*Attack vectors*	*Attack types*	*Solutions*
Application level security issues (Choudhury et al., 2011; Batyuk et al., 2011; Sahs and Khan, 2012; Doroodchi et al., 2009; Stephanow and Khajehmoogahi, 2017; Hashizume et al., 2013	(i) Web application security, (ii) Authentication and authorisation (IBM Developer Community, 2018), (iii) Security misconfiguration and (iv) Identity management and sign-on-process (Rashmi et al., 2013).	(i) SQL injection threats, (ii) cross site scripting and (iii) session hijacking	(i) Mutual authentication with session key establishment and identity management, (ii) Deploy static malware detection techniques, to manage the specific issues and problems of web service, (iii) A wide range of XML security standards are applied.
Data security level security issues (Barona et al., 2017; Rewagad and Pawar, 2013; Ranjan et al., 2014)	(i) Data access control, (ii) Data breaches, (iii) Data availability (Rocha et al., 2017), privacy (Symantec (2018) and confidentiality, (iv) Data integrity (Zissis and Lekkas, 2012), (v) Data locality (Choo, 2014), (vi) Data backup and recovery, and (vii) Data segregation.	(i) Weak and stolen credentials, (ii) improper configurations, (iii) unauthorised access and (iv) wrong entry of data into database.	(i) Implement cryptographic techniques and (ii) Homomorphic encryption technique
Deployment level security issues (Fernandez et al., 2016; Kari, 2014; Chouhan et al., 2014; Wu et al., 2010; Pearce et al., 2013)	Virtual network security	(i) Software interruption and manipulation, (ii) data mobility will be difficult, (iii) lack of connectivity requirement, and (iv) easy upgrades of programming flaws.	(i) Implementing diverse platform hardening methods, (ii) Features of bridge and route virtual networking style should be strengthened, (iii) Using malware detection techniques in virtualised environments

Table 1 Level-wise security issues of SaaS (continued)

Security issues	*Attack vectors*	*Attack types*	*Solutions*
Network level security issues (Shin et al., 2016; Seeber and Rodosek, 2014; Kao et al., 2018; Satam et al., 2015; Ghosh et al., 2017)	(i) Insecure SSL trust configuration, (ii) Network penetration and packet analysis, (iii) Session management weakness	(i) Network sniffing, (ii) reuse of IP address, (iii) DNS attacks, (iv) phishing attacks	(i) SDN-based information centric cloud framework, (ii) Anomaly-based intrusion (IDS) for the DNS protocol (DNS IDS), (iii) Real-time evidence gathering as a network characteristic next to invaders
Virtualisation level security issues (Paikrao and Pati, Zhu et al., 2017; 2018; AbdElRahem et al., 2016; Sumitra, B. and Misbahuddin, 2013; Sabahi, 2011; Dewangan et al., 2016; Singh and Pandey, 2013)	(i) Storage vulnerabilities, (ii) Network vulnerabilities and (iii) VM vulnerabilities	(i) DoS and DDoS attacks, (ii) Hypervisor root kit, (iii) VM Hopping, (iv) VM Escape, (v) VM Mobility, (vi) VM Sprawl, (vii) VM Stall and (viii) VM Hijack	(i) Symbolic execution techniques and detection framework which detects bugs in virtualisation implementations (ii) SecVirtuality as a service model for virtualisation vulnerabilities
Cyber security level security issues (Prinzlau, 2017; Surianarayanan and Santhanam, 2012; Gupta et al., 2016)	Regulatory compliance (Yimam and Fernandez, 2016; Brandall, 2018)	(i) Sales tax and nexus: Physical presence is most important otherwise need to pay penalty (ii) Provider focused auditing: Even before the legal audits occur provider would be audited by client. (iii) Legally mandated data protections. (iv) General data practices	(i) Provision of unauthorised firewalls, secure APIs and access, taking frequent backups, availability, provision of log files etc. (ii) Encryption of data at both import and export level. (iii) Having knowledge about the legal obligations, (iv) Performs an evaluation on external threats and must be authorised at suitable security level.

SaaS is built with multi-tenant architecture in which multiple users share the same services across the cloud. In the backdrop of SaaS security services, few interactions among users are mainly considered (i) cross questioning, (ii) discussion among the customers of same provider and same user, (iii) provider interactions, (iv) interactions among SaaS supplier and sub-suppliers and (v) the external invaders targeting any component of the SaaS service (Aime et al., 2011).

The security issues regarding SaaS and their respective attacks are presented in Table 2 where Y indicates that the security issue has been associated with the respective attack and N indicates its disassociation with the attack. The basis for indicating Y or N is by exhaustive study from the reference papers and the analysis of attacks covered in them. For instance, authentication and authorisation issue is observed for attacks such as: weak access control (Indu et al., 2018), DoS attacks (Deshmukha and Devadkar, 2015), unauthorised access (Mehta and Saini, 2016) and insider attack (Miltiadis et al., 2013) and is not an issue for attacks such as Multi-step, SQL injections. Another contribution worth mentioning here is network security issue, and it is observed for the attacks such as: multi-step, DoS attack, unauthorised access, SQL injections and is not an issue for the attacks such as weak access control and insider attack. Similarly, other issues and their respective attacks were provided.

Table 2 Security issues and respective attacks in SaaS (Y: Yes, N: No)

Security Issues	*Attacks*					
	Multi-step attack (Zimba and Chama, 2018)	*Weak access control (Indu et al., 2018)*	*DOS (Deshmukha and Devadkar, 2015)*	*Unauthorised access (Mehta and Saini, 2016)*	*Insider attack (Miltiadis et al., 2013)*	*SQL injections (Yassin et al., 2017)*
Authentication and authorisation	N	Y	Y	Y	Y	N
Availability and backup	Y	N	N	Y	Y	Y
Confidentiality	Y	Y	N	N	Y	Y
Data access	N	N	Y	Y	N	N

Table 2 Security issues and respective attacks in SaaS (Y: Yes, N: No) (continued)

Security Issues	*Attacks*					
	Multi-step attack (Zimba and Chama, 2018)	*Weak access control (Indu et al., 2018)*	*DOS (Deshmukha and Devadkar, 2015)*	*Unauthorised access (Mehta and Saini, 2016)*	*Insider attack (Miltiadis et al., 2013)*	*SQL injections (Yassin et al., 2017)*
Data breaches	N	Y	N	N	N	N
Data integrity	Y	N	N	Y	Y	Y
Data locality	N	N	N	N	N	N
Data privacy	N	N	N	Y	N	N
Data security	Y	N	Y	Y	N	Y
Data segregation	N	Y	N	N	N	N
Identity management	N	Y	Y	N	Y	N
Network security	Y	N	Y	Y	N	Y
Regulatory compliance	N	Y	N	N	Y	N
Virtualisation vulnerability	Y	N	Y	N	N	N
Web application security	Y	N	Y	N	N	Y

3 SDN versus non-SDN techniques in SaaS security handling

3.1 SDN in SaaS security handling

To provide an effective SaaS application, a customer relationship should be maintained securely. Large organisations with multiple branches, along with their clients who need to access cloud-based SaaS applications time to time (and where they choose not to incur transport and response time costs to backhaul this application), generally prefer to use lower cost internet connections. A service provider may alternatively meet such need with cloud-based solution wherein virtual network services combined with SDN could be flexibly deployed, self-provisioned and also managed centrally in the cloud. Using this option, the enterprise obtains reliable, low cost and quick access to SaaS applications via internet. This paradigm plans to simplify the networks and allow the progress through the programmability of networks (Dong et al., 2019). Further, the service provider would be able to deliver better and varied value added services.

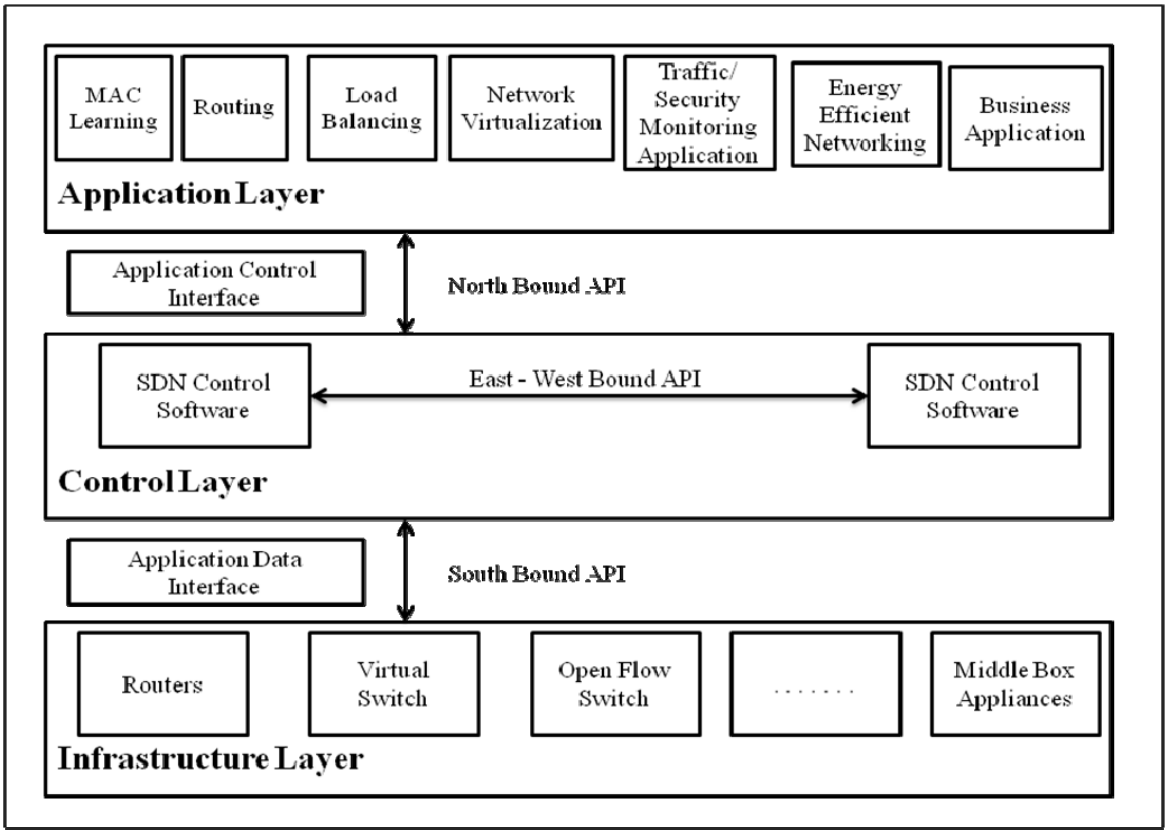
SDN is an unmarked technique to cloud computing, which uses open protocols like the OpenFlow and enables efficient network configuration to improve network scrutinising and performance. Security of a cloud environment is always a goal intended for enemies to take advantage of any of the system's vulnerabilities (El Moussaid et al., 2017). SDN turns out to be incredible architecture for the administration of large-scale and complex networks which may need reconfigurations continuously, and the network design with decoupled control and data planes (Cisco Inc., 2013; Hu et al., 2014). SDN is a network prototype, typically demonstrated by three primary features:

- A picture-perfect partition of data and control planes that offer enormous benefits, like trouble-free management, more programmability, and improved features like dynamic management of virtual networks.
- The network logic is abstracted from hardware into software implementation. It enables increased utilisation of resources and unlocks the potential for the latest applications in which the expenditure plans can be stated depending upon on a level of service providing.
- The presence of a network controller coordinates network devices by making forwarding decisions. Once the latest flow of packet arrives from the sender, the switch verifies for a flow rule. If an identical entry is found in the flow table, then the packet is forwarded to the receiver. If it does not match, the packet may be sent to the controller, which adds the latest forwarding entry to the flow table. Then, the switch forwards the packet to the receiver in a suitable port.

SDN provides network API to the application programmers. Hence, a centralised controller is used to maximise the reliability of the network, dynamic management, unified policy enforcement, minimising of configuration errors, and allows network in a simple and expedient environment, which is traffic-free.

Figure 1 shows the SDN architecture (Patel et al., 2016) with three layers, namely infrastructure, control, and application layers, with decoupled control and data planes.

Figure 1 SDN architecture



In the context of handling higher density, virtual machines transform the resources from time to time dynamically, where the conventional networks are inefficient. To defeat the limitations of historical networks, the cloud data centres initiated adopting SDN along with their Data Centre Network (Son and Buyya, 2017). Some of the cloud providers (e.g., Google (Vahdat et al., 2013)) have already adopted SDN, which provides a centralised controller, network-wide control, and visibility and a straight control over the traffic to increase their scalability and manageability. CloudSimSDN was introduced in Son et al. (2015), which activate the simulation of strategies for joint allotment of network resources. It is a novel simulation tool that is built upon the apex of CloudSim, where assets are dynamically supervised as well as configured in a data centre through a centralised controller.

Along with this feature, De Souza et al. (2017) launched a novel VM selection technique that judges not only a geographical location of the existing region but also the end-to-end latency prerequisite of the VMs. Though there is appropriate control logic in SDN, the heavy traffic can be circulated dynamically, which finally cuts the result of the gridlock (Cui et al., 2016). SDN makes batch processing possible with the excellent functioning of its network controller. Strong network management is provided with SDN, provides cloud abstraction and guarantees content delivery. It monitors attackers on the data plane. Software Defined Privacy is provided in Kemmer et al. (2016).

Table 3 defines the security issues addressed by SDN in SaaS. In Akhunzada et al. (2015), routing, authentication, data security and network security are dealt with SDN, with a distributed ad-hoc control plane. In Flauzac et al. (2015), with the support of data integrity functionalities and the digital signatures of SDN, the authorisation and data manipulations are controlled. From Sivaraman et al. (2013), virtualisation is attained. Similarly, from Ghosh et al. (2017), Patel et al. (2016), and Modarresi et al. (2017) the issues that are mentioned are minimised by the usage of SDN. Network security is one of the foremost issues in SaaS Security handling. Packet analysis and network penetration are the two major problems with it. Packet monitoring switches can be used for making the packet move in the correct direction. But this would be very expensive to implement in the cloud. The establishment of a packet monitoring scheme is one of the primary uses of SDN. It uses the network switches of low cost with an SDN controller, to permit for dynamic and straightforward configuration of a packet monitoring as well as analysis of the system.

SDN traceroute (Agarwal et al., 2014) is a tool for finding path of the network flow in SDN-enabled networks. By using the tangible forwarding mechanisms, the path is traced at each SDN-enabled device with no manipulation of forwarding rules that are being calculated, which grants the administrator to decide the forwarding performance of Ethernet packets. SDN traceroute crafts the smallest token of hypothesis regarding the exactness of controllers and switches. Still, as a substitute, it measures the actual forwarding performance of the network with a minimal amount of high-priority regulations to snare and inject the packet again at each step.

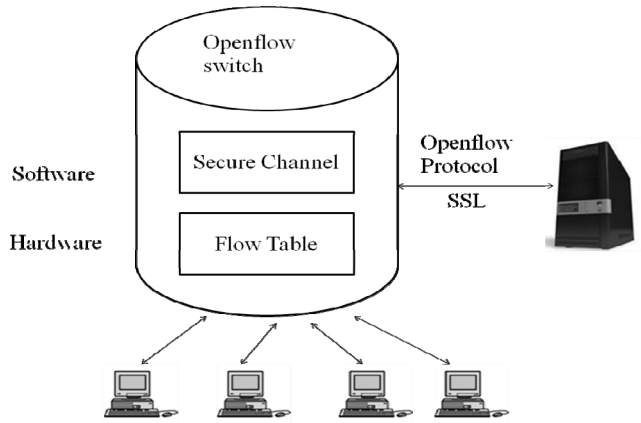
Table 3 SDN technique for security handling in SaaS

Techniques used and references	*Issues*	*Functionality*
SDN with a distributed ad-hoc control plane (Akhunzada et al., 2015).	Routing, authentication, data security and network security.	To achieve maximum synchronisation among SDN controllers.
Data integrity functionality in SDN and the exercise of digital signatures in support of SDN Software modules. (Flauzac et al., 2015).	Configuration data extraction and alteration, masking as authorised SDN controller.	Exclusively, the authorised persons are allowed to access the data.
Open SDN APIs (Sivaraman et al., 2013).	Attaining virtualisation.	Enables dynamic service quality management.
SDN-based information-centric cloud network (ICCN) (Ghosh et al., 2017).	Data availability, dynamic computations and poor network security performance.	To perform dynamic computations and improve the security in network.
NFV in association with SDN (Patel et al., 2016).	Spoofing attack, man in the middle attack, DoS and DDoS attacks and SDN provides centralised network provisioning, cloud abstraction, guarantees content delivery.	Offers a strong network management by means of routing and network virtualisation.
SDN in combo with fog nodes (Modarresi et al., 2017).	IP spoofing, intrusion detection.	Allows the packets to be received from a trusted source.

Figure 2 represents the OpenFlow switch specification (Rolbin, 2013) of SDN. The SDN standard deals with dividing the packet forwarding service of the forwarding devices, specifically control and data planes. This decoupling nature of SDN facilitates a novel architecture, in which the switches in the network are incorporated with flow tables, portray how the received packets are handled depending upon the identical fields similar to incoming port, the content of packet header, a destination address, outgoing port and so on. Elements of OpenFlow (Mahesh et al., 2017; Lai et al., 2016) are:

- *Flow table*: Defines the act of every flow to alert the switch and informs how to process each flow.
- *Secure channel*: It sends the packets by setting command through a connecting switch and remote switch
- *OpenFlow protocol*: Offers a standard controller that can communicate with the switch.

Figure 2 OpenFlow switch specification of SDN



By using the OpenFlow protocol, the rules are supervised by a controller which provides secure communication with switches (Patel et al., 2016). The SDN's nature of OpenFlow switch specification avoids packet sniffing and sends a packet within regular intervals of time with no data loss.

In Rolbin (2013), the SDN controller with OpenFlow protocol permits to find any unusual behaviour of network by the configuration of the POX-based firewall module, which is a python-based SDN controller platform allowing more flexibility. Virtual networks such as MININET can be used to organise and put off any malicious action on the network devices. With the aid of SDN and virtualisation, network threats can be identified in very beginning stages.

3.2 Non–SDN techniques in SaaS security handling

In SaaS, cloud providers send applications on the cloud infrastructure to the customers without installing the applications on their systems. Implementing security is one of the shared responsibilities of cloud service suppliers in SaaS. Networking systems which are not designed based on the paradigms of SDN could be encountered in reality. Hence, the non-SDN network governing functions ought to be divested to other physical controllers. As a result, any algorithm which maps the non-SDN virtual nodes onto SDN nodes should make a decision after considering the available space on the physical node and its related controller (Osgouei et al., 2017). Table 4 shows some of the significant security issues and existing non-SDN techniques. In Almorsy et al. (2014), a model driven security engineering approach is used to resolve a key gap in multi-tenant architecture at runtime. Another technique given in Paxton (2016) is Encryption and Key management techniques, Multifactor authentication, Segmentation and VM Introspection are used to get rid of data breaches, account hijacking and multi-tenancy threats. Similarly all the techniques were analysed and described in different references.

Table 4 Non-SDN techniques in SaaS security handling

Techniques used and references	*Issues*	*Functionality*
Model driven security engineering (Almorsy et al., 2014)	A key gap in multi-tenant architecture at runtime with lack of adaptable security support and lack of multi-tenant security engineering support.	It provides security requirements at runtime, which sustains holding, executing, and authenticating various tenants without any requirement to modify basic application/service.
Encryption and key management techniques, multifactor authentication, segmentation and VM introspection (Paxton, 2016)	Data breaches, account hijacking and multi-tenancy threats.	Data loss prevention tools for data breaches, mutual authentication, token-based authentication, biometric authentication for account hijacking and to fill gap and provide missing details to the hypervisor and segmentation at all levels to protect against multi-tenancy threats.
Image steganography and pixel key pattern (Kaur and Kaur, 2015).	Data privacy.	Image is used as cover in image stagenography in which the secret data is embedded which in turn detects the edges of images by pixel key pattern.
Digital signature and key exchange with elliptic curve diffie hellman (ECDH) and advanced encryption standard (AES) (Zissis and Lekkas, 2012; Rewagad and Pawar, 2013)	Confidentiality, integrity and authentication.	Trusted third party which in turn calls public key infrastructure operating in concert with SSO and LDAP Hussain and Yuvaraj (2015) and trusted computing.
Time-based proxy re-encryption scheme and attribute-based encryption (ABE) (Liu et al., 2014)	Confidentiality, scalability and authentication.	Attribute-based encryption (ABE) and proxy re-encryption (PRE) are combined to allot the cloud service provider (CSP) to execute re-encryption and to incorporate the idea of time into the combination of ABE and PRE.
Privacy-preserving semantics for multi-keyword ranked searching (MRSE) (Cao et al., 2014)	Privacy, integrity and usability.	Coordinating matching is used. Privacy and efficiency are guaranteed in this scheme and also gives low overhead on computation and communication.
Identity-based encryption (IBE) (Li et al., 2015)	Authentication.	By introducing the outsource computation into IBE: the constant efficiency is achieved for both computation at private key generator (PKG) and private key size at user; and authentication is not required during key-update between user and key update – cloud service provider (KU-CSP).
Identity-based cryptography (IBC), trusted cloud (TC) and elliptic curve cryptography (ECC) (Abbas, 2015).	Authentication, authorisation, robustness and privacy.	Improving the security of IAM in the cloud through ECC and trusted cloud. IBC is appropriate selection for IAM as it reduces the complexities of key management and ECC is robust algorithm which can resist against attacks.

3.3 SDN versus non-SDN techniques on various security issues

In this section, we discuss the efficiency of SDN and non-SDN. Later, Table 5 shows a comparison of these techniques with different issues of SDN and Non-SDN techniques.

3.3.1 Scenarios for SDN and non-SDN techniques

SDN can be used to deal with QoS management on large scale network, load balancing of traffic, dynamic agreements which are essential for the growth of an organisation. Using open APIs, SDN helps to centrally program network behaviour through software applications. Since SDN opens up previously closed networks, one can manage the entire network and all the devices consistently, no matter how complex the network is.

In non-SDN, there is no separation of control and data planes, and hence packet forwarding and high-level routing are on the same device and difficult to make high-level routing decisions. Further, traffic cannot be isolated and dynamic implementations become cumbersome.

3.3.2 Estimation of efficiency

The issues identified for computation of SDN and non-SDN techniques are (a) Network Security, (b) Account Hijacking, Spoofing and Privacy, (c) Access Control, (d) Virtualisation Vulnerability, (e) Authentication and Authorisation, (f) Packet Sniffing and Data Breaches. For each of the efficiency estimation, we allocate the value as either low or medium or high. Table 5 represents the comparison of SDN and Non-SDN techniques for several security issues. The issues considered for comparison are network security, account hijacking, spoofing, access control, virtualisation vulnerability, authentication and authorisation, packet-sniffing, and data breaches. For each of the issues, we assign numerical values. We arrive at this value by reviewing literature, quantitative analysis of results, relative comparisons of the quantitative results in various research papers, complexity of the scheme and mathematical complexity involved. For this quantitative analysis the values are given as:

- low: <40%,
- medium: >=40% and <80%,
- high: >=80%

Table 5 Comparison of SDN and non-SDN techniques

Security issues	*Non-SDN techniques*	*SDN techniques*	*Efficiency with non-SDN*	*Efficiency with SDN*	*Remarks*
Network security (Patel et al., 2016; Wu et al., 2016; Zhou et al., 2015)	Virtual network frame work on Xen platform.	Improving the network security through SDN and NFV integration and security analysis of SDN by applying AVISPA.	Low	Medium	The open vs. switch is not integrated into Xen. The SDN in combo with NFV provides an excellent network service.
Account hijacking, spoofing (Nagrathna and Salinie, 2017)	Multi-factor authentication, image steganography, single sign-on, IBC	Provides cloud abstraction and guarantees content delivery.	Low	Medium	Implementations of supervised learning approach with SDN to mitigate host location and SDN will monitor impersonate persons on data plane.
Access control (Nife and Kotulski, 2018)	Role-based access control.	SDN implementation with POX controller.	Low	High	SDN with POX provides centralised network provisioning to access data and denies the unauthorised access.
Virtualisation vulnerability (De Jesus et al., 2014)	HIDS (host-based intrusion detection systems) and NIDS (network-based intrusion detection systems).	OpenFlow of SDN implements virtualisation through a traffic differentiation practice which considers any packet header field.	Medium	High	SDN shapes and controls network traffic.
Authentication and authorisation (Hu et al., 2015; Oktian et al., 2018)	AES, LDAP, IBC.	SDN integrated with data integrity and implementation of REST API for SDN.	High	Medium	The security architecture of SDN will provide better results for authentication and authorisation.
Packet sniffing and data breaches (Paxton, 2016; Hu et al., 2015; Nife and Kotulski, 2018)	Data loss prevention tools, cryptographic methods.	SDN with decoupling nature and centralised control.	Low	Medium	Control and data plane are decoupled. So the packet incoming and outgoing decisions are done securely.

3.4 Advantages of SDN in solving security issues

The current systems are incapable of meeting the requirements of dynamic management, scalability, network traffic control, etc. due to the drastic increase in computer networking. SDN is emerging as an alternative that could profile and regulate network traffic. The decoupling feature of SDN enables centralised control of the network specifically for any size of the network which provides for:

- *Openness*: Openness comes from the SDN approach. Intelligent software can have control over hardware from various providers through open interfaces such as OpenFlow.
- *Network programmability*: Network activities are facilitated by SDN and controlled by the software that exists beyond the networking devices which offer physical connectivity. As a result, to support individual customers and new services, the network operators can shape the behaviour of their networks.
- *Centralised control and coordination*: Centralised control and coordination is achieved by separating the control and data planes, SDN can offer quick service delivery and provide more alertness in provisioning both physical and virtual network devices from a central location.
- *Minimise the capital expenditure*: It is minimised by reusing the existing hardware to track the instructions of an SDN controller, and deploying the cost-efficient hardware with more significant effect. Therefore, by implementing SDN, enterprises can easily optimise existing network devices.
- *Guarantees content delivery*: SDN guarantees delivering the data to the correct destination as it has the ability of controlling data traffic.

All choices such as routing and switching in conventional architectures etc. are within the knowledge of the controller. One of the major advantages of the security aspect is that SDN offers total vision and absolute mastery over the network traffic. This enables the implementation of consistent security policies as well as helps in the improvement of the same.

4 Open challenges of SDN technique in SaaS security handling

SDN faces challenges concerning increased demand. They are as follows:

1. *Increasing demand*: When it comes to the subject of promising latest trends and technologies in this era, the identification of several challenges is raising demand. For example, where there is enormous traffic, it takes more time for processing like video conferencing, browsing, uploading a video or file into the internet, and so on. In such cases, higher resource utilisation would improve the performance of a cloud (Horvath et al., 2015). For such type of enormous demands, new technologies should be implemented, but SDN deals only with developing new telecommunication infrastructure (Costa-Requena, 2014).
2. *Implementation*: Development of SDN implementation is still in an infant stage (Kobayashi et al., 2014). Different authors have different opinions. For example, Galis et al. (2013) made an extraordinary work of finding the implementation of new architecture without manipulating or reinventing the existing architecture. SDN requires re-engineering of entire network topology due to the financial limitations of enterprises and complete deployment of SDN facilitated network switches (Caraguay et al., 2013). Therefore, it remains a great challenge for the highly complex companies to implement the SDN. The SDN approach could be still justified by considering the advantages like scalability and reliability.
3. *Controller placement*: Controller placement dilemma influences abstracted control plane, starting flow-setup latencies to the reliability of the network, to fault tolerance, and lastly, the performance measures (Jammala et al., 2014).
4. *Scalability*: The practice of decoupled control and data planes has its own pitfalls. It generally includes a standard API for both planes, and the SDN controller becomes the restricted access in a situation, in which the network ranges the number of switches and nodes up.
5. *Performance*: It is a flow-based procedure, and performance is calculated based on two metrics: (i) flow-setup time and (ii) number of flows per second that the controller can switch. To overcome the restrictions on performance, focus is needed based on the factors that affect the flow-setup time and I/O performance of the controller (Shamugam, 2016).
6. *Security*: SDN is a gifted technology for computer networks and data-centre networks, but still it is lagging behind standardisation policies. The existing architecture of SDN does not comprise standards for accepting topology. SDN does not promote straight interactions among network nodes to allow association among devices (Jammala et al., 2014).
7. *Reliability*: SDN has a centralised controller. If the controller fails, the components associated with it would be at risk. Therefore, the system would not achieve reliability. To solve this problem, some countermeasure algorithms need to be imposed on SDN like dynamic load-balancing, Virtual Router Redundancy Protocol (VRRP) and Multi-Chassis Link Aggregation Group (MC-LAG) (Jammala et al., 2014).

5 Conclusions and future work

From the analysis of the existing works, it is observed that the SaaS environments are severely affected by various security issues, which may impact their adoption. If the right security module is not in place for the applications, the customers might not be able to leverage the benefits. This paper mainly focuses on the security issues of SaaS and their respective attacks. Although there are lots of concerns related to security, our research targets at identifying security issues and deciding on possible solutions through SDN and non-SDN techniques.

In future, researcher should focus on using SDN by resolving security issues in SaaS to: (i) design new algorithms with lower execution time, (ii) minimise the traffic load, (iii) optimise the cost and security, (iv) facilitate the heterogeneous network access, and (v) forward high-level decisions. Research work should be attempted at the simulation level for the intervention of SDN on SaaS model. With this approach, it is expected that SaaS would achieve a better security level than the applications that exist currently and hence would turn out to be an advantage in the design and operation of upcoming software architectures and services.

References

Abbas, S.A. (2015) 'Enhancing the security of identity and access management in cloud computing using elliptic curve cryptography', *Proceedings of the International Journal of Emerging Research in Management and Technology*, Vol. 4, No. 7, pp.8–15.

AbdElRahem, O., Bahaa-Eldin, A.M. and Taha, A. (2016) 'Virtualization security a survey', *Proceedings of the 11th International Conference on Computer Engineering and Systems (ICCES'16)*, IEEE, Cairo, Egypt, pp.32-40.

Agarwal, K., Rozner, E. and Dixon, C. (2014) 'SDN traceroute: tracing SDN forwarding without changing network behavior', *Proceedings of the 3rd Workshop on Hot Topics in Software Defined Networking*, ACM, pp.145–150.

Aime, M.D., Lioy, A., Pomi, P.C. and Vallini, M. (2011) 'Security plans for SaaS', *Proceedings of the New Frontiers in Information and Software as Services*, Springer, Vol. 74, No. 1, pp.81–111.

Akhunzada, A., Ahmed, E., Gani, A., Khan, M.K., Imran, M. and Guizani, S. (2015) 'Securing software defined networks: taxonomy, requirements, and open issues', *Proceedings of the IEEE Communications Magazine*, Vol. 53, No. 4, pp.36–44.

Almorsy, M., Grundy, J. and Ibrahim, A.S. (2014) 'Adaptable, model-driven security engineering for SaaS cloud-based applications', *Proceedings of the Automated Software Engineering*, Springer, Vol. 21, No. 2, pp.187–224.

Anjana and Singh, A. (2019) 'Security concerns and countermeasures in cloud computing: a qualitative analysis', *Proceedings of the International Journal of Information Technology*, Springer, Vol. 11, No. 4, pp.683–690.

Barona, R. and Anita, E.A.M. (2017) 'A survey on data breach challenges in cloud computing security: issues and threats', *Proceedings of the International Conference on circuits Power and Computing Technologies (ICCPC)*, IEEE, Kollam, India, pp.1–8.

Batyuk, L., Herpich, M., Camtepe, S.A., Raddatz, K., Schmidt, A-D. and Albayrak, S. (2011) 'Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within android applications', *Proceedings of the 6th International Conference on Malicious and Unwanted Software (MALWARE)*, IEEE, pp.66–72.

Brandall, B. (2018) *4 things SaaS Companies need to know about regulatory compliance*. https://www.process.st/regulatory-compliance/ (accessed on 6 December 2018).

Cao, N., Wang, C., Li, M., Ren, K. and Lou, W. (2014) 'Privacy-preserving multi-keyword ranked search over encrypted cloud data', *Proceedings of the IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 1, pp.222–233.

Caraguay, A.L.V., Lopez, L.I.B. and Villalba, L.J.G. (2013) 'Evolution and challenges of software defined networking', *Proceedings of the SDN for Future Network and Services (SDN4FNS)*, IEEE, Trento, Italy, pp.1–7.

Choo, K.K.R. (2014) 'Legal issues in the cloud', *Proceedings of the IEEE Cloud Computing*, Vol. 1, No. 1, pp.94–96.

Choudhury, A.J., Kumar, P., Sain, M., Lim, H. and Jae-Lee, H. (2011) 'A strong user authentication framework for cloud computing', *Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC'11)*, IEEE, pp.110–115.

Chouhan, P.K., Hagan, M., McWilliams, G. and Sezer, S. (2014) 'Network based malware detection within virtual environments', *Proceedings of the Large Scale Distributed Virtual Environments on Clouds and P2P*, pp.335–346.

Cisco Inc. (2013) *Software-defined networking: why we like it and how we are building on it*, White Paper.

Costa-Requena, J. (2014) 'SDN integration in LTE mobile backhaul networks', *Proceedings of the International Conference on Information Networking (ICOIN'14)*, IEEE, Phuket, Thailand, pp.264–269.

Cui, L., Yu, F.R. and Yan, Q. (2016) 'When big data meets software-defined networking: SDN for big data and big data for SDN', *Proceedings of the IEEE Network*, IEEE, Vol. 30, No. 1, pp.58–65.

De Jesus, W.P., Da Silva, D.A. and De Sousa Junior, R.T. (2014) 'Analysis of SDN contributions for cloud computing security', *Proceedings of the 7th International Conference on Utility and Cloud Computing*, IEEE/ACM, London, UK, pp.922–927.

De Souza, F.R., Miers, C.C., Fiorese, A. and Koslovski, G.P. (2017) 'QoS aware virtual infrastructures allocation on SDN-based clouds', *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, IEEE, Madrid, Spain, pp.120–129.

Deshmukha, R.V. and Devadkar, K.K. (2015) 'Understanding DDoS attack and its effect in cloud environment', *Proceedings of the 4th International Conference on Advances in Computing*, Elsevier, Vol. 49, pp.202–210.

Deshpande, P., Sharma, S.C., Peddoju, S.K. and Abraham, A. (2018) 'Security and service assurance issues in Cloud environment', *Proceedings of the International Journal of System Assurance Engineering and Management*, Springer, Vol. 9, No. 1, pp.194–207.

Dewangan, B.K. and Agarwal, A., Venkatadri and Pasricha, A. (2016) 'Credential and security issues of cloud service models', *Proceedings of the 2nd International Conference on Next Generation Computing Technologies (NGCT'16)*, Dehradun India, IEEE, pp.888–892.

Dong, S., Abbas, K. and Jain, R. (2019) 'A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments', *Proceedings of the* IEEE Access, IEEE, Vol. 7, pp.80813–80828.

Doroodchi, M., Iranmehr, A. and Pouriyeh, S.A. (2009) 'An investigation on integrating xml-based security into web services', *Proceedings of the 5th IEEE GCC Conference and Exhibition*, IEEE, pp.1–5.

El Moussaid, N., Toumanari, A. and El Azhari, M. (2017) 'Security analysis as software-defined security for SDN environment', *Proceedings of the 4th International Conference on Software Defined Systems (SDS'17)*, IEEE, pp.87–92.

Elsayed, M. and Zulkernine, M. (2019) 'Offering security diagnosis as a service for cloud SaaS applications', *Proceedings of the Journal of Information Security and Applications*, Elsevier, Vol. 44, pp.32–48.

Fernandez, E.B., Monge, R. and Hashizume, K. (2016) 'Building a security reference architecture for cloud systems', *Proceedings of the Journal of Requirements Engineering*, Springer, Vol. 21, No. 2, pp.225–249.

Flauzac, O., Gonzalez, C., Hachani, A. and Nolot, F. (2015) 'SDN based architecturefor IoT and improvement of the security', *Proceedings of the IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, IEEE, Gwangiu, South Korea, pp.688–693.

Galis, A., Clayman, S., Mamatas, L., Rubio Loyola, J., Manzalini, A., Kuklinski, S., Serrat, J. and Zahariadis, T. (2013) 'Softwarization of future networks and services - programmable enabled networks as next generation software defined networks', *Proceedings of the SDN for Future Networks and Services (SDN4FNS)*, IEEE, Trento, Italy, pp.1–7.

Ghosh, U., Chatterjee, P., Tosh, D., Shetty, S., Xiong, K. and Kamhoua, C. (2017) 'An SDN-based *Framework for Guaranteeing Security and Performance in Information Centric Cloud Networks*', *Proceedings of the10th International Conference on Cloud Computing (CLOUD)*, IEEE, Honolulu, CA, USA, pp.749–752.

Gupta, S., Gupta, S.C., Majumdar, R. and Rathore, Y.S. (2016) 'Measuring cloud security from risks perspective', *Proceedings of the 6th International Conference – Cloud System and Big Data Engineering (Confluence)*, IEEE, Noida, India, pp.214–220.

Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B. (2013) 'An analysis of security issues for cloud computing', *Proceedings of the Journal of Internet Services and Applications*, Springer, Vol. 4, No. 5, pp.1–13.

Horvath, R., Nedbal, D. and Stieninger, M. (2015) 'A literature review on challenges and effects of software defined networking', *Proceedings of the Procedia Computer Science, Elsevier*, Vol. 64, pp.552–561.

Hu, F., Hao, Q. and Bao, K. (2014) 'A survey on software-defined network and OpenFlow: from concept to implementation', *Proceedings of the IEEE Communications Surveys and Tutorials*, Vol. 16, No. 4, pp.2181–2206.

Hu, Z., Wang*, M., Yan, X., Yin, Y. and Luo, Z. (2015) 'A comprehensive security architecture for SDN', *Proceedings of the 18th International Conference on Intelligence in Next Generation Networks*, IEEE, Paris, France, pp.30–37.

Hussain, S.I.S. and Yuvaraj, V. (2015) 'A secure data access control method using AES for P2P storage cloud', *Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICJJECS'15)*, IEEE, Coimbatore, India, pp.1–5.

IBM Developer Community (2018) Available online at: https://www.ibm.com/developerworks/community/blogs/a9ba1efe-b731-4317-9724-a181d6155e3a/entry (accessed on 19 July 2018).

Indu, I., Anand, P.M.R. and Bhaskar, V. (2018) 'Identity and access management in cloud environment: Mechanisms and challenges', *Proceedings of the International journal of Engineering Science and Technology*, Elsevier, Vol. 21, No. 4, pp.574–588.

Jammala, M., Singha, T., Shamia, A., Asalb, R. and Lic, Y. (2014) 'Software defined networking: state of the art and research challenges', *Proceedings of the Journal of Computer Networks*, Elsevier, Vol. 72, pp.74–98.

Kao, D-Y., Wang, Y-S., Tsai, F-C. and Chen, C-H. (2018) 'Forensic analysis of network packets from penetration test toolkits', *Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT)*, IEEE, Chuncheon-si Gangwon-do, Korea (South), Korea (South), pp.363–368.

Kari, V. (2014) *The pros and cons of SaaS vs. on-premises deployment*. Available online at: https://smartbridge.com/pros-cons-saas-vs-premises-deployment (accessed on 4 November 2018).

Kaur, M. and Singh, H. (2015) 'A review of cloud computing security issues', *Proceedings of the International Journal of Advances in Engineering and Technology*, Punjab, India, Vol. 8, No. 3, pp.397–403.

Kaur, R. and Kaur, J. (2015) 'Cloud computing security issues and its solution: a review', *Proceedings of the 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, IEEE, pp.1198–1200.

Kemmer, F., Reich, C., Knahl, M. and Clarke, N. (2016) 'Software defined privacy', *Proceedings of the International Conference on Cloud Engineering Workshop*, Berlin Germany, IEEE, pp.25–29.

Ketel, M. (2018) 'Enhancing BYOD Security through SDN', *Proceedings of the Southeastcon*, IEEE, pp.1–2.

Kobayashi, M., Seetharaman, S., Parulkar, G., Appenzeller, G., Little, J., van Reijendam, J., Weissmann, P. and McKeown, N. (2014) 'Maturing of openflow and software-defined networking through deployments', *Proceedings of the Computer Networks*, Elsevier, Vol. 61, pp.151–175.

Lai, S-F., Su, H-K., Hsiao, W-H. and Chen, K-J. (2016) 'Design and implementation of cloud security defense system with software defined networking technologies', *Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, Jeju, Soth Korea, Vol. 1, No. 1, pp.292–297.

Li, J., Li, J., Chen, X., Jia, C. and Lou, W. (2015) 'Identity-based encryption with outsourced revocation in cloud computing', *Proceedings of the IEEE Transactions on Computers*, Vol. 64, No. 2, pp.425–437.

Liu, Q., Wang, G. and Wu, J. (2014) 'Time-based proxy re-encryption scheme for secure data sharing in a cloud environment', *Proceedings of the Information Sciences*, Elsevier, Vol. 258, pp.355–370.

Mahesh, A., Chandrasekaran, A., ArunKumar, R., SivaKumar, K. and Vigneshwaran, N. (2017) 'Cloud based firewall on OpenFlow SDN network', *Proceedings of the International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET'17)*, IEEE, Chennai, India, pp.1–6.

Mehta, S. and Saini, J. (2016) 'Tracking down unauthorized access by users in cloud', *Proceedings of the International Research Journal of Engineering and Technology (IRJET'16)*, Vol. 3, No. 8, pp.501–505.

Miltiadis, K., Nikos, V. and Dimitris, G. (2013) 'The insider threat in cloud computing', *Proceedings of the International Workshop on Critical Information Infrastructures Security*, Springer, Vol. 6983, pp.93–103.

Modarresi, A., Gangadhar, S. and Sterbenz, J.P.G. (2017) 'A framework for improving network resilience using SDN and fog nodes', *Proceedings of the Resilient Networks Design and Modeling (RNDM'17)*, IEEE, Alghero, Italy, pp.1–7.

Nagrathna, R. and Salinie, S.M. (2017) 'SLAMHHA: a supervised learning approach to mitigate host location hijacking attack on SDN controllers', *Proceedings of the 4th International conference on Signal Processing, Communication and Networking (ICSCN'17)*, IEEE, Chennai, India, pp.1–7.

Nife, F. and Kotulski, Z. (2018) 'New SDN-oriented authentication and access control mechanism', *Proceedings of the International Conference on Computer Networks*, Springer, Vol. 860, No.1, pp.74–88.

Oktian, Y.E., Lee, S-G. and Lam, H.Y. (2018) 'OAuthkeeper: an authorization framework for software defined network', *Proceedings of the Journal of Network and Systems Management*, Springer, Vol. 26, No. 1, pp.147–168.

Osgouei, A.G., Koohanestani, A.K., Saidi, H. and Fanian, A. (2017) 'Online assignment of non-SDN virtual network nodes to a physical SDN', *Proceedings of the Journal of Computer Networks*, Elsevier, Vol. 129, No. 1, pp.105–116.

Paikrao, R.L. and Pati, V.H. (2018) 'Security as a service model for virtualization vulnerabilities in cloud computing', *Proceedings of the International Conference On Advances in Communication and Computing Technology (ICACCT'18)*, IEEE, Sangamner, India, pp.559–562.

Park, T., Kim, Y., Yegneswaran, V., Porras, P., Xu, Z., Park, K.S. and Shin, S. (2019) 'DPX: data-plane eXtensions for SDN security service instantiation', *Proceedings of the Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA'19)*, Lecture notes in Computer Science, Springer, Vol. 11543.

Patel, P., Tiwari, V. and Abhishek, M.K. (2016) 'SDN and NFV integration in Openstack cloud to improve network services and security', *Proceedings of the International Conference on Advanced Communication Control and Computing Technologies (ICACCCT'16)*, IEEE, Ramanathapuram, India, pp.655–660.

Paxton, N.C. (2016) 'Cloud security: a review of current issues and proposed solutions', *Proceedings of the 2nd International Conference on Collaboration and Internet Computing*, Pittsburgh, PA, USA, IEEE, pp.452–455.

Pearce, P.M., Zeadally, S. and Hunt, R. (2013) 'Virtualization: Issues, security threats, and solutions', *Proceedings of the ACM Computing Surveys (CSUR'13)*, Vol. 45, No. 2, pp.1–39.

Prinzlau, M. (2017) *The 6 major cyber security risks to cloud computing*. Available online at: http://www.adotas.com/2017/08/the-6-major-cyber-security-risks-to-cloud-computing/ (accessed on 30 December 2018).

Ranjan, P., Mishra, P., Rawat, J.S., Pilli, E.S. and Joshi, R. (2014) 'Improved technique for data confidentiality in cloud environment', *Proceedings of the Networks and Communications (NetCom'13)*, Springer, pp.183–193.

Rashmi, Sahoo, G. and Mehfuz, S. (2013) 'Securing software as a service model of cloud computing: issues and solutions', *Proceedings of the International Journal on Cloud Computing: Services and Architecture (IJCCSA'13)*, Vol. 3, No. 4, pp.1–11.

Rath, A., Spasic, B., Boucart, N. and Thiran, P. (2019) 'Security pattern for cloud SaaS: from system and data security to privacy case study in AWS and Azure', *Proceedings of the IEEE Cloud tech Computers*, Vol. 8, No. 34, pp.1–28.

Rewagad, P. and Pawar, Y. (2013) 'Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing', *Proceedings of the International Conference on Communication Systems and Network Technologies (CSNT'13)*, IEEE, pp.437–439.

Rocha, E., Endo, P.T., Leoni, G., Braga, J. and Lynn, T. (2017) 'Analyzing the impact of power infrastructure failures on cloud application availability', *Proceedings of the International Conference on Systems, Man, and Cybernetics (SM'17C)*, IEEE, Banff, AB, Canada, pp.1746–1751.

Rolbin, M. (2013) 'Early detection of network threats using Software Defined Network (SDN) and virtualization', *Project submitted in partial fulfillment of the requirements for the Degree of Master of Engineering in Technology Innovation Management*, Ottawa, Ontario, Canada.

Sabahi, F. (2011) 'Virtualization-level security in cloud computing', *Proceedings of the 3rd International Conference on Communication Software and Networks (ICCSN'11)*, IEEE, Xian, China, pp.250–254.

Sahs, J. and Khan, L. (2012) 'A machine learning approach to android malware detection', *Proceedings of the European Intelligence and Security Informatics Conference (EISIC'12)*, IEEE, pp.141–147.

Satam, P., Alipour, H., Al-Nashif, Y. and Hariri, S. (2015) 'DNS-IDS: Securing DNS in the cloud era', *Proceedings of the International Conference on Cloud and Autonomic Computing*, IEEE, Boston, MA, USA, pp.296–301.

Seeber, S. and Rodosek, G.D. (2014) 'Improving network security through SDN in cloud scenarios', *Proceedings of the 10th International Conference on Network and Service Management (CNSM'14) and Workshop*, IEEE, Rio de Janeiro, Brazil, pp.376–381.

Sezer, S., Scott-Hayward, S. and Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M. and Rao, N. (2013) 'Are we ready for SDN? Implementation challenges for software-defined networks', *Proceedings of the IEEE communications Magazine*, IEEE, Vol. 51, No. 7, pp.36–43.

Shamugam, V. (2016) 'Software defined networking challenges and future direction: a case study of implementing SDN features on OpenStack private cloud', *Proceedings of the IOP Conference Series: Materials Science and Engineering*, pp.1–8.

Shin, S., Xu, L., Hong, S. and Gu, G. (2016) 'Enhancing network security through software defined networking (SDN)', *Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN'16)*, IEEE, Waikoloa, HI, USA, Vol. 1, No. 1, pp.1–9.

Singh, V. and Pandey, S.K. (2013) 'Cloud security related threats', *Proceedings of the International Journal of Scientific and Engineering Research*, Vol. 4, No. 9, pp.2571–2579.

Sivaraman, V., Moors, T., Matthews, J. and Russell, C. (2013) 'Virtualizing the access network via open APIs', *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, Santa Barbara, California, USA, pp.31–42.

Son, J. and Buyya, R. (2017) 'A taxonomy of SDN-enabled cloud computing', *Proceedings of the ACM Computing Surveys*, Vol. 1, No. 1, pp.1–31.

Son, J., Dastjerdi, A.V., Calheiros, R.N., Ji, X., Yoon, Y. and Buyya, R. (2015) 'CloudSimSDN: modeling and simulation of software-defined cloud data centers', *Proceedings of the 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid'15)*, IEEE, Shenzhen China, pp.475–484.

Song, H., Nguyen, P.H., Chauvel, F., Glattetre, J. and Schjerpen, T. (2019) 'Customizing multi-tenant SaaS by microservices: a reference architecture', *Proceedings of the International Conference on Web Services (ICWS)*, IEEE, Milan, Italy, pp.446–448.

Stephanow, P. and Khajehmoogahi, K. (2017) 'Towards continuous security certification of software-asa-service applications using web application testing techniques', *Proceedings of the 31st International Conference on Advanced Information Networking and Applications (ICAINA'17)*, IEEE, Taipei, Taiwan, pp.931–938.

Subashini, S. and Kavitha, V. (2011) 'A survey on security issues in service delivery models of cloud computing', *Proceedings of the Journal of Network and Computer Applications*, Elsevier, Vol. 34, No. 1, pp.1–11.

Sumitra, B. and Misbahuddin, M. (2013) 'A survey of traditional and cloud specific security issues', *Proceedings of the International Symposium on Security in Computing and Communications*, Springer, Vol. 377, No. 1, pp.110–129.

Surianarayanan, S. and Santhanam, T. (2012) 'Security issues and control mechanisms in cloud', *Proceedings of the International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM'12)*, IEEE, Dubai, UAE, pp.74–76.

Symantec (2018) *Data privacy and compliance in the cloud*. Available online at: https://www.symantec.com/content/dam/symantec/docs/white-papers/data-privacy-and-compliance-in-the-cloud-en.pdf (accessed on 1st December 2018).

Tsai, W.T., Bai, X.Y. and Huang, Y. (2014) Software-as-a-service (SaaS): perspectives and challenges', *Proceedings of the Science China Information Sciences*, Springer, Vol. 57, No. 5, pp.1–15.

Vahdat, A., Clark, D. and Rexford, J. (2015) 'A purpose-built global network: Google's move to SDN', *Proceedings of the ACM Queue*, Vol. 13, No. 8, pp.1–26.

Weihua, J. and Shibing, S. (2013) 'Research on the security issues of cloud computing', *Proceedings of the Intelligence Computation and Evolutionary Computation, Advances in Intelligent Systems and Computing*, Springer, Vol. 180, No. 1, pp.845–848.

Wu, H., Ding, Y., Winer, C. and Yao, L. (2010) 'Network security for virtual machine in cloud computing', *Proceedings of the 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT'10)*, IEEE, pp.18–21.

Wu, J., Wang, C-Y. and Li, J-F. (2016) 'LA-credit: a load-awareness scheduling algorithm for xen virtualized platforms', *Proceedings of the 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), International Conference on High Performance and Smart Computing, International Conference on Intelligent Data and Security*, IEEE, York, NY, USA, pp.234–239.

Yassin, M., Ould-Slimane, H., Talhi, C. and Boucheneb, H. (2017) 'SQLIIDaaS: a SQL injection intrusion detection framework as a service for SaaS providers', *Proceedings of the 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, New York, NY, USA, pp.163–170.

Yimam, D. and Fernandez, E.B. (2016) 'A survey of compliance issues in cloud computing', *Proceedings of the Journal of Internet Services and Applications*, Springer, Vol. 7, No. 5, pp.1–12.

Zhou, R., Liu, Z., Lai, Y. and Liu, J. (2015) 'Study on authentication protocol of SDN trusted domain', *Proceedings of the 12th International Symposium on Autonomous Decentralized Systems*, IEEE, Taichung, Taiwan, pp.281–284.

Zhu, G., Yin, Y., Cai, R. and Li, K. (2017) 'Detecting virtualization specific vulnerabilities in cloud computing environment', *Proceedings of the 10th International Conference on Cloud Computing (CLOUD'17)*, IEEE, Honolulu, CA, USA, pp.743–748.

Zimba, A. and Chama, V. (2018) 'Cyber attacks in cloud computing: modelling multi-stage attacks using probability density', *International Journal of Computer Network and Information Security (MECS'18*), Vol. 3, pp.25–36.

Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Proceedings of the Future Generation Computer Systems*, Springer, Vol. 28, No. 3, pp.583–592.