

Securing the Multitenancy Paradigm in Cloud Computing: An Exploration of Current Literature

Deepti Dave¹, Dr. Subhash Chandra Patel² and Dr. Jyoti Chauhan³

¹⁻³VIT Bhopal University, Kothrikalan, Bhopal-Indore Highway, Sehore MP, India 466114

Email: {deepti.dave2021, subhash.patel, jyoti.chauhan}@vitbhopal.ac.in

Abstract— Security in multi-tenant databases in cloud computing is a critical aspect, as it ensures that sensitive data is protected and isolated from other tenants. In a multi-tenant environment, multiple organizations or customers share the same infrastructure, making it challenging to ensure the security of their data. In this study, several papers have been analyzed from journals and conference papers, covering a variety of works on Security Multitenant databases in cloud computing. The articles in the literature used for the review were published between 2012 and 2022. This abstract presents a Hybrid approach for securing multi-tenant databases in cloud computing. This paper illustrates the approach which uses a combination of encryption and virtualization techniques to secure data and provide isolation between tenants. The main idea behind this approach is to balance the trade-off between security and performance, which are crucial aspects in multi-tenant environments. This approach's use of encryption ensures the security of data both in transit and at rest, and the virtualization process adds a layer of protection by isolating residents from one another. This survey shows that it is a viable solution for securing multi-tenant databases in the cloud, providing an acceptable level of security and performance.

Index Terms— Cloud Computing, Multi-tenancy, Cloud security, Cloud Threats and Cloud security controls.

I. INTRODUCTION

Cloud computing has become a popular choice for businesses and organizations looking for cost-effective and efficient computing solutions. However, as the utilization of cloud computing increments, so does the need for security to ensure that services are available and to prevent outages. Cloud security is a complex field that includes “computer security, network security, and information security”, and it involves the use of policies, technologies, and controls to protect data, applications, and the associated infrastructure of cloud computing [1] [2]. Encryption and key management are critical aspects of cloud security. Encryption is the method of changing over information into a coded format that is unreadable to unauthorized parties, and key management involves the creation, storage, and management of keys used to encrypt and decrypt data. By encrypting information time recently, it is sent to an inaccessible cloud capacity benefit, which ensures that the cloud storage service provider cannot access the data and that users can access specific parts of the data without compromising overall security.

Despite the many benefits of cloud computing, it is also susceptible to privacy and security attacks. These assaults can come from inside the Cloud supplier themselves, as they frequently have coordinate get to put away information and can take it for benefit. Subsequently, it is basic to guarantee that information security and

protection are secured amid communication on the cloud. This paper points to recognizing the issues related to cloud security and centers on information security and protection amid communication on the cloud. The remaining sections of the paper are structured as follows: Section 2 discusses the security risks associated with various cloud arrangement models, such as open, and private clouds, Section 3 examines security issues that arise in cloud environments and how they might be addressed, Section 4 looks into the security methods used by cloud service providers to protect client data and applications, Section 5 examines the many types of attacks that may occur in cloud environments, including information breaches and dissent of benefit assaults. Section 6 examines the various controls and innovations that were used to guard against security risks in cloud environments, such as encryption and access controls. Section 7 examines the need for untapped innovations to advance cloud security and protect against emerging risks. Section 8 summarises the paper's main findings and discusses potential areas for assistance research in cloud security.

II. THE CLOUD DEPLOYMENT MODEL SECURITY ISSUE

In an open cloud that empowers a public multi-tenant environment, as the quantity of clients increments, security dangers ended up additional extreme and assorted. To guarantee effective client-side and server-side assurance, it is basic to distinguish the regions that are defenceless to security assaults and to actualize instruments to secure them. Since there are several security issues in the open cloud, the recipients found it more secure to receive a private cloud arrangement which also offers the alternative to transfer to an open cloud in the future, on the off chance that is fundamental [3] [4]. Based on the arrangement shown of the cloud, security issues can be subdivided as:

A. Public Cloud Issues

In an open cloud, there are numerous clients on a shared stage and the benefits supplier is mindful of giving foundation security. Despite information being put away exterior of the client organization in an open cloud, it is critical to consider the opportunity for an insider assault from the benefit provider's conclusion. By transferring information to a cloud computing environment, the benefits provider's employees and subcontractors are included in the circle of insiders [3]. To avoid a system administrator from carrying out any noxious activities, approach authorization can be executed at the hubs and information centers. The three major steps in accomplishing this are: characterizing an approach, engendering the approach by employing a security arrangement engendering module, and implementing it through an arrangement requirement module.

B. Private Cloud Issues

Users have complete control over settings in a private cloud. The private cloud gives users the freedom to apply established security measures and procedures. Although private clouds are typically thought of as being more secure than public clouds, they nevertheless contain several problems that, if not fixed, might result in serious security risks. The security concerns stated for both private and public clouds are also applicable to the hybrid cloud paradigm, which mixes both.

III. CLOUD SECURITY AND PRIVACY

Cloud security is an advancing field that includes computer security, organized security, and data security. There are a few security issues and concerns related to cloud computing, but these issues can for the most part be separated into two wide categories: "security issues confronted by cloud suppliers and security issues confronted by their clients" [5]. Both parties have to guarantee the security of the cloud environment; "the supplier must guarantee that their foundation is secure and that their client's information and applications are ensured, whereas the client must take measures to brace their application and utilize solid passwords and confirmation measures. When an organization stores information or has applications on the open cloud, it loses physical to get to the servers facilitating its data, making it defenceless to insider assaults".

To relieve these dangers, Cloud Benefit suppliers must conduct exhaustive foundation checks for representatives who have access to the information center's servers physically. Within the cloud computing environment, security is characterized as "the capacity of a substance to control what data it uncovers almost itself to the cloud/cloud SP, and the capacity to control who can get to that data." One of the essential requirements to enable protection is security. This recommendation states that reasonable security measures should be used to protect personal data from risks such as "loss, unauthorized access, destruction, use, modification, or disclosure". "The Cloud Security Association (CSA) is a non-profit group that promotes the use of cutting-edge techniques to provide security in

cloud environments”. To ensure personalities and secure get-to administration, the CSA has released a Personality and Get-to Administration Direction that provides a set of recommended best practices.

IV. CLOUD SERVICE SECURITY

Security challenges can be divided into “network-level, user authentication-level, data-level, and generic issues”, according to the Cloud Benefit Show [2]. While each cloud reward show has unique security flaws, several issues are common to all of them. It is crucial to comprehend the linkages and circumstances between these cloud benefit models, according to current research on security problems in cloud computing [6]. SaaS and PaaS are constructed on upper region of IaaS; therefore, any IaaS security fault might affect how they are managed. In any case, it is additionally genuine that a breach in PaaS or SaaS can influence the security of IaaS. Additionally, PaaS provides a platform for developing and distributing SaaS apps, increasing the dependency on security between them. Due to these extreme circumstances, an attack on any cloud benefit layer can jeopardize the above layers. These relationships and situations between cloud model types could also present security risks. A PaaS provider, who may also rent a system from an IaaS provider, can provide a development environment to a SaaS provider. Each provider is accountable for protecting their services, which could lead to a clashing combination of security models. This will moreover make confusion over which benefit the supplier is capable of once an assault happens. Security observing for Cloud Benefit has appeared in Table I.

TABLE I. MONITORING SECURITY FOR CLOUD SERVICE

Monitoring Techniques	PaaS	SaaS	IaaS
Application monitoring	Inspecting application logs for flaws	Allow	Check application event logs for interruptions and application defencelessness logs for vulnerabilities
Network monitoring	Provider responsibility	Allow	Observe the virtual instances' network interfaces
Database monitoring	Provider responsibility	Allow	Introduce database security by observing computer program on virtual machines facilitating databases, and log occasions to a devoted log server
Host monitoring	Provider responsibility	Allow	Track safety occurrences from host IDSs like OSSEC. Send event logs to a specific, long-lasting log server. watch the system logs for VM security events.

A. Security Issues with SaaS

SaaS or Software as a Service offers application administrations on demand, including “e-mail, conferencing software, and business applications like ERP, CRM, and SCM” [7]. Among the three crucial cloud computing conveyance models, SaaS clients have the slightest control over security. The utilization of SaaS applications may bring up a few security concerns.

a. Data Security

Any innovation could raise information security concerns, but it becomes a significant issue when SaaS customers are forced to rely on their suppliers for reliable security [8] [9] [10]. The specific measures and technological advancements used to support data management are included in information security. The supplier is in charge of maintaining the data's security while it is being prepared and stored for the SaaS demonstration. Since information is located in the provider's information centers, “administrative compliance issues such as information security, isolation, and security that must be upheld by the supplier” may arise. Compliance within the SaaS model can be complicated.

b. Application Security

Blemishes in web submissions can make defencelessness for SaaS applications. The safety encounters in SaaS submissions are comparable to any web application innovation, but conventional security arrangements may not be compelling in securing against assaults, so unused approaches are vital [9]. Aggressors regularly utilize the net to compromise users' computers and perform pernicious exercises such as taking touchy information [11].

c. Multi-Tenancy

Multi-tenancy can lead to the visibility of residual data by other tenants, as multiple consumers from various organizations share resources or applications. This can pose a significant security risk, as data from different tenants might be stockpiled in the same database, increasing the potential for data leakage. To mitigate this risk, security policies must be implemented to confirm that customer data is kept distinct and protected [12].

d. Access Control

The ease of receiving applications over the web employing a web browser can make it more helpful for clients but too uncovered the benefit of extra security dangers. The Cloud Security Alliance [13] has identified the top threats in the area of mobile computing, such as “information-stealing mobile malware, insecure networks (Wi-Fi), vulnerabilities found in the device's operating system and official applications, insecure marketplaces, and proximity-based hacking”.

B. Security Threats for PaaS

PaaS (Platform as a Service) cloud situations give a comprehensive environment for planning, creating, testing, conveying, and supporting custom applications. Two computer program layers are included in PaaS application security: the security of the PaaS platform itself and the security of client applications sent on the platform [14]. PaaS providers are concerned with safeguarding the platform's software stack and taking into account the runtime engine that powers client apps. However, PaaS models also take into account security concerns connected to mashups, including information and setup security [15]. PaaS users must depend on “the security of third-party services and web-hosted development tools”. From the perspective of application development, designers must deal with the difficulty of creating safe applications that will be supported by the cloud. Additionally, they need to be aware that any modifications to PaaS components could jeopardize the security of their apps. In expansion, to secure improvement strategies, designers must be educated about information legitimate issues to guarantee that data isn't put away in improper areas. PaaS engineers don't more often than not have get to the fundamental layers, so suppliers are capable of securing the fundamental framework and the application administrations [16]. Designers must moreover guarantee that the advancement environment apparatuses given by a PaaS supplier are secure.

a. Access Control

Within the PaaS model, the CSP (Cloud Benefit Provider) is capable of overseeing getting control of the organize, servers, and the application stage foundation, whereas the client is dependable for get to control of the applications conveyed on the PaaS stage. This includes managing end-user access, including provisioning and authenticating users.

C. Security issues with IaaS

Presuming the virtual machine screen is secure and free of security flaws, IaaS (Infrastructure as a Service) shows that cloud clients have more control over security than other methods [9]. They are conscious of appropriately designing security approaches and have control over the software running on their virtual machines. However, cloud providers are in charge of managing the basic computing, organization, and capacity foundation. IaaS gives a pool of assets such as “servers, capacity, systems, and other computing assets within the shape of virtualized frameworks”, which are gotten to through the Web. Cloud suppliers must take critical measures to secure their frameworks to play down dangers coming about from “creation, communication, checking, adjustment, and portability” [17]. IaaS clients can essentially secure the cloud resources they have been given, unlike PaaS and SaaS clients. IaaS clients have complete access to the virtualized visitor VMs that the hypervisor innovation has enabled and separated from one another.

a. Virtualization

IaaS gives customers the ability to run a range of applications by allowing “users to create, clone, share, move, and roll back virtual machines”. But it also gives attackers new chances because there is a second layer that needs to be protected [11]. Virtualized situations are powerless against all sorts of assaults a bit like conventional frameworks, but securing them is more challenging as virtualization includes more focus on passage and increments interconnection complexity.

b. Virtual Machine Monitor (VMM)

A VMM or hypervisor can divide up virtual machines. A hacked VMM could put its virtual machines in danger as well. A low-level computer application called the VMM controls and keeps track of virtual machines, and like

many other regular programs, it could be vulnerable to security attacks [18]. All client spaces can be made public to malicious insiders by a powerless hypervisor. A malicious server could be substituted for a victim's virtual machine by an attacker using the movement module in the VMM.

c. Virtual Networks

Virtual networks increase the interconnectivity of VMs, which poses cloud computing a huge security concern [19]. The most secure technique is to use dedicated physical channels to connect each VM directly to its own. In any case, the majority of hypervisors connect VMs with virtual systems for better organized and effective communication.

d. Availability Management

Both cloud computing and cloud storage infrastructure should be taken into account when evaluating reliability for the IaaS delivery paradigm. IaaS providers might as well offer additional services such as “account management, message queue service, identity and authentication service, database service, billing service, and monitoring services”. As a result, when managing availability, it is important to consider all of the services that a user utilizes for their company and IT requirements.

V. ATTACKS ON CLOUD DATA

The frequency and variety of attacks on cloud data are increasing. Table II illustrates the different types of threats, the attacking method, and the layers where they occur most frequently. A risk alludes to a potential assault that will result in the abuse of data or assets, whereas defencelessness alludes to imperfections in a framework that empower an assault to be effective. Some of them are:

A. Attacks using Cross-Site Scripting (XSS)

A client-side code infusion attack known as XSS allows an attacker to insert malicious scripts into a legitimate website or web application. XSS, which happens when a web programme outputs user input that hasn't been checked or hasn't been encoded, is one of the most common vulnerabilities in web applications [20]. The targeted website must expressly contain user input on its pages in order for an XSS attack to work. It falls under the category of non-persistent and determined. Non-persistent gaps happen when server-side applications employ data provided by a web client, most commonly via HTTP query parameters or HTML form entries, to instantaneously interpret and present a page of results for and to that client without adequately sanitising the request. Determined XSS happens when the server saves the attacker's information without using correct HTML escaping, and the attacker's information is then permanently shown on "typical" pages returned to other clients during normal browsing. An example of a web forum where participants are permitted to publish messages with HTML design for other users to see.

B. SQL injection attacks

SQL Infusion could be a sort of assault where pernicious code is embedded into standard SQL code, permitting the aggressor to pick up unauthorized get to a database and get to sensitive data [21]. The attacker's input information is some of the time confused by the site as client information, permitting it to be gotten to by the SQL server. This gives the assailant information on the internet site's working and the capacity to create changes.

C. Man in the Middle attacks (MITM)

Another common course of assaults, especially in SaaS, is called MITM. In this sort of assault, a substance attempts to capture a continuous discussion between a sender and a client to infuse wrong data and pick up get the critical information being exchanged between them [22].

D. DoS/DDoS Attacks

A denial-of-service (DoS) assault is an endeavour to form a machine or organize an asset inaccessible to its planning clients by incidentally or inconclusively hindering or suspending the administrations of a have associated with the web. When a DDoS attack originates from several, sometimes thousands, intriguing IP addresses, it is said to be disseminated. Criminals that carry out denial-of-service attacks usually target locations or services offered by well-known web servers, such as banks and credit card payment gateways. The most characteristic of a DoS assault is the unequivocal endeavour by the assailant to avoid true blue clients from getting to the benefit [23].

VI. CLOUD SECURITY CONTROLS

Cloud security architecture is only effective if the appropriate defensive measures are implemented. An efficient cloud security architecture should take into account potential security management issues and address them through security controls. These measures are taken to guard against systemic flaws and lessen the impact of attacks [24]. The types of controls that make up cloud security architecture include:

TABLE II. CLOUD THREATS

Threats	Attack type	Layer
Data leakage	When the off-base individuals get the information when it is being sent, kept, examined, or handled, this is often known as data spillage.	SPI
Denial of Service	A pernicious client might take each asset accessible. Due to a need for assets, the framework is incapable to fulfil any demands from other substantial clients.	SPI
Account or service hijacking	There are numerous ways to steal an account, including through social engineering and shoddy credentials. If an attacker manages to obtain a user's credentials, he can carry out harmful operations like reading confidential information, altering data, and rerouting any transaction.	SPI
Data manipulation	By altering the data provided from the server application to their application component, users can attack web applications.	S
Sniffing/Spoofing virtual networks	Using ARP spoofing, a malicious VM can track the virtual network or even divert data from/to other VMs.	I
Malicious VM creation	When a genuine account is created, an attacker can produce a VM image with malicious code, like a Trojan horse, and store it in the provider repository.	I
VM hopping	When a VM can reach another VM, it occurs.	I

A. Preventive controls

Preventive controls improve the security of a system by identifying and eliminating vulnerabilities. One example is implementing strong authentication for cloud users, which ensures that only authorized individuals can access the system and positively identifies who is accessing it.

B. Detective controls

Detective controls are activated to detect and respond to any security occurrences. These controls are used to identify and respond to attacks on cloud frameworks and the fundamental communication basis, including “framework and organized security checking, interruption location, and anticipation” [24]. In case of an assault, detective controls trigger the fundamental preventative or remedial measures to relieve the issue.

C. Deterrent controls

Assaults on a cloud framework are implied to be diminished through obstacle approaches. Obstruction controls frequently lower the danger level by telling potential aggressors that there will be negative repercussions for them if they remain, compared to a caution sign on a fence or property.

D. Corrective controls

Remedial measures more often than not include decreasing the harm to reduce the impacts of an occurrence. They take effect either amid or taking after an occurrence. One illustration of remedial control is re-establishing framework reinforcements to repair a compromised framework.

VII. TECHNOLOGY REQUIRED FOR CLOUD SECURITY

A few crucial limits, such as “security, compliance, privacy, and legal problems, prevent the use of cloud computing”. Security is considered the most significant barrier, as the cloud represents a new computing model and there is a dearth of knowledge regarding how to shift application security to the cloud and ensure security at all levels [25]. This uncertainty has made information executives cautious about adopting cloud computing. Research into secure data processing in the context of cloud computing has been gaining attention in recent years. Cloud security is a complex issue that includes protecting data confidentiality and privacy. While encryption and authentication are essential technologies for cloud security, they only address specific concerns and cannot provide a complete security solution alone.

Encryption is used to protect data while in transit and at rest, making it unreadable and inaccessible to unauthorized parties. However, encryption alone is not sufficient to protect against other security threats such as unauthorized access or data breaches. Authentication is used to confirm the identity of users and devices, and to ensure that only authorized individuals have access to sensitive data and resources. However, even if access is granted to only authorized users, data may still be vulnerable to breaches if proper security protocols are not in place. A complete security solution for cloud systems also includes technologies such as “firewalls, intrusion detection, and prevention systems, virtual private networks, identity and access management systems, security information and event management tools, and vulnerability management software”. These technologies work together to provide a comprehensive security solution that protects data, applications, and infrastructure from unauthorized access, misuse, and breaches. Additionally, technologies like containerization, multi-factor authentication, and security orchestration, automation, and response (SOAR) are becoming more popular in recent years to enhance cloud system security. Fig. 1, depicts the various Cloud security requirements which is crucial for organizations to continuously evaluate and update their security measures to keep up with the ever-evolving threat landscape.



Figure 1: Requirement for Cloud Security

VIII. CONCLUSION AND FUTURE WORK

Security is a major obstacle to the adoption of cloud computing because of the lack of control and visibility over data and services in the cloud. Organizations have to rely on third-party providers for security services, which can be difficult to verify and monitor. This makes it challenging for organizations to ensure that their data and services are secure. Future research could focus on developing new security technologies and solutions that provide better visibility and control over data and services in the cloud. Additionally, research could be done on how to improve collaboration and communication between organizations and CSPs to ensure robust security measures are in place. Another area of future research could be the development of new security standards and regulations for cloud computing to provide a clearer framework for ensuring the security of data and services in the cloud. Finally, future work could also focus on the implementation of security best practices and guidelines for organizations using the cloud, as well as the development of security awareness programs to educate employees and users on maintaining secure data and services in the cloud.

REFERENCES

- [1] Qi, H. and Gani, A., 2012, May. “Research on mobile cloud computing: Review, trend, and perspectives”. In 2012 second international conference on digital information and communication technology and its applications (DICTAP) (pp. 195-202). IEEE.
- [2] Guzek, M., Bouvry, P. and Talbi, E.G., 2015. “A survey of evolutionary computation for resource management of processing in cloud computing,” IEEE Computational Intelligence Magazine, 10(2), pp.53-67.
- [3] Tianfield, H., 2012, October. “Security issues in cloud computing”. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 1082-1089). IEEE.
- [4] De Cusatis, C., Cannista, R. and Hazard, L., 2014, October. “Managing multi-tenant services for software defined cloud data center networks”. In 2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST) (pp. 1-5). IEEE.
- [5] Dalla, L.O.F.B., 2020. “IT security Cloud Computing”.

- [6] Hossain, M.M., Fotouhi, M. and Hasan, R., 2015, June. "Towards an analysis of security issues, challenges, and open problems in the internet of things". In 2015 IEEE World Congress on Services (pp. 21-28). IEEE.
- [7] Akande, A.O. and Van Belle, J.P., 2014, October. "Cloud computing in higher education: A snapshot of software as a service". In 2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST) (pp. 1-5).
- [8] Sugumaran, M., Murugan, B.B. and Kamalraj, D., 2014, February. "An architecture for data security in cloud computing". In 2014 World Congress on Computing and Communication Technologies (pp. 252-255). IEEE.
- [9] Chang, V. and Ramachandran, M., 2015. "Towards achieving data security with the cloud computing adoption framework". IEEE Transactions on services computing, 9(1), pp.138-151.
- [10] Tari, Z., Yi, X., Premaratne, U.S., Bertok, P. and Khalil, I., 2015. "Security and privacy in cloud computing: vision, trends, and challenges". IEEE Cloud Computing, 2(2), pp.30-38.
- [11] Zhao, G., Xu, K., Xu, L. and Wu, B., 2015. "Detecting APT malware infections based on malicious DNS and traffic analysis". IEEE access, 3, pp.1132-1142.
- [12] Benzidane, K., Khoudali, S. and Sekkaki, A., 2012, December. "Autonomous agent-based inspection for inter-vm traffic in a cloud environment". In 2012 International Conference for Internet Technology and Secured Transactions (pp. 656-661). IEEE.
- [13] Luna, J., Suri, N., Iorga, M. and Karmel, A., 2015. "Leveraging the potential of cloud security service-level agreements through standards". IEEE Cloud Computing, 2(3), pp.32-40.
- [14] Gass, O., Meth, H. and Maedche, A., 2014. "PaaS characteristics for productive software development: an evaluation framework". IEEE Internet Computing, 18(1), pp.56-64.
- [15] El Moctar, C.B.O.M. and Konaté, K., 2017, March. "A survey of security challenges in cloud computing". In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 843-849). IEEE.
- [16] Bokhari, M.U., Shallal, Q.M. and Tamandani, Y.K., 2016, March. "Cloud computing service models: A comparative study". In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 890-895). IEEE.
- [17] Bitam, S., Mellouk, A. and Zeadally, S., 2015. "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks". IEEE Wireless Communications, 22(1), pp.96-102.
- [18] Brohi, S.N., Bamiah, M.A., Brohi, M.N. and Kamran, R., 2012, December. "Identifying and analyzing security threats to virtualized cloud computing infrastructures". In 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM) (pp. 151-155). IEEE.
- [19] Moreno-Vozmediano, R., Montero, R.S., Huedo, E. and Llorente, I.M., 2017. "Cross-site virtual network in cloud and fog computing". IEEE Cloud Computing, 4(2), pp.46-53.
- [20] Johari, R. and Sharma, P., 2012, May. "A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection". In 2012 international conference on communication systems and network technologies (pp. 453-458). IEEE.
- [21] Qian, L., Zhu, Z., Hu, J. and Liu, S., 2015, January. "Research of SQL injection attack and prevention technology". In 2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF) (pp. 303-306). IEEE.
- [22] Mainka, C., Mladenov, V. and Schwenk, J., 2016, March. "Do not trust me: Using malicious IdPs for analyzing and attacking Single Sign-On". In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 321-336). IEEE.
- [23] Keshri, A., Singh, S., Agarwal, M. and Nandiy, S.K., 2016, December. "DoS attacks prevention using IDS and data mining". In 2016 International Conference on Accessibility to Digital World (ICADW) (pp. 87-92). IEEE.
- [24] Shameli-Sendi, A., Jarraya, Y., Pourzandi, M. and Cheriet, M., 2016. "Efficient provisioning of security service function chaining using network security defense patterns". IEEE Transactions on Services Computing, 12(4), pp.534-549.
- [25] Ahmad, N., 2017, March. "Cloud computing: Technology, security issues and solutions". In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 30-35). IEEE.