International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development

Abhishek[1*] and Pranav Khare[2]

[1]Independent Researcher
[2]Independent Researcher, Woodinville, WA, USA

Received 01 Nov 2021, Accepted 10 Dec 2021, Available online 13 Dec 2021, **Vol.11, No.6 (Nov/Dec 2021)**

Abstract

Software as a service (SaaS) and other contemporary applications rely on the scalable, on-demand resources made possible by cloud computing, which has changed the way computer services are delivered. SaaS provides numerous benefits; in particular, it is cheaper, easy to use and readily scalable, but it also means large risks because its construction is multi-tenant and based on cloud technologies. These risks encompass data theft, unauthorised access, identity threats as well as compliance concerns, all of which translate to potential hefty monetary and brand losses. The following paper aims to explore the historical development of and the security issues surrounding cloud computing with an emphasis on SaaS. Major security issues, for instance, data separation, network insecurity, and web application risks are described using examples. Moreover, the paper defines the guidelines for the secure SaaS model and such pillars as encryption, access control, IAM, security audits, and security incidents management. By integrating these strategies, organisations can mitigate security risks, ensure compliance with regulatory standards, and maintain user trust while leveraging the full potential of SaaS applications.

Keywords: *Loud computing, SaaS security, data security, SaaS Application, cloud security patterns.*

Introduction

In the past, people would use the idea of a cloud to represent the internet. This application stems mostly from its generic representation in network diagrams as a cloud, which is used to expose the transportation of data over carrier backbones to its ultimate destination on some other portion of the cloud. This phrase originated in 1961 and gained widespread use by year's end [1].

Computing in the cloud is sometimes called internet computing. Online cloud computing services are generally available. Users are granted access to internet resources throughout the internet using clouds. Cloud computing eliminates the need to physically store critical resources and makes them accessible from any location at any time[2]. Cloud computing is well illustrated by Google Apps, which can extend services to over a billion devices via the cloud [3].

Security concerns, however, become more apparent with the broad use of cloud computing, especially with SaaS applications. Some of these difficulties include security breaches, non-authorized access as well as multi-tenant system weakness.

*Corresponding authors' ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.11.6.11

These risks require strong secure access protocols, use of encryption and constant security audit and overhauls. Staying compliant and having the protection of better threat detection frameworks add to the improvement of the SaaS applications' security environment[4].

Cloud-based applications of SaaS nature bring unparalleled convenience and flexibility along with built-in security risks associated with such software design. Due to the fact that all users in a multi-tenant model share the same space, there is a larger probability that an issue may impact multiple users. Such threats directly call for the development of a suitable security framework that singles out measures aimed at protecting data, preserving users' confidence, and enhancing operational reliability. The best practice is to encrypt data to ensure it is safe both when stored and when in transit; the second is to bake in robust constraints for users; and the third is to adhere to all regulations that govern the use of SaaS while utilising its advantages. This synchronisation makes certain that the factors of SaaS that relate to scalability and accessibility can get the best Systems without undermining the aspects of security and reliability[5].

This paper's goal is to examine the main security issues with SaaS applications in cloud computing settings and to provide solutions to these problems. Therefore, this paper aims at comparing cloud security

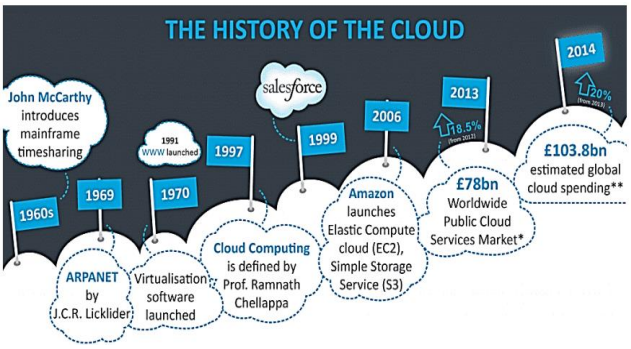
development over the years and discussing threats like data leakages, multi-tenancy, and identity management to ensure organisations get practical guidelines on how to increase the security, compliance, and reliability of SaaS apps while remaining cost-effective and reliable to their users.

Structure of paper

This research is organised as follows: Section II reviews the evolution of cloud security. Section III examines challenges in securing SaaS applications. Section IV discusses best practices for secure SaaS development. Section V provides recommendations for improving SaaS security, and Section VI concludes with key findings and future research directions.

The Evolution of Cloud Security

Figure 1 shows that the last decade has been the most formative for cloud computing, which is today acknowledged as a pervasive and revolutionary technology [6]. However, centralised computer systems emerged in the 1950s, marking the conceptual beginnings of cloud computing. During this era, mainframe systems were large and prohibitively expensive, making it impractical for organisations to allocate individual systems for each user[7]. Instead, these systems were shared among multiple users, reflecting the foundational principles of modern cloud computing.



Cloud computing evolution phases

Also, clearly, not many out of each odd single specialist expected induction to one reliably as they do today[8]. Taking everything into account, most affiliations would be two or three machines, and thereafter realise "time-sharing" plans which engaged various customers to get to the central concentrated worker PC from related stations. These stations were referred to as "inept terminals" since they did not possess any dealing power whatsoever. This kind of pooled computing resources is, in the end, the starting point and most basic explanation of appropriated registration[9].

J.C.R. Licklider, an American PC analyst, proposed an integrated path of PCs in the 1960s, which was a watershed moment in distributed computing. In 1969, "Lick", as he is much of the time known, developed an unrefined interpretation of the Internet, called the ARPANET. The ARPANET was the first network to enable the division of advanced sources among computers located in different physical locations. Additionally, Lick envisioned a place where all individuals would be linked by personal computers and ready to access data from any location. Sound unmistakable? Clearly it does; it is the Internet, all things considered, and a requirement for getting to every one of the benefits that the cloud sorts it out.

All through the drawn out that followed, various further movements in cloud advancement showed up. Consider an example, in 1972, IBM conveyed a working structure (OS) called the Virtual Machine (VM) working system[10]. Virtualisation is the one which is a virtual PC that acts similarly as a certifiable one, and acts with an operational OS. The thought progressed with the Internet, and associations began offering "virtual" private associations which could be rented as assistance, in the end inciting the improvement of the bleeding edge conveyed processing establishment during the 1990s [11].

Security Threats with Current Cloud Computing

The following are examples of some of the most prevalent risks to data security in the modern cloud:

Data breaches

The most prevalent sort of information security event is data breaches, which may result in significant financial losses for companies [12]. When malicious actors have illegal access to data stored in the cloud, a data breach may ensue. Data breach symbolic representation is shown below in Figure 2.

Data breach symbolic image

Malware

Software with the intent to steal information, harm systems, or impede operations is known as malware [13]. Email attachments, malicious websites, and software vulnerabilities are the three main vectors via which malware may attack cloud-based systems. The symbolic representation of malware is shown below in Figure 3.

Malware symbolic image

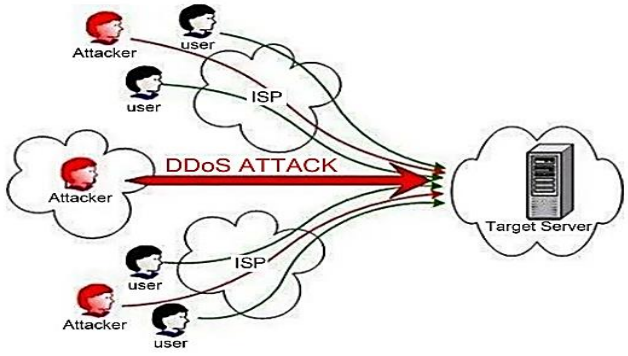
Phishing attacks

Phishing attacks aim to deceive users into divulging confidential information, such login credentials or financial details [14]. Any number of channels, including email, social media, and fraudulent websites, may be used to launch phishing attacks. Figure 4 displays a symbolic picture used in phishing.

Phishing symbolic image

Denial-of-service attacks

The goal of a denial-of-service attack is to prevent legitimate users from accessing a cloud-based system by flooding it with traffic [15]. Botnets, which are basically just networks of infected computers, may be used to launch DoS assaults. The symbolic representation of a denial-of-service attack is shown below in Figure 5.

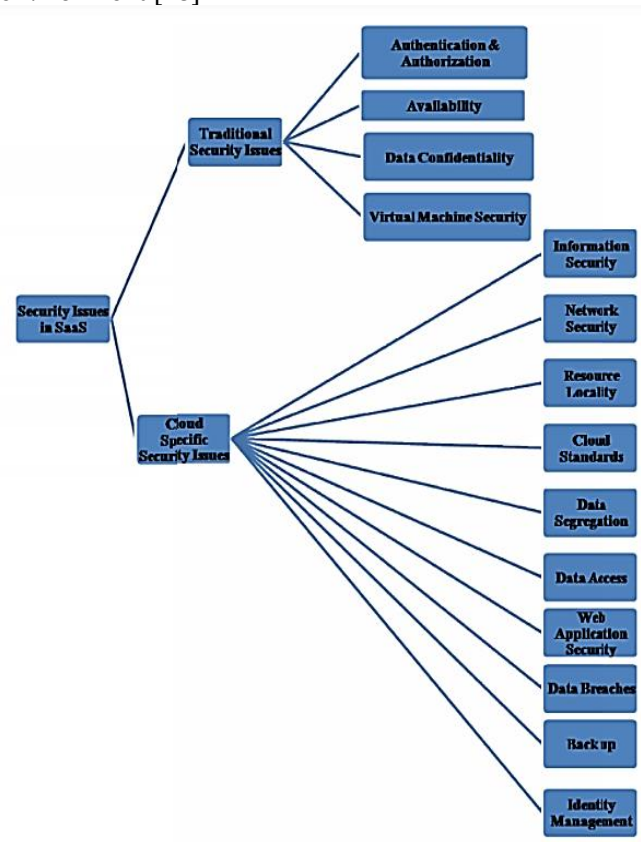


Denial-of-service symbolic image

Here are a few real-life examples to help you understand how breaches might affect organisations that are housed in the cloud. Considering that an increasing number of businesses utilise cloud-based data storage, the instances of cloud data breaches have also escalated. Managers might have financial and image-related losses if a cloud data leak occurs[16][17].

Challenges In Securing Saas Applications

Since software as a service application rely on cloud infrastructure and a multi-tenant architecture, their security is of the utmost importance. Information leakage, unauthorised access, veil threats in virtualisation, and sharable access are significant security issues. Solving these problems requires utilisation of suitable data encryption methods, stringent data access controls, and efficient mechanisms for separation of tenant data. Employing and incorporating high risk threat detection systems, along with following the guidelines of organisations like the GDPR or HIPAA are also important [4]. It is suggested to perform the monitoring and security audits repeatedly with the aim to track all new threats successfully to create strong security of the SaaS environment [18].



Security issues in SaaS

Data security and access control are only two of the many new issues brought about by the paradigm shift to cloud computing [19]. Over the past decade, extensively explored these challenges, contributing to a deeper understanding of critical security concerns in cloud environments discussed in Figure 6 and points mentioned below:

Information Security

Data that is sensitive to an enterprise remains inside the organisation's boundaries in a conventional on-

premise application deployment architecture, where it is protected by the company's rules for physical, logical, and human access control. In contrast, the SaaS provider ends up storing company data outside of the enterprise perimeter [20].

Network Security

The SaaS provider ends up storing sensitive data that has been processed by the SaaS application after receiving it from the organisations. Protecting sensitive information from leaking out requires securing every data flow across the network. This necessitates the implementation of robust security measures for network traffic encryption, including SSL and TLS [21].

Resource Locality

In software as a service (SaaS) cloud environment, end users use the services offered by cloud providers—possibly in different legal domains—without fully understanding where the resources for these services are stored [22]. This presents a possible issue in the event of conflicts, which are sometimes beyond cloud providers' control. In many organisational architectures, data localisation is crucial due to compliance and data privacy regulations in different nations[23].

Cloud standards

Cloud standards from several standard-setting bodies are necessary to establish interoperability and to improve the stability and security of clouds. For instance, it's possible that one cloud provider's storage services aren't compatible with another provider's [24]. Cloud service companies sometimes use so-called "sticky services" to hold onto consumers; these services make it hard for users to switch providers; for example, Google Drive and IBM Blue Cloud aren't compatible with Amazon S3.

Data Segregation

A key feature of cloud computing is multi-tenancy. Thanks to multitenancy, SaaS systems can accommodate numerous users' data storage needs. There will be no separation of consumers' data in this scenario. It is feasible for other users to access the data of other users in this environment [25]. Hacking via the application's vulnerabilities or inserting client code into the SaaS system are two ways to accomplish this breach.

Data Access

The security guidelines that users are given while accessing data are the primary cause of data access issues. Generally speaking, a small company may utilise a cloud service offered by another supplier to conduct its operations [26]. Each employee of this company will have access to a specific collection of data depending on its own security regulations.

Web application security

SaaS is software that may be installed on a personal computer or local area network and/or operate behind a firewall. Among the primary features are network-based access to and administration of commercial software, the ability to administer operations from centralised locations rather than at each customer's site, and the ability for customers to access applications remotely over the Web [27].

Data breaches

A breach in the cloud environment might possibly affect the data of all users since it contains data from different users and business organisations. The cloud, therefore, becomes a very valuable target. According to the Verizon Business Breach Report blog, external criminals are the biggest danger (73 percent), but it have the least effect (30,000 compromised data), which leads to a weakness in virtualisation.

Backup

Applications hosted in the cloud are not well-suited to the conventional backup strategies used by legacy applications and data centres, which were mostly developed for consumer and web-based apps. In order to enable rapid recovery in the event of catastrophes, the SaaS provider must provide frequent backup of all important company data [28].

Identity management and sign-on process

The field known as identity management (IdM) or ID management focusses on a system's ability to identify users and govern their access to its resources by imposing constraints on their identities. Many see this as a major obstacle to effective information security [29].

Implementing Best Practices for Secure Saas Development

This section focuses on essential best practices for ensuring security in SaaS solutions. It focuses on measures that would ensure proper design and implementation to avoid leakage of users' data and compromise of the system.

Data Encryption and Protection

Security of data is a crucial aspect in relation to SaaS, where confidentiality, integrity and availability of information are critical hallmarks of SaaS security, where the information is protected even when it is being transferred from the client to the server.

Encryption and key management best practices applied in practice lower the likelihood of data leaks and unauthorised data access.

Encryption at Rest and in Transit

Provider security mechanisms apply strong Data Encryption Standard, especially Advanced Encryption Standard – AES 256 when data is stored, which encompasses file systems and databases. For data in transit there is a use of protocols like TLS 1.2 or higher in the communication between clients and servers. Even in the case of data intercepture or physical entry, these safeguards will prevent unauthorised access [30].

Key Management Strategies

The essence of the security of encryption is based on a pair of keys used for the purpose of encryption and decryption. Azure Key Vault as well as AWS KMS are integrated tools for managing the keys to solutions. These services help to consolidate key storage and offer controls for rotating keys to lower exposure while offering strong access measures. Another option for managing or storing keys is by using a tamper resistant platform known as a Hardware Security Module (HSM).

Identity and Access Management (IAM)

To control and ultimately constraint the number of users accessing SaaS services, there must be IAM. This will guarantee the ' that only the privileged user can perform certain operations or retrieve some data.

Role-Based Access Control (RBAC):

RBAC is a security measure that only gives users authorisation to those portions of a system that it require for their roles. This is much easier for preventing privilege abuse. For instance, the developers can only be allowed to work in the development environments, while the auditors are only allowed to view logs [31].

Multi-Factor Authentication (MFA)

MFA is an additional security feature in which the client has to employ not only an identity password but also undergo time-based OTP or biometric check. The popular applications for MFA include Google Authenticator or YubiKey; in general, such tools provide great protection against credential stuffing [32].

Application Security Best Practices

Application security concerns itself with safeguarding SaaS software against threats and exploits by use of secure programming and liable testing procedures.

Secure Coding Standards

To limit the effects of continually occurring vulnerabilities as the SQL injection and cross-site scripting (XSS), the developers should follow the good coding practices like the ones stated in the OWASP Top 10. With parameterised queries and validated input, the development is safe from a SQL injection attack [33].

Regular Security Testing and Vulnerability Assessments

Static and dynamic testing is done with the aim of detecting risks in as early as the development and deployment phases. These are done by prone applications such as Veracode and OWASP ZAP to provide assurance of the application's strength.

Network Security

Network security helps to prevent unauthorised access and in addition protect the SaaS infrastructure from cyber threats [34].

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)

There are Application layer Firewalls like Web Application Firewall to screen the traffic and prevent SaaS apps from DDoS and other suspicious requests. IDS/IPS systems assume the role of supervision and detection of active intrusions, making for an aggressive protection strategy.

Secure VPNs and Network Segmentation

VPN protocols such as OpenVPN assure the creation of secure encrypted channels between endpoints. Through isolation of a network by partitioning certain segments of a network (like the production, development, and testing segments), the network is actually bolstered in terms of security.

Incident Response and Recovery

Mitigation of damage and insurance of the company stability during the period of security infringement obliges the usage of proper incident response and recovery approaches.

Establishing an Incident Response Plan

This implies that if an organisation has an incident response strategy then such security event may even be better detected, contained, and mitigated. The plan helps businesses react quickly and efficiently to breaches by outlining procedures for recovery and root cause investigation.

Backup and Disaster Recovery Mechanisms

Regular backups, coupled with automated recovery systems, ensure data integrity and availability during outages or cyberattacks. Tools like AWS Elastic Block Store (EBS) snapshots provide point-in-time recovery options, while geographically dispersed backup storage adds redundancy for added resilience.

Literature Review

Cloud security and best practices for protecting SaaS applications are discussed in this part of the research. The reviewed work primarily focuses on key security risks, mitigation strategies, compliance requirements, and emerging trends in SaaS development methodologies.

In this study, Xu, Zhang and Shuang (2016) present to pose a novel solution that combines the unified data collection with a hybrid data storage and analysis, which provides strong customisation through the web service. They had implemented the proposed framework called Log on Cloud (LOC). Through extensive experiments, they demonstrated the effectiveness of this framework. However, more and more services are popping up online due to the popularity of cloud computing and service computing[35].

In this study, Akinrolabu, New and Martin (2019) evaluating the potential dangers of a SaaS service that runs on several clouds requires doing a case study to prove that a supply chain inclusive risk assessment technique is effective. CSPs can use the CSCCRA model to analyse the risk of the SaaS application, determine the monetary value of the risk, and identify critical suppliers. The model also helps CSPs map their supply chain and identify weak security spots within the chain. The CSCCRA approach is innovative in that it allows CSPs to do risk assessments more often in reaction to changes in the supply chain, and it adjusts to the ever-changing cloud environment, which is crucial for the delivery of SaaS applications[36].

In this work, Lopez-Viana et al. (2020) shows how customised SaaS upgrades on CDs at the edge of the IoT have been successful. This might open up new IoT-edge business models. A CD process flow for customised SaaS apps at edge nodes and an architectural architecture of a highly distributed (cloud and edge) IoT system are presented in this paper. The CD process flow and the architectural concept are both implemented in a precision agricultural case study[37]. In this study, Ghaffari, Gharaee and Forouzandehdoust (2017) to propose a reference model and practical guidance for safeguarding cloud computing environments by combining security requirements and division of duties models. The suggested security reference model takes into account the security controls and needs for every cloud tier as well as for each service type. Further, it makes the management of security measures distinct from the duties of the cloud provider and the cloud client. People interested in providing or using cloud computing environments may find this document immediately helpful as it covers all the essentials of security protocol[38].

This study, Bhajantri and Mujawar (2019) investigates a range of security concerns from each of these angles. In addition to introducing the idea of Identity and Access Control in the cloud, the article provides a concise overview of the security concerns at the infrastructure and data levels. Additionally, many approaches to address or prevent cloud security vulnerabilities are covered. Through the use of third-party cloud service providers, cloud computing makes it possible to tap into a common pool of resources. It has several advantages, including efficiency, scalability, adaptability, minimal operating costs, and more[39].

Conclusion and Future Scope

This paper has discussed the development of cloud computing and the main security threats related to the SaaS model, such as unauthorised access, sharing of the tenant space, and network threats. Hence, in worrying over these challenges, the paper underlines effective solutions like the ones discussed above, including medio- and long-term goals of an all-encompassing security approach encompassing reliable encryption, access, and security assessment mechanisms. Safeguarding the quality of data content, adherence to related regulations and retaining the confidence of users is critical to fully unlocking SaaS solutions. Protection of data and risk reduction in the dynamic interconnected environment is possible only through such measures.

Future research should then address development of more flexible security paradigms for SaaS environments relying on AI and ML to detect and mitigate emerging threats. Additionally, exploring blockchain-based solutions for enhancing data privacy and implementing decentralised access controls can address limitations in current security models. As regulatory requirements evolve, further studies are needed to evaluate the effectiveness of compliance mechanisms and their integration into SaaS security strategies. Finally, collaborative efforts between academia and industry will be crucial to drive innovation in creating more resilient and secure cloud-based applications.

References

[1] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*. 2016. doi: 10.1201/9781439806814.

[2] H. Gupta and D. Kumar, "Security threats in cloud computing," in *2019 International Conference on Intelligent Computing and Control Systems, ICCS 2019*, 2019. doi: 10.1109/ICCS45141.2019.9065542.

[3] V. Kumar and F. T. S. Chan, "A superiority search and optimisation algorithm to solve RFID and an environmental factor embedded closed loop logistics model," *Int. J. Prod.*

Res., vol. 49, no. 16, 2011, doi: 10.1080/00207543.2010.503201.
[4] S. G and M. S, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions," *Int. J. Cloud Comput. Serv. Archit.*, vol. 3, no. 4, pp. 1–11, 2013, doi: 10.5121/ijccsa.2013.3401.
[5] A. A., "Enhancing Elasticity of SaaS Applications using Queuing Theory," *Int. J. Adv. Comput. Sci. Appl.*, 2017, doi: 10.14569/ijacsa.2017.080136.
[6] P. Srivastava and R. Khan, "A Review Paper on Cloud Computing," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2018, doi: 10.23956/ijarcsse.v8i6.711.
[7] V. V. Kumar, F. W. Liou, S. N. Balakrishnan, and V. Kumar, "Economical impact of RFID implementation in remanufacturing: a Chaos-based Interactive Artificial Bee Colony approach," *J. Intell. Manuf.*, 2015, doi: 10.1007/s10845-013-0836-9.
[8] V. V. Kumar, M. K. Pandey, M. K. Tiwari, and D. Ben-Arieh, "Simultaneous optimization of parts and operations sequences in SSMS: A chaos embedded Taguchi particle swarm optimization approach," *J. Intell. Manuf.*, 2010, doi: 10.1007/s10845-008-0175-4.
[9] R. P. Padhy and M. R. Patra, "Evolution of Cloud Computing and Enabling Technologies," *Int. J. Cloud Comput. Serv. Sci.*, 2012, doi: 10.11591/closer.v1i4.1216.
[10] V. V Kumar, M. Tripathi, M. K. Pandey, and M. K. Tiwari, "Physical programming and conjoint analysis-based redundancy allocation in multistate systems: A Taguchi embedded algorithm selection and control (TAS&C) approach," *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.*, vol. 223, no. 3, pp. 215–232, Sep. 2009, doi: 10.1243/1748006XJRR210.
[11] C. S. Yoo, "Cloud Computing: Architectural and Policy Implications," *Rev. Ind. Organ.*, 2011, doi: 10.1007/s11151-011-9295-7.
[12] V. V. Kumar, F. T. S. Chan, N. Mishra, and V. Kumar, "Environmental integrated closed loop logistics model: An artificial bee colony approach," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.
[13] V. V. Kumar, S. R. Yadav, F. W. Liou, and S. N. Balakrishnan, "A digital interface for the part designers and the fixture designers for a reconfigurable assembly system," *Math. Probl. Eng.*, 2013, doi: 10.1155/2013/943702.
[14] V. V. Kumar, A. Sahoo, and F. W. Liou, "Cyber-enabled product lifecycle management: A multi-agent framework," in *Procedia Manufacturing*, 2019. doi: 10.1016/j.promfg.2020.01.247.
[15] V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, "Warranty failure analysis in service supply Chain a multi-agent framework," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.
[16] P. Mell and T. Grance, "The NIST definition of cloud computing," in *Cloud Computing and Government: Background, Benefits, Risks*, 2011. doi: 10.1016/b978-0-12-804018-8.15003-x.
[17] V. V Kumar, M. Tripathi, S. K. Tyagi, S. K. Shukla, and M. K. Tiwari, "An integrated real time optimization approach (IRTO) for physical programming based redundancy allocation problem," *Proc. 3rd Int. Conf. Reliab. Saf. ...*, no. August, 2007.
[18] V. V Kumar, "An interactive product development model in remanufacturing environment : a chaos-based artificial bee colony approach," 2014.
[19] M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.
[20] S. K. R. Anumandla, V. K. Yarlagadda, S. C. R. Vennapusa, and K. R. V Kothapalli, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," *Technol. \& Manag. Rev.*, vol. 5, no. 1, pp. 45–65, 2020.
[21] S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, "Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement," *Technol. Manag. Rev.*, vol. 3, no. 1, pp. 46–62, 2018.
[22] C. L. Devi, D. Kanyakumari, and K. Venkataramana, "Security issues in SaaS of cloud computing," *Int. J. Sci. Eng. Res.*, vol. 8, no. 5, pp. 34–40, 2017.
[23] M. A. Shajahan, N. Richardson, N. Dhameliya, B. Patel, S. K. R. Anumandla, and V. K. Yarlagadda, "AUTOSAR Classic vs. AUTOSAR Adaptive: A Comparative Analysis in Stack Development," *Eng. Int.*, vol. 7, no. 2, pp. 161–178, Dec. 2019, doi: 10.18034/ei.v7i2.711.
[24] V. K. Yarlagadda, S. S. Maddula, D. K. Sachani, K. Mullangi, S. K. R. Anumandla, and B. Patel, "Unlocking Business Insights with XBRL: Leveraging Digital Tools for Financial Transparency and Efficiency," *Asian Account. Audit. Adv.*, vol. 11, no. 1, pp. 101–116, 2020.
[25] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.
[26] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of elevator controllers for energy efficiency," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2012. doi: 10.1109/ISCE.2012.6241747.
[27] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of intelligent controllers for elevator energy efficiency," in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.
[28] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.
[29] M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, "Performance evaluation of energy efficient intelligent elevator controllers," in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.
[30] R. Goyal, "THE ROLE OF BUSINESS ANALYSTS IN INFORMATION MANAGEMENT PROJECTS," *Int. J. Core Eng. Manag.*, vol. 6, no. 9, pp. 76–86, 2020.
[31] M. Gopalsamy, "Artificial Intelligence (AI) Based Internet-ofThings (IoT)-Botnet Attacks Identification Techniques to Enhance Cyber security," *Int. J. Res. Anal. Rev.*, vol. 7, no. 4, pp. 414–420, 2020.
[32] A. Kumar, R. Garine, A. Soni, R. K. Arora, R. C. Dublin, and I. Researcher, "Leveraging AI for E-Commerce Personalization : Insights and Challenges from 2020," pp. 1–6, 2020.
[33] R. K. A. Sanjay Sharma, Munish Gupta, Ajay Kumar, *Risk assessment exposure to radon concentration and heavy metal contamination in drinking water samples in some areas of Jammu and Kashmir, India*. 2012.

[34] A. S. Ramakrishna Garine, Rajeev Arora, Anoop Kumar, "Advanced Machine Learning for Analyzing and Mitigating Global Supply Chain Disruptions during COVID-19," *SSRN*, pp. 1–6, 2020.

[35] P. Xu, Y. Zhang, and K. Shuang, "Log on Cloud: A SaaS Data Collection, Storage, and Analysis Framework," in *Proceedings - 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, DASC 2016, 2016 IEEE 14th International Conference on Pervasive Intelligence and Computing, PICom 2016, 2016 IEEE 2nd International Conference on Big Data*, 2016. doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.151.

[36] O. Akinrolabu, S. New, and A. Martin, "Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study," in *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*, 2019. doi: 10.1109/CSCloud/EdgeCom.2019.00-14.

[37] R. Lopez-Viana, J. Diaz, V. H. Diaz, and J. F. Martinez, "Continuous Delivery of Customized SaaS Edge Applications in Highly Distributed IoT Systems," *IEEE Internet Things J.*, 2020, doi: 10.1109/JIOT.2020.3009633.

[38] F. Ghaffari, H. Gharaee, and M. R. Forouzandehdoust, "Security considerations and requirements for Cloud computing," in *2016 8th International Symposium on Telecommunications, IST 2016*, 2017. doi: 10.1109/ISTEL.2016.7881792.

[39] L. B. Bhajantri and T. Mujawar, "A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures," in *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, 2019. doi: 10.1109/I-SMAC47947.2019.9032545.