Analysis of Load Balancing Techniques in Cloud Computing

Nisha Sharma, Khushboo Saifi, Parul Nain, Dr Sachin Sharma
Faculty of Computer Applications, Manav Rachna International
Institute of Research & Studies, Faridabad-121001, India

Abstract: Cloud computing is a method to upsurge the volume or enhance the potential vigorously without capitalizing on a new structure or buying new software. It can also be defined as the distribution of computing facilities including storage, databases, servers, networking and numerous more for the connected cloud. Cloud computing nowadays is growing at a faster pace and has become the most developing component of the IT Industry. But as more and more data of companies or individuals are added to the cloud the concern of data security remains an issue, therefore it is very vital to assure the safety and confidence to share the data for evolving cloud computing applications. In this paper, we will show the different types of computing platforms also we have debated security dangers and worries in cloud computing as well as important stages that an individual can take to remove the safety risks or how can one secure their data. This paper also solves the significant aspect of security-related challenges that scholars and researchers are confronting in the security of cloud computing.

Index Terms: Cloud Computing, Software, Platform, Infrastructure. Load Balancing

1. Introduction

These days cloud computing is growing at a very faster pace and have expanded substantially in the last few years (roughly 2 decades) and there is still a lot more for the cloud computing business to expand? In. Cloud computing is a facility that provides various resources and services to its customers over the Internet with reduced complexities. All the services such as data storage, management and sharing facilities, software requirements in different business streams such as messaging software, E-mail management Software, enterprise resource planning (ERP), documentation management and SaaS (services of SaaS model), Develop, run and manage applications (services of PaaS model) and Virtual hardware facilities (services of IaaS model).

Today all the companies in the IT sector as well as other areas (on demand) have realized that by Incorporating the use of cloud services into their streams will reduce their respective workload by a great margin and that they can reach a new level of excellence just by this one small step that too at the insignificant rate.

According to Gartner cloud computing is basically a type of computing where the proficiencies of IT industry are delivered as a service to customers over the Internet.

With tremendous growth comes the heavy duties of providing these services accurately and ensuring the customers of their integrity check, customers must be ensured that their confidentiality is take care of. According to the IDCI survey (2010), security is the major concern that holds back almost 74% of the IT executives and CIO’s from adopting cloud service models [1] (SAAS, PAAS and IAAS).

The international market of cloud computing is estimated to nurture rapidly within a few years, having such potential for its growth it is important for the cloud computing business that it must address the challenges that are obstacles in its

path towards success. All the data that is given to the cloud by its various users is then moved towards the large data hubs, where data tampering is one of the issues and hence management and storage are not trustworthy. The different security problems include Physical access issues, Access susceptibilities, web application exposures such as physical control of data and cross-site scripting, confidentiality and control issues, structured Query Language injection, matters linked to identity and credential administration, and subjects related to data authentication

, tampering, integrity, data loss, confidentiality and theft; all these problems are encompassed in the following fundamental security issues - application security, Security associated with third-party resources, data storage safety and data transmission security.

This research thus explains various security subjects in cloud computing service models namely Platform as a Service (PAAS), Software as a Service (SAAS), Infrastructure as a Service (IAAS), then gives the current possible ways that address them and make the cloud services free from them as much as possible.

2. Background

There are namely three broad categories under which cloud computing services are classified: -

Infrastructure as a Service, Platform as a Service and Software as a Service.

Service Models: -

a. Software as a Service (SAAS)

SAAS can be defined as distributing software applications over the internet. This type of computing does not require users to install applications on their devices or servers. The application resides on a distant cloud system which can be accessed through the website or an API request. With the support of the application on their devices, the user can store, modify or analyze data and collaborate on projects [2].

b. Platform as a Service (PAAS)

PAAS is interpreted as a platform facility that utilizes tools and methods used to develop and host applications in the same surroundings in which it is made. It can also be defined as an environment where users can manage their applications. Along with this, they can also test their applications for which there are inbuilt tools for enhancement, customize and many more functions [2].

c. Infrastructure as a Service (IaaS)

IAAS is computing facilities where the vendor delivers admittance to various services like storage networks, servers and their platform which can be used for the same purpose for example organizations use their network for the same. It also permits the administrative tasks to be done virtually hence providing time for additional tasks [2].

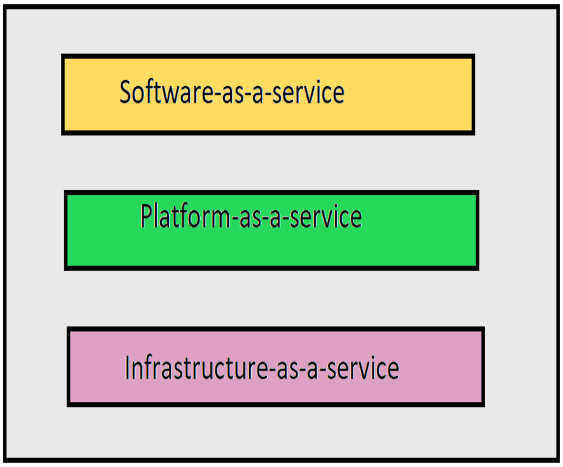

Figure1. Cloud layers and access technologies

Load balancing is a crucial aspect of cloud computing and machine learning systems [3]-[5] as it ensures that resources are allocated efficiently to meet the demand for computing power. In machine learning systems [6]-[11], load balancing can be achieved through techniques such as model parallelism, data parallelism [12] [13], and hybrid parallelism.

3. Security Issues in Cloud Computing

As we have discussed above the cloud provides three services, SAAS, PAAS and IAAS, there are security issues with them too. To mitigate these security issues, cloud computing providers and Android users can take measures such as implementing multi-factor authentication, encryption, regular security audits, and keeping software up to date [14]-[19]. SAAS posses' high level of desegregated utility but nominal client authority or flexibility. As opposed to SAAS, PAAS possesses high flexibility as well as high client authority. It is due to a relatively lower level of generalization, IAAS provides more client authority over security than other two services. Before going further, we must understand the reliance of one on another. IAAS host both SAAS and PAAS, as a result, any contravention in IAAS will lead to security city issues in the rest. PAAS gives a platform for SAAS for developing app applications we see here that strike against any of the service layer will majorly affect other layers too. This reliance may lead to security hazards. We are going to discuss various security issues regarding these services [2].

a. Security issues in Software as a Service (SAAS)

Users of Software as a service have small command over security in comparison to other proposed services. Therefore, usage may lead to severe security distresses.

i. Application Security

These applications are typically derived from the network through a Browser [20]-[23]. Yet, blemishes in these types of web applications can generate exposure for the SAAS applications. Strikers use the web as a way towards getting into clients' computers and perform spiteful activities like stealing someone's important or secretive data. However, security provocations in these applications are not so dissimilar to website applications but then again preventive measures for web applications cannot effectively protect SAAS applications, therefore, other measures were needed.

ii. Multi tenancy

Software as a service application might be grouped into developed models that are resolved by following characteristic—configurability, scalability through meta-data and multi-tenancy. The security issues are worse in the second and third model than in the first model. In the third model, multi-tenancy is added that means a sole existence helps every client hence increasing resource efficiency. As data from various occupants are stored in the same database therefore chances of data leakage among them are very high. The client's data should be kept secured from other clients.

iii. Data security

Securing data is a major worry in every application. Clients rely on SAAS providers for security. However, backups are also created in order to recover data in damage cases but that too has security matters. Most agreed upon standards do not envision compliance with guidelines in the world of cloud computing. SaaS can cause compliance issues which are security, segregation and data privacy.

iv. Accessibility

Accessing applications allows access to any network device but welcomes security hazards too. Programs can access any network device, but doing so exposes you to security hazards. The present condition of mobile computing is covered in a study by the Cloud Security Alliance; along with the biggest threats in this area include operating system flaws, insecure Wi-Fi networks, information-stealing mobile malware, unsafe marketplaces, and hackers.

b. Platform-as-a-service (PAAS)

PAAS application safety issues comprise of two software layers i.e., the security of client's applications on the PAAS platform and the security of Platform as a service platform. Providers of Platform service applications are accountable for the security.

i. Third-party relationships

PAAS causes security issues due to mash up where mash up means merging several source elements into one integrated unit. PAAS has to rely on the development tools hosted by the web as well as on the third-party relationships.

ii. Underlying Infrastructure security

Providers have to take care of the security measures because developers are not allowed to access the underlying infrastructure security. Even when the applications are developed by the developers and they assure everything related to it, they still can't assure the security of development environment tools. These tools are offered by PAAS for the creation of SAAS applications.

c. Infrastructure-as-a-service (IAAS)

Numerous resources, including storage, servers, networks, and other computing resources, are delivered as a virtualized system through the internet using infrastructure as a service. It is considered one of the best in terms of security from other two models. However, security issues can arrive if there's any problem in the virtual machine. Threats arise because of communication, creation, modification and mobility.

Security issues due to IAAS are described below.

i. Virtual machine

Users can execute a variety of programmed by using virtualization, which enables them to build, clone, share, migrate, and roll back virtual computers [24]. But virtualization allows assailants security problems because of the creation of extra layers. Virtualization provides virtualized environment is beneficial but on the other hand causes malicious security risks too.

ii. Virtual Networks

As a part of IAAS, resource pooling allows various tenants to share the same network components and this component sharing allows attackers to launch cross-tenant attack. The safest way is to repair each virtual machine along with its host using physical channels.

Bridged and routed virtual network configurations increase the changes of sniffing and spoofing virtual networks.

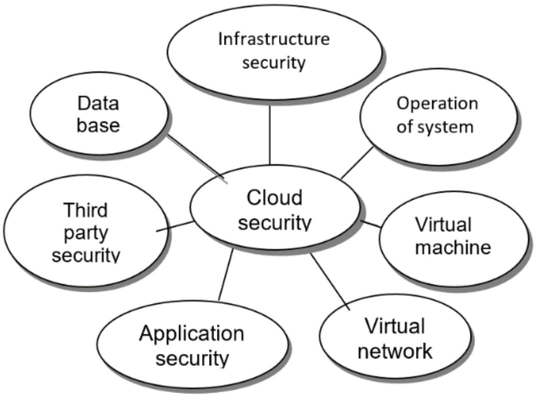

Figure 2. Cloud security issues

4. Threats in cloud computing [15]

a. Account or service hijacking

If we have weak credentials, then there are high chances of account theft and hijacking, it can also be done by social engineering. As a result, attacker ultimately gains access to the personal sensitive data of users and hence changes it for its malicious purposes such as to redirect any transaction.

b. Data Scavenging

Until the device is destroyed the data remains on it in the same way which can be accessed by attacks .

c. Data Leakage

Data may get into wrong hands either due to weak security measures due to technical tricks of attackers when it is being stored, processed or transferred among users.

d. Denial of Service Attack (Dos)

An attacker may gain control over all the Services on a system hence making its legitimate user not able to access the resources.

e. Data manipulation

Web applications are attacked through the tampering of information directed from their application's component towards the server's application component.

f. VM Escape

Virtual machine disappearance exploits the hypervisor and takes charge of given infrastructure.

g. VM Hopping

A Virtual machine increases admittance to another VM hypervisor vulnerability exploitation.

h. Sniffing/spoofing virtual Networks

Malevolent virtual machine redirects packages to virtual by listening to the virtual machines.

5. Vulnerabilities in Cloud Computing

a. Insecure interfaces and API's:

Cloud Services are offered through API's and security largely determined by these interfaces: Problems arises due to Weak Credentials: Insufficient authorization checks and Insufficient input data validation.

b. Unlimited allocation of resources: Overbooking or over provisioning due to inaccurate resource usage.

c. Data related Vulnerabilities:

i. Data backlogs are done by Data-related providers whore, not trusted to be completely removed due to incomplete elections.

ii. Data is allocated to different jurisdiction having different rules.

iii. Customers do not know where the data belonging to them is [2].

d. Vulnerabilities in Virtual Machines

Allocation and de-allocation are not restricted for resources with VM's.

VM's IP address are not hidden within the cloud hence attacker can map target VM 's location.

Data Leakage is possible due to flexibility of VM's to be copies (uncontrolled snapshots).

6. Current security measure/counter measure

There are various developments going on in the concern of solutions regarding the cloud security issues there are various group and organizations that are interested in making the cloud services safer by providing some standards. The Cloud security alliance (CSA) has gathered interested organizations and individuals for this purpose.

a. Resource Isolation

For safer data during processing resources should be isolated.

b. Encrypted Protocols

It must be used as much as possible to avoid TP spoofing.

c. Dynamic Credential [25]

When the user's position changes or a certain number of data packets have been transmitted, these changes happen.

d. Fragmentation redundancy -scattering (FRS) technique [26]

Fragile information is segregated in inconsequential pieces.

Across different sites of the distributed system, these fragments are scattered showing redundancy.

This provides security for storage and intrusion tolerance.

e. Digital Signatures [26]

Data is secured using digital signatures.

f. Homomorphism encryption

This permits simultaneous calculation on coded message without being exposed.

g. Encryption

It ensures the security of sensitive data. It can moreover be utilized to halt side channel assaults on cloud capacity de-duplication but offline dictionary attacks may occur exposing individual keys [2].

h. Web application Scanner

It provides scanning of web applications for identifying the possible security vulnerability.

i. Development Framework

It should have taught security architecture as a security for a web application.

j. Accessibility vulnerabilities

For this purpose, one should close the idle services, keep patches upgraded and access to rights of applications and clients ought to be decreased.

Table 1.Cloud software issues and their solutions.

SOFTWARE	PROBLEMS	SOLUTIONS
1. Software as a services (SAAS)	• Application security • Multi-tenancy • Data Security	• Encryption protocol • Virtual private cloud • Data masking
2.Platform as a services (PAAS)	• Third-party relationship • Underlying infrastructure security	• Resource location • Development framework
3.Infrastructure as a service (SAAS)	• Virtual machine • Virtual network	• Encryption • Dynamic Credential

7. Load Balancing in Cloud Computing

Load balancing can be defined as an approach of scheduling tasks among nodes with effective utilization and resource monitoring as its main objective.

An algorithm for is measured efficient at the time it is working against faults as well as it is expandable and is guaranteeing to produce highest throughput.

There exist various categories of load balancing algorithms today as given below [27].

a. Static Load Balancing

This type of load balancing technique is usually non-pre-emptive in nature and has predefined set of rules that must be followed according to the given input. This technique requires knowledge about resource available and setup of system.

Some of the examples for this technique includes central manager, two phase scheduling, artificial bee colony search etc.

b. Dynamic Load Balancing

This type of balancing technique is usually pre-emptive in nature and not have the requirement of input knowledge. It basically depends on system's current state and hence, increases overall working. Some of the examples for this technique includes round-robin algorithm, throttled load balancing algorithm, artificial ant colony search etc.

7.1 Load Balancing Optimization Algorithms

This segment is showing reviews on different optimization algorithms of load balancing. This shows different behaviors to tackle large amount of data.

a. Throttled Load Balancing Algorithm

This algorithm is based on the current state of virtual managers. If any VM is in availability, the request will be allotted else request is dismissed. In [1], Author has made the comparison between throttled algorithm and round robin in terms of cost used

and time. Throttled is considered superior in terms of cost as reduced virtual machines per hour usage.

b. Ant Colony Optimization Algorithm

Ant Colony Optimization has been defined as a probabilistic technique algorithm to find the optimal path. It follows the ant behavior for solving the optimization issue. When ants are hungry, they secrete pheromone named chemical trail. Other ants follow the trail with higher pheromone scent. In , the author has shown that this similar phenomenon is used for allocating the tasks. Task Scheduler along with resource manager monitors resources and task allocation flow.

c. Honeybee Optimization Algorithm

This optimization algorithm of load balancing basically, follows the honeybee behavior. Honey bees are of two categories: There is a discoverer

one that searches the food and passes the information of food source to the other bees who follows the pathway directed to them by the discoverer honeybee. Discoverer honeybees then perform the famous waggle dance. The dance that is being performed by them shows the value and amount of food and span of the dance tells us about how far is food from the beehive [28]. In this paper [29] a upgraded version of honeybee algorithm is being proposed as the basic algorithm might generate disproportion of load between the nodes. In this upgraded algorithm, it is proposed that a minimum value is there for every server and when the length of server surpasses that value, load is shifted on separate one, and are carried out separately also upgrading the throughput of the system.

d. Genetic Algorithm

This algorithm is the key algorithm for optimization. Genetic algorithm basically follows the idea of how the biological population is generated. As per Darwin’s Theory, the term “Survival of the fittest” explains that how the tasks scheduling is done and how the tasks are assigned to the resources according to the fitness function value of every parameter [30]. The main fundamentals of genetic algorithm are: First of all, it initializes the population, then evaluates the fitness, then the selection process occurs and after that crossover and mutation happens. The new population is added to the old population. This is main aim of genetic algorithm and this is the main idea in [31] which shows how the load is balanced using genetic algorithm.

e. Generalized Priority Task Scheduling Algorithm

Generally, priority is an important issue in task scheduling in cloud environments. In this algorithm it is proposed that those tasks are given priority first which have the large size. Higher the size of the task is, highest will be their rank in priority.

VMs are also prioritized but they are ranked on the basis of their Million Instructions per second (MIPS) value. VM will be ranked highest, if their MIPS is higher.

f. Agent-Based Load Balancing

In conventional load balancing, load balancers focus on allocating task to the right servers in order to prevent a system from becoming overloaded. A mobile agent, an independent software programmer that runs on behalf of the network user, is used in this load balancing strategy. Within two walks, this agent completes one walk. Firstly, it collects all data on the servers' status using an average task computation, and then secondly, it examines the servers' overloaded and under loaded conditions. The agent used in load balancing enhances the system's throughput and reaction time [13].

MEASURES	DTFT (junaid, sohail, rais,2020	Bayes net (Çigs¸ar & Ünal, 2019)	ACOFTF (Junaid, Sohail, Ahmed, et al., 2020)	CA-MLBS (2022)	Multi class (2020)	J48 (2020)

The effectiveness of load balancing is measured by a number of variables, including throughput, processing time, response time, etc. The strategy will be more effective the faster the task is completed. The features of the task are assessed during allocation and processing time in estimated finish time task scheduling [14], which improves performance and resource utilization by ensuring the maximum use of virtual machines. This prevents blocking of processes in queues. It also estimates the task's finish time earlier during allocation.

Table 2. Analysis of various load balancing algorithms

Metrics	Throughput	Scalability	Response time	Processing time	System stability	Cost	Performance	Resource utilization
Throttled Algorithm	X	X	✓	✓	X	✓	X	X
Ant colony optimization	X	X	X	X	X	X	✓	✓
Honeybee foraging	✓	✓	X	X	✓	X	X	X
Genetic algorithm	X	X	X	X	✓	X	✓	✓
Generalized Priority	✓	X	X	X	X	X	X	✓
Agent-based scheduling	✓	X	✓	X	X	✓	X	X
Estimated finish time	X	X	X	X	X	X	✓	✓

7.2. Performance Analysis

Various research papers have been studied for finding the load balancing. The table below shows a comparative study of existing methods on various metrics such as precision, accuracy, recognition value, and F-measure. It was concluded from the comparative table that CA-MLBS algorithm gives the best accuracy as compared to other techniques for load balancing [32]-[34].

Table 3: Classification results for accuracy, recall, precision, and F-measure

Accuracy	0.974	0.825	0.984	0.988	0.96	0.824
Precision	0.963	0.814	0.959	0.968	0.96	0.818
Recall	0.951	0.814	0.973	0.979	0.96	0.825
F-measure	0.977	0.824	0.966	0.988	0.97	0.821

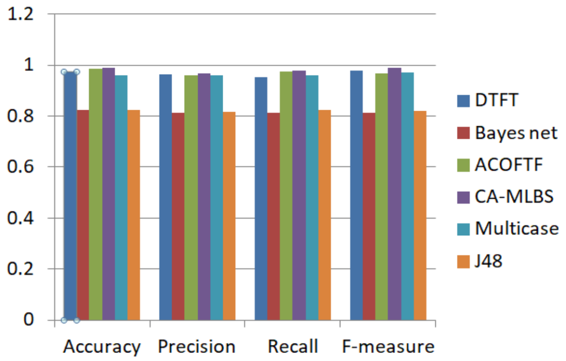

Figure 3: Comparative study of exiting methodologies

8. Conclusion

We have seen that cloud computing has shown rapid growth in the last decade and still has a great potential in growing. But to achieving these higher levels and exercise potential cloud computing business needs to first avoid its flaws and its challenges. For this it has to come up with appropriate solutions. We have seen various problems in this paper and how they are affecting the cloud market value and goodwill. Though it provides various benefits to users it also raises some security issues which threaten many users and leading to slow down of its use. Understanding the current threat that it possesses to the users who are still reluctant the cloud services usage will greatly help the cloud computing business to expand which not only benefits the cloud but also provides benefits in every way. As discussed, virtualization, storage and networks are the greatest problems in it.
There are some current solutions listed here as well, but new security technology is also required, along with updated conventional solution that can function with cloud architecture. If these loose ends of the security will be addressed and rectified then cloud will grow more rapidly. In addition to these service providers, users are also required to be aware and use the various services provided by the cloud by paying attention to everything. The users must be vigilant about providing their credentials and related sharing of such data. Our research paper is intended to cater to the current problem in the cloud computing service providers as well as how to avoid them.

The researchers have put forth a variety of load balancing strategies for efficient and consistent execution. According to the analysis, different algorithms operate on various factors, but none of them operate when all the parameters are taken into account. All of the suggested algorithms are effective in some way. We have performed a comparative analysis of various existing methodologies to find out which provides best accuracy on load balancing. We got to the conclusion that CA-MLBS algorithm exceeds other algorithms.

References

[1] H. Shoja, H. Nahid, and R. Azizi, “A comparative survey on load balancing algorithms in cloud computing,” in Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Jul. 2014, pp. 1-5. doi: 10.1109/ICCCNT.2014.6963138.
[2] “Top 11 cloud security challenges and how to combat them | TechTarget,” Security.

https://www.techtarget.com/searchsecurity/tip/Top-11-cloud-security-challenges-and-how-to-combat-them (accessed Apr. 15, 2023).

[3] K. Aggarwal, S. K. Singh, M. Chopra, S. Kumar, and F. Colace, “Deep Learning in Robotics for Strengthening Industry 4.0.: Opportunities, Challenges and Future Directions,” in Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities, N. Nedjah, A. A. Abd El-Latif, B. B. Gupta, and L. M. Mourelle, Eds., in Studies in Computational Intelligence. Cham: Springer International Publishing, 2022, pp. 1-19. doi: 10.1007/978-3-030-96737-6_1.

[4] M. Chopra, S. K. Singh, K. Aggarwal, and A. Gupta, “Predicting Catastrophic Events Using Machine Learning Models for Natural Language Processing,” Data Mining Approaches for Big Data and Sentiment Analysis in Social Media, 2022. https://www.igi-global.com/chapter/predicting-catastrophic-events-using-machine-learning-models-for-natural-language-processing/www.igi-global.com/chapter/predicting-catastrophic-events-using-machine-learning-models-for-natural-language-processing/293158 (accessed Dec. 17, 2022).

[5] I. Singh, S. K. Singh, R. Singh, and S. Kumar, “Efficient Loop Unrolling Factor Prediction Algorithm using Machine Learning Models,” in 2022 3rd International Conference for Emerging Technology (INCET), May 2022, pp. 1-8. doi: 10.1109/INCET54531.2022.9825092.

[6] S. Gupta, S. Agrawal, S. K. Singh, and S. Kumar, “A Novel Transfer Learning-Based Model for Ultrasound Breast Cancer Image Classification,” in Computational Vision and Bio-Inspired Computing, S. Smys, J. M. R. S. Tavares, and F. Shi, Eds., in Advances in Intelligent Systems and Computing. Singapore: Springer Nature, 2023, pp. 511-523. doi: 10.1007/978-981-19-9819-5_37.

[7] Xu, Z., He, D., et al. (2021). Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical wsns. IEEE Journal of Biomedical and Health Informatics.

[8] A. Mishra (2023) Homomorphic Encryption: Securing Sensitive Data in the Age of Cloud Computing, Insights2techinfo, pp.1, https://insights2techinfo.com/homomorphic-encryption-securing-sensitive-data-in-the-age-of-cloud-computing/

[9] Al-Qerem, et al. (2020). IoT transaction processing through cooperative concurrency control on fog-cloud computing environment. Soft Computing, 24(8), 5695-5711.

[10] G. Mengi, S. K. Singh, S. Kumar, D. Mahto, and A. Sharma, “Automated Machine Learning (AutoML): The Future of Computational Intelligence,” in International Conference on Cyber Security, Privacy and Networking (ICSPN 2022), N. Nedjah, G. Martínez Pérez, and B. B. Gupta, Eds., in Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 2023, pp. 309-317. doi: 10.1007/978-3-031-22018-0_28.

[11] F. J. G. Peñalvo et al., “Sustainable Stock Market Prediction Framework Using Machine Learning Models,” Int. J. Softw. Sci. Comput. Intell. IJSSCI, vol. 14, no. 1, pp. 1-15, Jan. 2022, doi: 10.4018/IJSSCI.313593.

[12] S. Kumar, S. Kr. Singh, N. Aggarwal, and K. Aggarwal, “Evaluation of automatic parallelization algorithms to minimize speculative parallelism overheads: An experiment,” J. Discrete Math. Sci. Cryptogr., vol. 24, no. 5, pp. 1517-1528, Jul. 2021, doi: 10.1080/09720529.2021.1951435.

[13] S. Kumar, S. K. Singh, N. Aggarwal, B. B. Gupta, W. Alhalabi, and S. S. Band, “An efficient hardware supported and parallelization architecture for intelligent systems to overcome speculative overheads,” Int. J. Intell. Syst., vol. 37, no. 12, pp. 11764–11790, 2022, doi: 10.1002/int.23062.

[14] A. Sharma, S. K. Singh, S. Kumar, A. Chhabra, and S. Gupta, “Security of Android Banking Mobile Apps: Challenges and Opportunities,” in International Conference on Cyber Security, Privacy and Networking (ICSPN 2022), N. Nedjah, G. Martínez Pérez, and B. B. Gupta, Eds., in Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 2023, pp. 406–416. doi: 10.1007/978-3-031-22018-0_39.

[15] Yadav, U. S.,et al. (2022). Security and privacy of cloud-based online online social media: A survey. In Sustainable management of manufacturing systems in industry 4.0 (pp. 213-236). Cham: Springer International Publishing.

[16] Gaurav A. (2022) Cloud Computing and IT Industry, Insights2Tecinfo, pp.1 https://insights2techinfo.com/cloud-computing-and-it-industry/

[17] Gupta, B. B., Yamaguchi, S., & Agrawal, D. P. (2018). Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimedia Tools and Applications, 77, 9203-9208.

[18] Stergiou, C. L., et al. (2021). InFeMo: flexible big data management through a federated cloud system. ACM Transactions on Internet Technology (TOIT), 22(2), 1-22.

[19] M. Singh, S. K. Singh, S. Kumar, U. Madan, and T. Maan, “Sustainable Framework for Metaverse Security and Privacy: Opportunities and Challenges,” in International Conference on Cyber Security, Privacy and Networking (ICSPN 2022), N. Nedjah, G. Martínez Pérez, and B. B. Gupta, Eds., in Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 2023, pp. 329–340. doi: 10.1007/978-3-031-22018-0_30.

[20] J. Grover and S. Katiyar, “Agent based dynamic load balancing in Cloud Computing,” in 2013 International Conference on Human Computer Interactions (ICHCI), Aug. 2013, pp. 1-6. doi: 10.1109/ICHCI-IEEE.2013.6887799.

[21] Quamara, M., et al. (2019, October). MQTT-driven remote temperature monitoring system for IoT-based smart homes. In 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE) (pp. 968-970). IEEE.

[22] Casillo, M., et al., (2021). Fake News Detection Using LDA Topic Modelling and K-Nearest Neighbor Classifier. In Computational Data and Social Networks: 10th International Conference, CSoNet 2021, Virtual Event, November 15–17, 2021, Proceedings 10 (pp. 330-339). Springer International Publishing.

[23] Zhou, L., et al. (2022). Panner: Pos-aware nested named entity recognition through heterogeneous graph neural network. IEEE Transactions on Computational Social Systems.

[24] 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, p. 5, Feb. 2013, doi: 10.1186/1869-0238-4-5.

[25] "Top Threats Working Group | CSA." https://cloudsecurityalliance.org/research/working-groups/top-threats/ (accessed Apr. 15, 2023).

[26] "Cloud Security and Privacy [Book]." https://www.oreilly.com/library/view/cloud-security-and/9780596806453/ (accessed Apr. 15, 2023).

[27] M. Junaid et al., "Modeling an Optimized Approach for Load Balancing in Cloud," IEEE Access, vol. 8, pp. 173208–173226, 2020, doi: 10.1109/ACCESS.2020.3024113.

[28] D. B. L.d. and P. Venkata Krishna, "Honey bee behavior inspired load balancing of tasks in cloud computing environments," Appl. Soft Comput., vol. 13, no. 5, pp. 2292–2303, May 2013, doi: 10.1016/j.asoc.2013.01.025.

[29] J. Yao and J. He, "Load balancing strategy of cloud computing based on artificial bee algorithm," in 2012 8th International Conference on Computing Technology and Information Management (NCM and ICNIT), Apr. 2012, pp. 185–189.

[30] K. Dasgupta, B. Mandal, P. Dutta, J. K. Mandal, and S. Dam, "A Genetic Algorithm (GA) based Load Balancing Strategy for Cloud Computing," Procedia Technol., vol. 10, pp. 340–347, Jan. 2013, doi: 10.1016/j.protcy.2013.12.369.

[31] "IJCTT - Efficient Optimal Algorithm of Task Scheduling in Cloud Computing Environment." https://ijcttjournal.org/archives/ijctt-v9p163 (accessed Apr. 15, 2023).

[32] "CA-MLBS: content-aware machine learning based load balancing scheduler in the cloud environment - Adil - 2023 - Expert Systems - Wiley Online Library." https://onlinelibrary.wiley.com/doi/full/10.1111/exsy.13150 (accessed Apr. 15, 2023).

[33] Negi, P., Mishra, A., et al. (2013). Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment. arXiv preprint arXiv:1304.7073.

[34] Gupta, B. B., Gupta, S., & Chaudhary, P. (2017). Enhancing the browser-side context-aware sanitization of suspicious HTML5 code for halting the DOM-based XSS vulnerabilities in cloud. International Journal of Cloud Applications and Computing (IJCAC), 7(1), 1-31.