Open Access Article

CLOUD COMPUTING DATA SECURITY CHALLENGES AND ALGORITHMS TO PROTECT SECURITY ISSUES

Dr. A. Kalaivani
Assistant Professor, Department of Computer Applications, Nehru Arts and Science College, Coimbatore.

Dr. S. Sangeetha
Head & Assistant Professor, Department of Information Technology,Sri Vasavi College(SFW), Erode.

Abstract

Cloud computing is a rapidly increasing technology that enables more efficient use of information technology infrastructure, services, and applications. It is an architecture for delivering computer services through the internet to a set of shared resources such as networks, storage, services, and applications. These clouds enable corporations, public and private organizations to optimize their capacities without incurring additional setup, staffing, or license expenditures. Due to the effectiveness of this system, which is based on a pay-per-use paradigm, numerous businesses such as banking, health care, geosciences, and education are embracing it. This article provides an overview of cloud computing and discusses its characteristics, services, and deployment approach. This article discusses the many advantages of cloud computing, as well as the associated problems and applications along with data security challenges and innovative Algorithms for security protections.

Keywords: Security Issues, Challenges, Cloud Data, Data Transmission, Securitycompliance.

抽象的

云计算是一种快速发展的技术，可以更有效地使用信息技术基础设施、服务和应用程序。它是一种通过互联网向一组共享资源（如网络、存储、服务和应用程序）提供计算机服务的架构。这些云使企业、公共和私人组织能够优化其容量，而不会产生额外的设置、人员配备或许可支出。由于这个基于按使用付费模式的系统的有效性，银行、医疗保健、地球科学和教育等众多企业都在接受它。本文概述了云计算，并讨论了它的特性、服务和部署方法。本文讨论了云计算的许多优势，以及相关的问题和应用，以及数据安全挑战和用于安全保护的创新算法。

关键词：安全问题、挑战、云数据、数据传输、安全合规。

I Introduction

Cloud computing services include software as a service (SaaS) and platform as a service (PaaS), to name a few of examples. In cloud computing, privacy protection is critical [2], and earlier encryption solutions have failed

Received: October 05, 2021 / Revised: October 31, 2021 / Accepted: November 30, 2021 / Published: December 31, 2021

About the authors：Dr. A. Kalaivani

Corresponding author- *Email:

to offer an adequate privacy protection mechanism for the cloud environment [3. The importance of personal or business information to cloud service customers cannot be overstated, even if the material's creator has no awareness that their content will be utilized for the advantage of others [4].

Privacy is not a huge problem in typical software development environments. In contrast, protecting individuals' privacy in cloud computing is a major concern at the moment because these materials are typically stored in an unencrypted form on a machine, but the materials' owner may include multiple organization operators, resulting in the disclosure of commercially sensitive information and the possible loss of privacy material [5]. As a result, protecting individuals is critical. When developing a cloud computing service system to handle information security problems, it is necessary to conduct a comprehensive evaluation of all factors and to increase user confidence in the legal system's conditions. The performance of the system must also be examined and measured at each step, as well as at the end of the process.

Cloud computing is an important application for Internet development because it processes and deposits data such as credit cards, account dense, and personal preference profiles, photo behavior calendar, financials, health, and other personal information, among other things. [7] The cloud provides services to users without allowing them access to hardware master control power. The absence of privacy protection that comes with cloud computing is the most significant disadvantage of the technology for both corporations and individuals. In many cases, this is the primary reason why businesses and people alike refrain from using cloud service solution packages. A reliable and effective test technique for the cloud computing material's privacy right system does not yet exist [2, despite the fact that cloud computing material security is increasing]. Aside from that, various kinds of cloud computing services need the implementation of a tailored data security protection solution. One of the primary goals of this study is to provide an analytical framework for cloud computing that will allow researchers to assess the fit and unfit quality relationships of material protection and determine which cloud computing service applications should be safeguarded. Deliberating on the fit-and-unfit quality connections of cloud computing service protection while developing an academic model for cloud computing privacy and material security. Which kind of news should be protected from being leaked? (4) The outcome of the analysis acts as a point of reference for future research and makes a contribution to the practical field.

II Related Works

In this part, we examine relevant works that addressed the topic of cloud security via the use of machine learning methods. An approach described by Khan et al. [15] addresses security flaws in the cloud system to improve its performance. The lack of interest in information persists as a result of the outsider's instability in storing, managing, and forming the information. Over the jumbled data, the scientists employed artificial neural networks (ANNs).

Khilar et al. [16] conducted an assessment of trust-based security risks and difficulties associated with cloud computing architectures. They described CC as an ad hoc processing condition to which hosts may allocate resources

at any moment and from any location. Thus, information is more flexible, unavoidable, and diverse as a consequence of this. As a safe approach for distributed computing systems, the authors proposed an access control paradigm based on trust.In order to provide an authorized client access to the cloud, and to pick an asset for computing, their notion is largely driven by this desire to offer access. The perceived trustworthiness of both clients and cloud assets is taken into account when making decisions.

The authors of [17] looked at cloud security issues and models in depth in [18]. According to the authors, distributed computing raises a unique set of security issues, and they looked at the resulting organizational mobility models. However, the critical progress of the cloud by itself results in the likelihood of considerable security. The process for relocating a model should not conflict with the required features and capabilities of the existing model. Another model devoted to increasing the presenting model's characteristics must not jeopardize or weaken other essential elements of the existing model.

Bhamare et al. [18] examined the use of machine learning models to enhance data security. Distributed computing was considered since it is gaining significant momentum and virtualized servers are becoming well-known as a feasible foundation and solution for massive corporate applications [19]. The researchers adopted an aid approach to address distributed computing security risks and protection problems [20]. They investigated fundamental dangers and protection concerns in distributed computing, as well as the merits and weaknesses of several current systems. The authors of [21] examined the CC threat categorization model's viability for detecting and resolving security concerns using machine learning methods. Additionally, they presented a strategy for categorizing CC risks based on the capability of using machine learning techniques to differentiate them. In CC, security risks and concerns were resolved using machine learning algorithms and protective measures [22].

Additionally, they found five noteworthy themes that demand scrutiny in the hunt for security vulnerabilities and defense methods for machine learning.Selamat et al. [23] investigated machine learning strategies for resolving malware security risks and CC security. The researchers presented a barrier framework that makes use of three machine learning algorithms and chose them based on their high-accuracy virus detection.In [24], Shamshirband et al. conducted a comprehensive study of frameworks for interruption recognition that make use of a computational insight approach. CC and MCC standard diagrams and management methodologies, as well as auditing security threats connected with these unique situations were also part of their study.

Prior research looked at cloud security concerns and threats through the lens of one or two machine learning methods. A number of machine learning approaches to cloud security concerns are examined in this article. Additionally, we examine several methods and determine which strategies are the most effective at resolving the problem. To conduct the primary comparison with other surveys and articles, we assess the problem and resolve the legal difficulties using a distinct supervised and unsupervised method.

Reference	Areas focused	Security Issues	ML Techniques	Impact in Cloud	Year
[26]	Security and threat issues	Yes	Supervised learning	Long term issues	2011
[24]	Trust based access control	No	Unsupervised learning	A few solutions accessible	2019
[28]	Cloud security	Limited	Unsupervised learning	Minor or intermediate issues	2018
[21]	Protection preserved encrypted data	Limited	Supervised and unsupervised learning	Minor or Intermediate Issues	2019
[27]	Security issues and datasets	Limited	Supervised learning	Minor or intermediate issues	2016
[29]	Cloud threats classification	No	Unsupervised learning	A few solutions accessible	2017
[25]	Security issues	Limited	Supervised and unsupervised learning	Minor issues	2020

Table1. Comparison of Related Research

III Security Levels in Cloud Computing

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

IVCloud ComputingOperation Principle

Software as a service (SaaS) is one of three main components of the cloud computing architecture, along with platform as a service (PaaS) and network infrastructure as a service (IaaS).

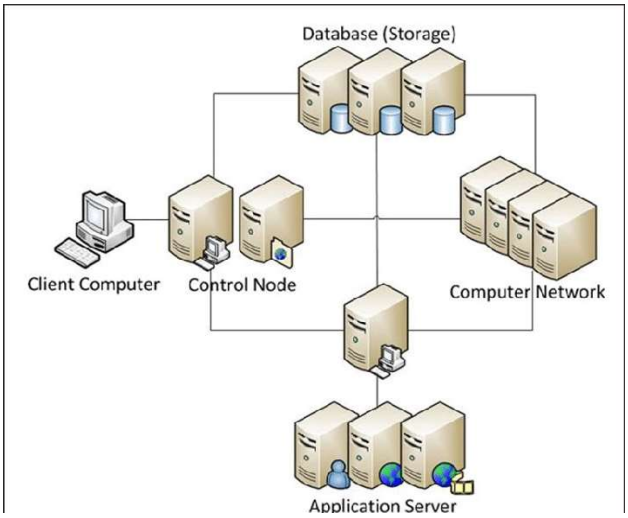

Fig 1 : Operation principles of Cloud Computing

V Optimization Model

Figure 3 Denotes a comparative analysis method to cloud computing optimization for processing privacy protection solutions and security issues; this model is built on that technique. In this study, a Global Authentication Register System (GARS) on third-party clouds of trust (TTP) is proposed, which offers a disposable registration certification service to both subscriber premises and clouds. However, the Public Cloud part establishes the right of privacy frame and model in the public cloud, and the encryption mechanism uses this study's GARS calculating method to process and protect the privacy material.

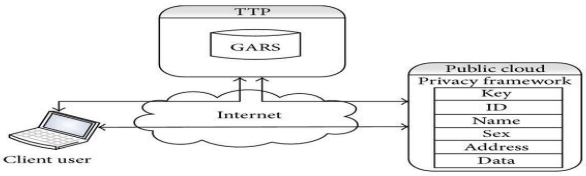

Fig 2 : Optimization Model for Cloud Computing

VI Data Transmission

When a user uploads files to a cloud storage server through the internet, a copy is made. When a user requests this information, they do it using a web-based interface. The server either returns the files to the user or permits direct access to them on the server. IaaS; provides a number of advantages but also some drawbacks. IaaS delivers infrastructure using virtual machines (VMs), yet VMs are becoming more outdated. This is because the cloud's capacity to provide security does not match the VM's ability to provide security. By agreeing on an erasure time frame, the customer and cloud provider may work together to overcome issues connected to deletion of data and other relevant issues. Compatibility concerns exist in IaaS due to the usage of outdated software by client-only apps, which might raise the price. Hypervisor security depends on dividing physical resources across VMs. An application service provider (ASP) provides a cloud-based platform for the creation and delivery of software applications. Interoperability, host vulnerability, privacy-aware authentication, service continuity, and fault tolerance are some of the security issues facing PaaS providers.

The client has to depends on the service provider for proper security measure and in

case of multi user don't gate to access the data of each other in order to maintain the security and assure that the applications will be available whenever that will be need. In SaaS software vender made the applications on its private server and deployed in cloud computing infrastructure service available by third party (Amazon, Google etc.) that can reduce the investment in infrastructure services and provide the better service to the customer how ever in SaaS model enterprises data is available at SaaS provider data center

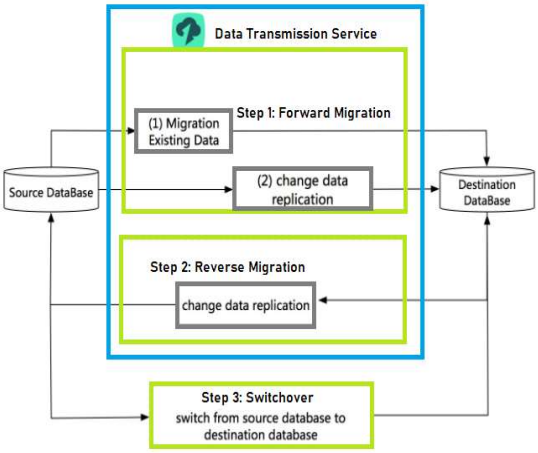

Fig 3 : Data Transmission Model

Communications takes a data transmission, splits it down into little parts, and transmits each bit via a channel one at a time. The receiver gathers the fragments and reassembles them to reconstruct the original message. Serial communication is the most prevalent mode of electronic device communication. Google Drive is a cloud storage service that enables you to store files online and access them from any smartphone, tablet, or computer. Additionally, Drive enables people to edit and contribute on files.The sensitive data of the various enterprises continue the reside within inside and the boundary of the cloud which is subject to which physical ,logical and personnel security and types of access control. In SaaS model the data is stored in a server and that can be transmit or can be communicate within the cloud. For these purpose security checks are essential to ensure the data security vulnerabilities in applications or through malicious employees. These force to develop security of the cloud data during transmission and face to challenges.

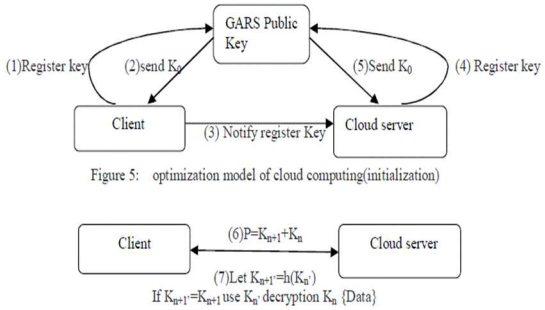

Fig 4 : Optimization of Cloud Computing

Cloud Models	Pros	Cons
Community	• More flexible and scalable • More secure than public cloud	• Organization • Data segregation
Public	• High Scalability • Reliability • Flexibility	• Less customizability • Less secure
Hybrid	• High scalability • More	• Security compliance • Infrastructure dependent

	flexible • Low cost • More secure	
Private	• More control • More reliable • Cost and energy efficient • High security and privacy	• Scalability • Security breaches • Lack of visibility • Limited services • Data loss

Table 2: Comparison of cloud models

VII TypesofAlgorithms

The construction of a function that maps a contribution to the yield to procedure data yield sets constitutes supervised learning, a machine learning activity. Identifying data that applies to a wide number of preparation models is made possible by this capacity to elicit. Data science includes a substantial amount of managed learning[17]. Prepared data includes various prepared models, and administering learning is the machine learning assignment that begins with that preparation. The information yield of a supervised neural network is known. A comparison is made between the expected and actual yields from the neural system. Because of the mistake, the settings have been changed and the neural system has been re-addressed. The administered neural system is employed in a feed-forward neural system[21].

Assumption 1: Use the K-Nearest Neighbor approach. Simple administered machine learning formula that can solve both characterization and regression issues. The solution to a regression issue is a real number (a decimal number). Using the information in the table below, it can tell how much someone weighs in proportion to their height.

This machine uses SVM (Support Vector Machines) technology. The use of supervised machine learning for data collecting and relapse prevention is highly recommended. It is often used when characterization is an issue. The classifier uses SVMs to draw a line between the two categories (hyper-plane). To use naive Bayes, you have to agree that highlights are factually independent, and that is what makes it supervised machine learning based on the theory. But it has been shown to be a great classifier in spite of this assumption

This machine-learning technique is used to draw inferences from datasets that include unmarked answers. Unsupervised learning approaches such as cluster analysis are quite popular. Use it to identify hidden patterns or clusters in your data during exploratory investigation.

Unsupervised The neural network does not know what the information will generate since it has no previous knowledge of it. The system's primary purpose is to sort and classify data based on a wide range of factors. The brain system connects various sources of information and assembles them into a cohesive whole. K-Means: Unsupervised learning approach that is simple and well-known. While maintaining centroids as small as feasible in light of the existing circumstances, the K-means approach finds k

centroids and then generates each data point to a nearby grouping.

VIII CloudSecurityMLAlgorithms

This section looks at a number of machine learning technologies that have been used to solve security problems in the CC environment.

SupervisedLearning

When employing model data yield sets, you may learn to restrict the amount of commitment you can make to produce a yield. This is known as supervised learning in machine learning. It derives a limit using data derived from a large number of planning models. Supervised machine learning algorithms are ones that need external assistance.AES stands for Advanced Encryption Standard and is a symmetric encryption algorithm. AES developed by two Belgian cryptographers Joan Doeman and Vincent Rljmen. AES is used to protect sensitive information implemented in hardware and software. It is suitable, suppose want to encrypt a private text into decrypt able format [3], [4]. The best example is, when demand to send sensitive information in email. The decryption of this information is possible if know the correct password.

Supervised ANNs

Computer algorithms that replicate the way the human mind analyzes and processes data are known as artificial neural networks (ANNs). They are components of a computational architecture. The machine learning institutions are responsible for resolving problems that would be impossible or intractable for people or statistical principles to handle.DES means data encryption standard is a symmetric key algorithm. DES uses the same key for encrypt and decrypt the message and the same private key is well-known by the one and other i.e. sender and receiver. DES takes 64- bits of plain text as an input and produces 64-bits of cipher text.

According to Hussin et al. [19], ANN algorithms were used to predict basic distributed computing security issues. To discover security weaknesses in a financial institution, a neural network method was used in conjunction with other techniques. The use of artificial neural networks (ANNs) was used to improve the execution and learning capabilities of neural networks. Levenberg-Marquardt (LMBP) algorithms were used to anticipate the display of the cloud security level in advance of its actual presentation. For the preparation phase, the LMBP is a nonlinear improvement model that is used to assess the accuracy of forecasts as well as to minimize error between genuine yields and the focus of attention; the mean square error (MSE) is evaluated to decide the presentation. The cloud Delphi procedure was used for informal social meetings as well as for inquiry purposes. The Delphi method was employed to extract information from knowledgeable individuals. The ANN algorithm was used as the measurable information model in order to anticipate issues associated with distributed computing. Using the LMBP technique, it was possible to forecast cloud security issues.

When applied to the CC security challenge affecting financial institutions, LMBP algorithms have been demonstrated to be especially productive for testing and preparing systems. Complex attacks in cloud settings are difficult to detect because cloud frameworks are

composite and dispersed, making it difficult to identify complex attacks. Additional to this, various portable registering and storing devices are connected to cloud structures in order to expedite a client's entrance, increasing the intricacy and difficulty of identifying digital assaults. [page break] Several researchers, including Sayantan et al. [26], uncovered digital threats in cloud settings that are crucial for cloud arrangement security. A comprehensive technique for identifying digital assaults in cloud infrastructures as well as remote processing devices has been developed and demonstrated. The use of an ANN was one of the techniques that was advocated. The ANN was developed using data from the system's traffic on the cloud stops' connecting connections, which was collected throughout the development process. ANN requires a significant amount of processing power, thus a hereditary calculus-based strategy to reducing the quantity of structures mined from system-traffic data has been developed and is now being merged in this methodology. As an example, two important instructive collections of system traffic were used to demonstrate this procedure, with the results demonstrating much improved discoveries when compared to current methods for detecting digital assaults in cloud arrangements. The approach used makes use of organized informational collections of system traffic for the aim of building and evaluating guided machine learning in an artificial neural network.

At this time, models for effective and secure system framework structures, such as the Internet of Things (IoT) and big data analytics, are emerging at a quicker pace than they have at any other time in recent history. The edge processing of an IoT structure is a data organization that takes place at or around the data's identifiers in an IoT system. Al-Janabi and colleagues described how secure edge computing may be utilized in the Internet of Things to safeguard data while also increasing speed. It was the goal of this research to provide a concise summary of the principles and characteristics, as well as the security and application of IoT-enabled edge preparation, as well as the security implications of such preparation in today's data-driven world Aiming for brevity, the writers examined the ideas, advantages, security, and practical applications of Internet of Things-enabled edge processing, as well as the security implications of such processing in today's information-driven world. During the course of building a scalable, reliable, secure, and distributed computing architecture, the authors examined the many variables to take into consideration. In addition, the writers discussed the fundamental ideas that underpin risk management systems for security operations. In addition, they examined the difficulties and opportunities related with edge computing technology. Finally, the authors addressed two contextual investigations, proactive stopping and substance conveyance arrangement (CDN), as well as various ways for using Internet of Things frameworks to complete everyday tasks.

IX Conclusion

Security risks and assaults were assessed in this research as the most difficult concerns in Cloud computing. Numerous machine learning techniques, including as ANNs, K-NN, and K-Means, were examined as potential answers to the security vulnerabilities in CC. We examined many suggested solutions for cloud security that made use of machine learning algorithms. We conducted an analytical

study and analysis of the recommended methodologies, emphasizing their relative merits and demerits. Additionally, we identified numerous study paths that need additional exploration in the future.

References

1. Lim,S.Y.;Kiah,M.M.;Ang,T.F.SecurityIssuesandFutureChallengesofCloudServiceAuthentication.*Polytech.Hung.***2017**, *14*, 69–89.
2. Borylo, P.;Tornatore, M.;Jaglarz, P.;Shahriar, N.;Cholda, P.;Boutaba, R. Latency and energy-awareprovisioningofnetworkslicesincloudnetworks.*Comput.Commun.* **2020**,*157*,1–19.
3. Carmo, M.; Dantas Silva, F.S.; Neto, A.V.; Corujo, D.; Aguiar, R. Network-Cloud Slicing Definitions for Wi-Fi Sharing Systems to Enhance 5G Ultra-Dense Network Capabilities.*Wirel. Commun. Mob. Comput.***2019**, *2019*,1–17.
4. Dang, L.M.; Piran, M.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing forhealthcare.*Electronics***2019**,*8*,768.
5. Srinivasamurthy, S.; Liu, D. Survey on Cloud Computing Security. 2020. Available online: https://www.semanticscholar.org/(accessedon19July2020).
6. Mathkunti,N.CloudComputing:SecurityIssues.*Int.J.Comput.Commun.Eng.***2014**,*3*,259–263
7. Stefan, H.;Liakat, M. Cloud Computing Security Threats And Solutions.*J. Cloud Comput.***2015**, *4*, 1.[CrossRef]
8. Fauzi,C.;Azila,A.;Noraziah,A.;Tutut, H.;Noriyani,Z.OnCloudComputingSecurityIssues.*Intell. Inf.DatabaseSyst. Lect.NotesComput.Sci.* **2012**,*7197*,560–569.
9. Palumbo,F.;Aceto,G.;Botta,A.;Ciuonzo,D.;Persico,V.;Pescapé,A.CharacterizingCloud-to-userLatencyas perceived by AWS and Azure Users spread over the Globe.In Proceedings of the 2019 IEEE GlobalCommunicationsConference (GLOBECOM), Taipei,Taiwan, 7–11 December2019; pp.1–6.
10. Hussein,N.H.;Khalid,A.AsurveyofCloud ComputingSecuritychallengesandsolutions.*Int.J.Comput.Sci.Inf.Secur.***2017**,*1*,52–56.
11. LeDuc,T.;Leiva,R.G.;Casari,P.;Östberg,P.O.MachineLearningMethodsforReliableResourceProvisioninginEdge-CloudComputing:ASurvey.*ACMComput.Surv.***2019**,*52*,1–39.
12. Li,K.;Gibson,C.;Ho,D.;Zhou,Q.;Kim,J.;Buhisi,O.;Gerber,M.Assessmentofmachinelearningalgorithmsincloudcomputingframeworks.InProceedingsoftheIEEESystemsandInformationEngineering DesignSymposium,Charlottesville,VA, USA,26April2013;pp.98–103.
13. Callara, M.;Wira, P. User Behavior Analysis with Machine Learning Techniques in Cloud ComputingArchitectures.In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa,Algeria,24–25November2018;pp.1–6.
14. Singh,S.;Jeong,Y.-

Security:Issues,Threats,andSolutions.*J.Netw.Comput.Appl.***2016**,*75*,200–222.

15. Khan, A.N.; Fan, M.Y.; Malik, A.; Memon, R.A. Learning from Privacy Preserved Encrypted Data on CloudThroughSupervisedandUnsupervisedMachineLearning.InProceedingsoftheInternationalConferenceonComputing,MathematicsandEngineeringTechnologies,Sindh,Pakistan,29–30January2019;pp.1–5.
16. Khilar,P.;Vijay, C.;Rakesh, S. Trust-Based Access Control in Cloud Computing Using Machine Learning.In *Cloud Computing for Geospatial Big Data Analytics*; Das, H., Barik, R., Dubey, H., Roy, D., Eds.; Springer:Cham,Switzerland,2019;Volume49,pp.55–79.
17. Subashini,S.;Kavitha,V. A Survey on SecurityIssuesinService Delivery Models of Cloud Computing.*J.Netw.Comput.Appl.***2011**,*35*,1–11.
18. Bhamare, D.; Salman, T.; Samaka, M.; Erbad, A.; Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In Proceedings of the International Conference on Information Science and Security, Jaipur,India, 16–20 December 2016; pp. 1–5.
19. Li, C.; Song, M.; Zhang, M.; Luo, Y. Effective replica management for improving reliability and availabilityinedge-cloudcomputingenvironment.*J.ParallelDistrib.Comput.***2020**,*143*,107–128.
20. Purniemaa, P.; Kannan, R.; Jaisankar, N. Security Threat and Attack in Cloud Infrastructure: A Survey.*Int. J.Comput.Sci.Appl.***2013**,*2*,1–12.
21. Yuhong, L.; Yan, S.; Jungwoo, R.; Syed, R.; Athanasios, V. A Survey of Security and Privacy Challenge inCloudComputing:SolutionsandFuture Directions.*J.Comput.Sci.Eng.***2015**,*9*,119–133.
22. Chirag, M.; Dhiren, P.; Bhavesh, B.; Avi, P.; Muttukrishnan, R. A survey on security issues and solutions at differentlayers ofCloudcomputing.*J.Supercomput.***2013**,*63*,561–592.
23. Behl,A.;Behl,K.Ananalysisofcloudcomputingsecurityissues.InProceedingofthe WorldCongresson Information and Communication Technologies,Trivandrum, India, 30 October–2 November 2012;pp.109–114.
24. Selamat,N.;Ali,F.Comparisonofmalwaredetectiontechniquesusingmachinelearningalgorithm.*Indones.J.Electr.Eng.Comput.Sci.***2019**,*16*,435.]
25. Shamshirband, S.; Fathi, M.; Chronopoulos, A.T.; Montieri, A.; Palumbo, F.; Pescapè, A. ComputationalIntelligence Intrusion Detection Techniques in Mobile Cloud Computing Environments: Review, Taxonomy,andOpenResearchIssues.*J.Inf.Secur.Appl.***2019**,1–52.