Machine vs Non-Machine Learning Approaches to Cloud Security Solutions: A Survey

Gopal Krishna Shyam[#1], Srilatha Doddi[*2]

[#]School of Computing and Information Technology, REVA University, Bangalore 560064, IN
[1]gopalkrishnashyam@reva.edu.in
* School of Computing and Information Technology, REVA University, Bangalore 560064, IN
* Department of CSE, Sreenidhi Institute of Science & Technology, Hyderabad 501301, IN
[2]doddisrilatha@gmail.com

Abstract—**Cloud computing is a trending paradigm that provides both physical and logical computational resources as services over the Internet. The basic advantages of the cloud are, a reduction of IT organization's infrastructure cost, flexibility to access and use the services. Regardless of its advantages, it has raised several security concerns such as data availability, data privacy, data location, authentication, authorization, access control, network security, web security, and virtual machine security etc. which may potentially hamper its growth. In recent years, the expansion of several types of dynamic threats such as data breaches, account hijacking, insecure interfaces, advanced persistent threats, shared technology vulnerabilities, and distributed denial of service attacks target the cloud to disrupt cloud services and can compromise security. To tackle several security issues, solutions can be provided through a set of control based technologies such as next generation firewalls, cryptography techniques, intrusion detection systems, software defined networks, machine learning techniques etc. In this paper, we focus on comparative analysis of several cloud security issues through machine learning and non-machine learning approaches. Some open challenges for further research have also been suggested.**

Keyword-Attacks, Cloud computing, Cloud security, Intrusion detection system, Machine learning.

I. INTRODUCTION

Cloud computing is a trending model that provides computational resources such as compute, storage, network, operating system, application development and deployment environment, application software, media etc. as services over the Internet. Cloud Computing is gaining popularity due to its basic advantage of IT organizations' infrastructure cost savings [1]. Cloud computing has become a social phenomenon used by most people every day as they are migrating the applications and data from a local machine to a remote machine. The basic idea behind cloud computing is layered and flexible architecture. The reference model of cloud computing is presented in the Fig. 1.

The National Institute of Standards and Technology (NIST) defines five essential characteristics, four deployment models, and three service models of cloud computing. The five essential characteristics of cloud are broad network access, resource pooling, on-demand self service, rapid elasticity and measured service and four deployment models of cloud include public cloud, private cloud, hybrid cloud and community cloud. The infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) are the three service models of cloud.

In IaaS layer, infrastructural services like compute (i.e. virtual machines), storage, and networks can be delivered to the end users. The PaaS layer provides databases, software libraries, application development and run-time environments for developing, testing, delivering and managing the application software'. In SaaS, application software' are delivered to the end users without installing these on local machines.

In a public cloud, the resources are openly accessible to several organizations. Whereas, in a private cloud, the resources are used exclusively by a single organization. A hybrid cloud is a mixture of private and public cloud that provides data and applications to be shared between several organizations. Whereas, in a community cloud, the cloud infrastructure supports a specific community that has shared mission, policies and service requirements.

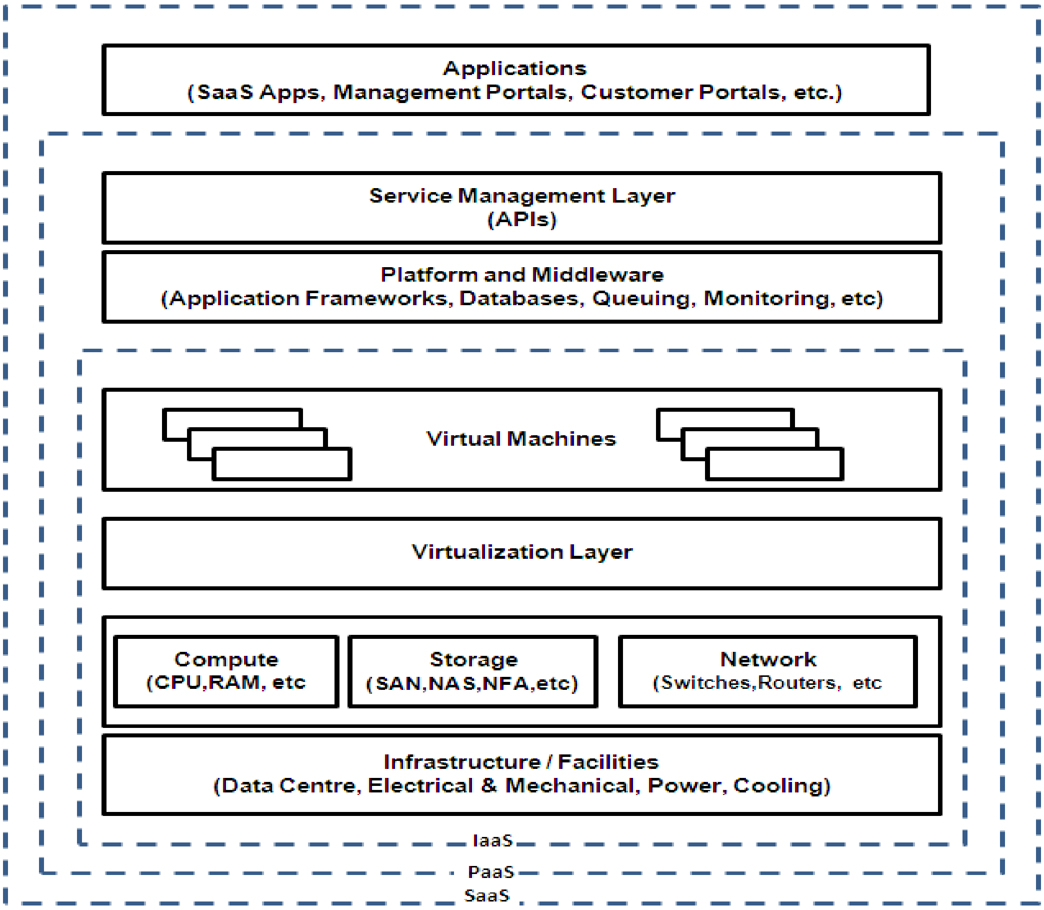
Applications
(SaaS Apps, Management Portals, Customer Portals, etc.)
Service Management Layer
(APIs)
Platform and Middleware
(Application Frameworks, Databases, Queuing, Monitoring, etc)
Virtual Machines
Virtualization Layer
Compute
(CPU,RAM, etc
Storage
(SAN,NAS,NFA,etc)
Network
(Switches,Routers, etc
Infrastructure / Facilities
(Data Centre, Electrical & Mechanical, Power, Cooling)
IaaS
PaaS
SaaS

Fig. 1.Reference Model of Cloud Computing [2]

In the cloud, infrastructure cost reduction, increased scalability, service reliability, flexible and easy to use are the basic benefits to end users. On the other hand, data security, data privacy, and trust management, service level agreement (SLA), compliance, data availability, data location, data integrity, network and virtual machine (VM) security etc. are the several security issues and challenges [3]–[9]. These issues are to be addressed to make the cloud environment secure and free from launching the threats that target the cloud system.

Security is a condition in which data and applications are protected against its confidentiality, integrity and availability (CIA triad) requirements in the desired state and at the right time. In cloud, these security issues have been created as a center of attention since its inception. The novel tools and techniques always necessitate strengthening the security of cloud services [10] and these may come along with its various specifications and methods.

An analysis of the related work with a survey based on the cloud security issues, attacks, open challenging issues, and solutions through the machine learning and non-machine learning approaches are presented in Table I.

The papers [7], [9], [11]–[18] focuses on a detail discussion on different security issues and challenges in cloud computing and recommended solutions. The papers [12], [19], [14], [18], [7] discusses about the threats in cloud and its countermeasures. The papers [7], [19]–[21] provides an overview about attacks in cloud and its defense mechanisms through non-machine learning techniques and the papers [7], [12], [16]–[18], [21] proposes some open challenging issues.

Also, the papers [19]–[23] does not focus on cloud security issues and its solutions in cloud. The papers [9], [11], [13], [15]–[17], [20]–[23] does not focus on threats and its solution. The papers [9], [11], [23], [12]–[18], [22] does not focus on attacks and solutions through non-machine learning approaches. The papers[9], [11], [13]–[15], [19], [20], [22], [23] does not focus on the open challenging security issues.

There is a lack of discussion on the security issues, threats, attacks and suggested solutions through various technologies and techniques in the above mentioned papers. Also, none of the above mentioned paper deals with the threat and attack detection solutions using machine learning approaches.

TABLE I
Summary of Comparative Analysis of Existing Survey Papers Related to Cloud Security Issues, Threats, Attacks and Suggested Solutions Through Non-Machine Learning and Machine Learning Approaches

Authors/Topics Discussed	**Cloud security issues and challenges**	**Solutions to security issues in cloud**	**Threats in cloud**	**Solutions for threats in cloud**	**Attacks in cloud**	**Non-Machine Learning approaches for Attacks in Cloud**	**Machine Learning for attacks**
Verma et al. [11]	✓	✓	X	X	X	X	X
Radwan et al. [12]	✓	✓	✓	✓	X	X	X
Parveen Kumar [13]	X	X	X	X	✓	✓	X
Chou et al. [14]	X	X	✓	X	✓	X	X
Coppolino et al. [15]	X	X	✓	✓	✓	✓	X
Sun et al. [16]	✓	✓	X	X	X	X	X
Parekh [8]	✓	✓	X	X	✓	X	X
Hashizume et al. [17]	✓	✓	✓	✓	X	X	X
An et al. [18]	✓	X	✓	X	X	X	X
Zissis et al. [19]	✓	✓	X	X	X	X	X
Iqbal et al. [20]	X	X	X	X	✓	✓	X
Ali et al. [21]	✓	✓	X	X	X	X	X
Puthal et al. [22]	✓	✓	X	X	X	X	X
S.Singh et al. [23]	✓	✓	✓	✓	✓	X	X
Singh et al. [6]	✓	✓	✓	✓	✓	✓	X
This Survey	✓	✓	✓	✓	✓	✓	✓

Note: Here "X" means that particular topic is not covered in the paper and "✓" means that particular topic is covered in the paper.

The rest of the paper is organized as follows. The section II provides a brief discussion on various cloud security issues and its solutions. Section III deals with the types of attacks in cloud computing and suggested solutions. Section IV presents cloud security solutions to defence attacks using non-machine learning approaches. Section V presents automation of threat and attack detection using machine learning techniques. And finally, some open challenging issues are presented in Section VI.

II. SECURITY ISSUES IN CLOUD COMPUTING

In this section, we present a brief introduction about the major security issues in cloud computing, and then present the solutions to address the issues. In general, a security issue is something that happensin any resource of the system in the form of attack, misconfiguration, failure, weakness and damage etc. The cloud specific security issues are raised due to the characteristics of cloud computing and its related technologies such as grid, service oriented, network, web, virtualization etc.

The major security issues and challenges related to cloud computing are categorized and reviewed as follows.

A). Gartner[3] identified seven major security issues in cloud computing which are: A) privileged user access, B) regulatory governance, C) data segregation, D) data location, E) long-term viability, F) data recovery, and G) investigative support.

B). Rabiprasad et al. [4] presented adetailed survey on security issues present in cloud: i) network security, ii) virtual machine security, iii) access to applications and servers, iv) data transmission, v) data security, vi) data integrity, vii) data privacy, viii) data segregation, ix) data availability, x) data location, xi) security policy, xii) patch management, and xiii) compliance.

C). Srinivasan et al. [5] presented the taxonomy of security challenges based on two aspects, including1). architectural and technological aspects and 2). regulatory and process related aspects. i) logical storage segregation, ii) multi-tenancy, iii) identity and access management, iv) insider attacks, v) virtualization, vi) key management and cryptography are the architectural and technological challenging issues and I) regulatory compliance gaps and governance, II) insecure application programming interfaces (APIs), III) service level agreement (SLA), IV) cloud and cloud service provider (CSP) migration issues, and V) trust management are regulatory and process related challenging issues.

D). Ashish et al. [7]have presented the classification of cloud security issues based on i) virtualization, ii) network, iii) Internet and service related, iv) data storage and computing, v) access control, vi) trust management, vii) software and viii) compliance and legal aspect.

E). Wang [8]discusses amajor security and privacy issue which includes include i) authentication and identification, ii) lack of user control, iii) policy integration, iv) service availability, v) unclear responsibility, vii) access control, viii) unauthorized data usage, and vii) auditing.

F). Disha et al. [24] presented a comprehensive analysis of security challenges on deployment and service models, and issues particular to the network layer of the cloud. The issues relevant to cloud deployment models include i) motility of data and data residuals, ii) elastic perimeter, iii) cloning and resource pooling, iv) shared multi-tenant environment, v) authentication and identity, and vi) unencrypted data etc. and the major issues in cloud service models are a) data leakage, b) malicious attacks, c) backup and storage, d) service and account hijacking, e) virtual machine hopping and f) shared technological issues. A) Structured Query Language (SQL) injection attack, B) Extensible Markup Language (XML) wrapping attack, C) flooding attack, D) browser security, E) incomplete data deletion etc. are the network concerns in cloud.

A brief discussion on different security issues and challenges of cloud computing are presented in [7], [9], [22], [11]–[18]. The summary of each security issue is discussed as follows.

1) Authentication: It is the process of verifying the credentials of the users requesting access to cloud applications and data.
2) Authorization: It is the system through which the privileges are granted to the users to access the cloud resources.
3) Key Management: It refers to the management of cryptographic keys such as key creation, key storage, key backup, key rotation, key expiration, key archival and key destruction activities etc.
4) Data Confidentiality: It allows sensitive or confidential data tobe accessible only to authorized users.
5) Data Security at Rest: It refers to a situation when the data is stored on permanent storage devices like hard disk or tapes, such data must be prevented from unauthorized access.
6) Data Security in Transit: It refers to protecting sensitive data while the data is moving from one location to another such as across the Internet.
7) Data Privacy: It is the ability of an individual to protect sensitive data about themselves.
8) Data Integrity: Data integrity ensures that the data is not deleted, modified or fabricated by unauthorized party after it is generated, stored or transmitted.
9) Access Control: Access control is the specific confinement of access to a place or other asset to coordinate who or what can see or utilize assets in a handling circumstance.
10) Data Segregation: Storing of one user's data separated from another user's data.
11) Data Availability: It is the circumstance in which information continues to be accessible at a required level of execution.
12) Data Location: Information processed in an electronic correspondences organized by an electronic interchanges benefit demonstrating the geographical position of the terminal gear of a client of an open electronic correspondence administration.
13) Data Backup: Data backup is the way towards copying information to permit recovery of the copy set after an information misfortune occasion to be ready to restore them if there should be an occurrence of information misfortune.
14) Auditing: The mechanism to collect and evaluate the evidence to find out whether service provider protects cloud resources, preserves integrity of data, management of resources strongly and attains organizational milestones successfully.
15) Non-Repudiation: refers to a method in which the dispatcher cannot refuse the sent messages and that the recipient cannot deny having received messages.

16) Network Security: It is a set of practices that are to be followed to prevent and monitor illegitimate access, and abuse of network resources.

17) Virtual Machine Security: Virtual machine security is the aggregate measures, strategies and procedures that guarantee the protection of a virtualization framework or virtual machines.

18) Web Application Security: The set of practices for securing the sensitive data stored online from unauthorized access.
19) Data Recovery: It is the way towards recovering out of reach, lost, debased, harms or designed information from storage media when they can't be gotten up typically.
20) Identity and Access Management (IAM): IAM is the system of approaches or advances for guaranteeing that the best possible individuals in an endeavor have the proper access to innovation assets.
21) Privileged User Access: A privileged user access is someone who has managerial access to basic cloud resources like administrators and their recruitment procedure.
22) Regulatory Compliance: Regulatory compliance depicts the information an organization seeks to know about how to achieve milestones and find the ways to accept some important laws, approaches, and directions.
23) Long-term Viability: The success of a business organization is projected by its long term endurance and its power to gain profits over some period of time.
24) Trust Management: Trust administration is building up trust for distributed computing administration that guarantees secure information access through trust commendable cloud specialist organization.
25) Data Access: Data access refers to programming exercises related to storing, fetching or manipulation of data residingin a database or other media.

The potential attacks can be raised on the cloud technology due to several security issues and improper implementation of its solutions. The major threats and attacks arise in cloud that hampers the growth of the cloud technology and its taxonomy includes:

1) Ahmed et al. [25] presented the generalized threat taxonomy based on human and technological factors as root categories in a cloud computing model.

2) Jouini et al. [26] proposed the model for threat taxonomy, based on, I) the threat classification criteria including, i) agent, ii) source, iii) intention, and iv) motivation, and II) potential impact of threats such as, i) destruction or motivation of information, ii) theft or loss of information, iii) disclosure of information, iv) elevation of privilege, vi) denial of use, and vii) illegal usage.

3) Cloud Security Alliance (CSA) [27] identified twelve notorious threats with reference to the cloud service model and ranked the threats based on their rigorousness. The taxonomy of threat include i) data breach, ii) insufficient credentials, identity and access management, iii) insecure interfaces, iv) vulnerabilities in systems, v) hijacking of accounts/services, vi) malicious insider, vii) advanced persistent threats, viii) data loss/leakage attacks, ix) inadequate due diligence, x) nefarious and abuse use of cloud services, xi) denial of service (DoS) attacks, and xii) shared technology vulnerabilities.

4) Gupta et al.[28] presented an exhaustive survey on taxonomy of cloud threats and classified the threats based on i) the location of security attacks, and ii) the service layer of cloud. They further, classified the location of attacks into I) cloud service users' end and II) providers' end and cloud service layer attacks into I) infrastructure layer security attacks, II) virtual machine security attacks, III) platform layer security attacks, IV) application layer security attacks, and V) invalid modification attacks.

5) Coppolino et al. [19] presented an overview of attacks that can be launched against cloud infrastructure layer of cloud such as i) network-based attacks (includes DoS attacks, sniffing attacks, and spoofing attacks), ii) hardware-based attacks (includes tracing attacks, timing attacks, access-driven attacks, side-channel attacks, boot integrity attacks, data directed attacks and probing attacks) and iii) hypervisor-based attacks (includes direct kernel structure manipulation attacks, code injection attacks, and root kit attacks).

The solutions for the security issues in cloud computing environment are essential for efficiently designing the cloud based systems. In the Table II, we present the suggested solutions from the existing work related to the cloud security issues, and identified attacks with respect to a specific security issues in cloud.

TABLE II
The Solutions for Cloud Security Issues and Potential Attacks

Security Issue	**Solutions**	**Attacks Identified**
Authentication [29]	a. Use Attribute Based Signature (ABS) Algorithm b. Use Public Key Infrastructure (PKI) based Single Sign On(SSO) mechanism c. Use Digital Signatures d. Use Security Assertion Mark-up Language (SAML) Protocol e. Use Multi-factor Authentication Schemes.	Brute-Force and Dictionary
Authorization [30]	1) Use Open Authorization (OAuth) Protocol 2) Use Certificate Based Authorization Protocol 3) Multi-tenancy Authorization Model 4) Role based Multi-tenancy Access Control Mechanism	Path/Directory Traversal, and Parameter Manipulation
Data Confidentiality	1) Use strong encryption techniques such as, a) Fully Homomorphic Encryption (FHE) b) Attribute Based Encryption (ABE) c) Hierarchical Attribute-Based Encryption (HABE) 2) Use Public Key Infrastructure Pub	Phishing, Password and Packet Sniffing
Key Management [31]	1. Use File Assured Deletion (FADE) Protocol 2. Intrusion Detection System (IDS)	Sandwich And Brute Force
Data Privacy [32]	1. SecCloud Protocol 2. Cloud Data Encryption Standard (DES) Algorithm 3. PKI encryption	Data Leakage And Path Traversal
Data Integrity [18]	a. Transaction should follow ACID properties b. Secure Shell (SSH) Protocol	Man-In-The-Middle, Session Hijacking and Data Diddling
Access Control [33][34][35]	a. Adopt strong encryption schemes such as. i) Attribute Set Based Encryption (ASBE) ii) Hierarchical Attribute-Set-Based Encryption (HASBE) b. Use Role Based Multi-tenancy Access Control Mechanism	Replay and Masquerading
Data Segregation [18]	a. Use Cryptographic Separation of Data b. Follow the policy of Service Level Agreement	Data Leakage
Data Availability[36]	a. Proxy re-encryption scheme based on time-based b. Adopt Block chain based distributed cloud with software networking	DoS/DDoS
Data Location	a. Enterprises require that the CSPs store and process data in particular jurisdictions and follow the privacy rules of those jurisdictions	Man-In-The-Middle
Data Backup and Recovery [37][38]	a. CSPs need to ensure that sensitive data is to be regularly back up [18] b. Use Seed Block Algorithm c. Cold/Hot Backup Strategy	Authentication and Tampering
Network Security [16][39][40][41]	a. Use Strong Cryptographic Algorithms b. Intrusion Detection and Prevention Systems(IDPS) c. Digital Certificates d. Use tree-rule firewall e. SnortFlow for intrusion prevention f. Cloud based Software Defined Networking technology g. CloudSec using VM Introspection (VMI) Technique h. Use standard protocols such as Secure Socket Layer (SSL) and Internet Security Protocol (IPSec)	DoS /DDoS, Phishing, DNS Spoofing , ARP Spoofing, IP Spoofing and Port Scanning

Security Issue	Solutions	Attacks Identified
Virtual Machine Security [16] [42]	a. Use software-based network components, such as bridges, and software-based network configurations, and routers [16] b. Use Cyber Guarder	Malware, Spoofing, Sniffing, Cross-VM, VM Escape, Rootkit, Hyperjacking and Timing Side-
Web Application Security [42]	a. Use XML signature and XML Encryption techniques b. Use HTTPS protocol	SQL Injection, Cross Site Scripting, Spoofing, Metadata Spoofing, Man-In-The-Middle and Eavesdrop
Identity and Access Management [16][7][43]	a. Adopt SPML, SAML, OAuth, and XACML standards b. Use claim based identity management system c. Use Simple Privacy-preserving identity management d. Use Federated IAM	XML Wrapping
Privileged User Access	a. CSPs must have the knowledge on the hiring and access control mechanisms of cloud administrators	-
Regulatory Compliance	a. CSP must be able to submit to external Audits and security certifications to cloud customers b. CSP needs to frame unified regulatory compliance	-
Trust Management	a. Public Key Infrastructure based trust model b. SLA verification based trust model	-

III. CLOUD ATTACKS AND SOLUTIONS

In this section, we focus on an overview of the attacks in cloud computing and also, suggest the solutions for attacks to provide security in the cloud environment.

A. Cloud Attacks

Many of the organizations move forward to the cloud computing paradigm. It looks for some hackers to follow. Some of the potential cyber security attack vectors that criminals may attempt include phishing attack, DoS attack, sniffing attack, spoofing attack side-channel attack, boot integrity attacks, data directed attack, kernel structure manipulation attack, code injection attacks, replay attack, modification attacks, man in middle attack, malware attack, brute force attack, and hyperjacking attack etc. Table III describes several attacks target the cloud and the solutions for the attacks in cloud are presented in Table IV.

TABLE III
Attacks in Cloud

Type of Attack	Description
Phishing Attack	Obtain confidential information such as user names, passwords and credit card details often for malicious reasons, by disguising as a trusted entity in electronic communications.
SQL Injection Attack	Injection of malicious SQL commands using client input data to the application that is then passed to the database instance for execution and is intended to affect the execution of predefined SQL commands.
Cross-Site Scripting (XSS) Attack	This is a type of computer security vulnerability that is usually found in web applications. It also allows attackers to inject client side scripts into web pages accessed by other users.

Type of Attack	**Description**
Denial-of-Service Attack	Attacks that are denying or blocking the cloud services, so that services are unavailable to actual users or prevent cloud user services from being able to access the data and applications.
Spear Phishing Attack	Spear phishing is an email scam aimed at a specific person, organization or company. Although they often intend to steal data for malicious purposes, cybercriminals can also install malware on a specific user's computer.
Brute Force Attack	A brute force attack is a technique used to decipher passwords. The success of this attack depends to a large extent on powerful computing capabilities because thousands of possible passwords must be sent to a target user's account until they find the correct access.
Hyperjacking attack	Attackers attempt to build and execute a very thin hypervisor that takes full control of the underlying operating system.

TABLE IV
Cloud Attacks and Solutions

Type of Attack	**Solutions**
DoS/DDoS Attack [44] [45]	a. Use next generation firewalls such as Tree-rule based firewall b. Intrusion detection system c. Multilevel Thrust Filtration (MTF) mechanism d. Strong authentication and authorization mechanisms e. Use Covariance-matrix method f. Use Network packet filtering mechanism
SQL injection Attack	a. Employ a strong virtual machine isolation mechanism b. To check integrity by using MD5, SHA hash algorithms c. Use secure web browsers and d. Adopt SDN technology based cloud
Hyperjacking Attack	a. VM isolation mechanism b. Install Virtual machine monitor security software c. Monitor virtual machine activities d. Redesign the cloud architecture and e. Design a hierarchical secure virtualization model
Metadata spoofing Attack	a. To access a metadata file namely, web security description language (WSDL), a strong authentication mechanism is needed.
Phishing Attack	a. Use the Hyper Text Transfer Protocol Strict Transport Security (HSTS) protocol
Backdoor channel Attack	a. Employ a strong authentication and authorization mechanism b. Use Virtual machine isolation mechanism
Man-in-middle Attack	a. Develop a proper secure socket layer (SSL) architecture
Port scanning Attack	a. Require a strong port scanning security mechanism
User to Root Attack	a. Require a strong authentication mechanism

Type of Attack	Solutions
Malware Attack [46]	a. Install a antispyware or anti-malware softwares and b. Adapt CloudIntell-A cloud Intelligent malware detection system
Spoofing Attack [47]	a. Use Network Packet Filters (NPF) b. Use Packet Resonance Strategy (PRS)
Side channel Attacks/Co-resident Attack [48][49][50]	a. Use a secure VM allocation policy namely Previously Selected Server First (PSSF) b. Use dynamic cache coloring mechanism

IV. CLOUD ATTACKS SOLUTIONS THROUGH NON-MACHINE LEARNING APPROACHES

In this section, we present numerous non-machine learning approaches presented for effective identification of attacks in the cloud computing environment. Some of the non-machine learning techniques such as SDN, cloud IDS/IDPS, firewalls and cryptography etc. which are reviewed as follows.

A. Software Defined Networking (SDN) Technology

SDN provides a novel and energetic network design for cloud computing, the good features of SDN makes it easier to detect and defense against Distributed Denial of Service attacks in cloud computing.

Yan et al. [51] have reviewed about the defense mechanism against DDoS using SDN in cloud computing environment and have also addressed how to prevent SDN itself from becoming a victim of DDoS attack.

Wang et al. [52] have examined the security mechanism in enterprises to defense against DDoS detection using the combination of Cloud and SDN technologies and also designed a highly program based network architecture to allow attack detection and a flexible control structure that permits fast and specific attack prevention.

AlEroud et at.[53] presented a technique to detect DoS attacks in a SDN environment, using a packet aggregation technique and an inference mechanism to generate attack signatures and guess the attacks.

Meng et al.[54] focused on the detection of insider attacks in healthcare SDN by the using Bayesian Trust Management approach.

B. Intrusion Detection System(IDS)

The intrusion detection was considered to be a significant issue in the cloud to identify abnormal or malicious behavior. IDS system is a software application or a device used to recognize malicious activities in order to gain the access to a cloud resource or service.

The key challenge of IDS is to reliably distinguish between legal users and illegal users or identify legal activities from illegal activities. Traditionally, there are two types of IDS approaches namely, i) Knowledge-based IDS and ii) Behavior-based IDS.

1) Knowledge or Signature Based IDS: It identifies the attacks by searching for particular patterns or signatures of well-known attacks. These systems are also known as detection by appearance or misuse detection. The basic advantage of misuse detection system is that it can easily detect known attacks accurately, however itcannot detect new or unknown attacks.

2) Behavior-Based IDS: This system attempts to identify the malicious behavior from the normal behavior and, works based on the classification model to train normal behavior and compares the new behavior against normal behavior and classifiesthe behavior as either normal or anomalous. If the behavior is deviated from normal behavior, it is classified it as anomalous. It is also known as anomaly detection or detection by behavior. The basic advantage of anomaly detection is detecting the unknown or new attacks, however itsuffers from high false positives i.e. classifies unknown normal behavior as malicious behavior.

Several IDSs can detect the attacks through either the behavior based technique or the knowledge based technique. Instead, a novel and challenging IDS should be developed to integrate both techniques because the signature based detection system is reliable in detecting known attacks with low false positive alarms, but it does not detect unknown attacks or even minor modifications to known attacks. Instead, the anomaly based technique detects unknown attacks but it raises false positives. To improve the detection accuracy of malicious behavior, distributed and collaborative IDSs are emerging.

Compared to IDS, Intrusion Detection and Prevention Systems are the systems along with IDS, have the ability to respond through raising alarms, logging a user off, halt or shut down the system on the detection of intrusions.

Numerous IDS approaches have been developed using data mining and machine learning techniques, statistical analysis, artificial intelligence techniques such as genetic algorithms, artificial neural networks, fuzzy logic, swarm intelligence, and artificial immune system etc.

C. Firewalls

A recent research was conducted on the detection of the intrusion to save the data of the user and resources based on the cloud storage from malpractices. Thus, the resulting research suggested the firewall as an efficient approach in detecting the malicious behavior or threats among the cloud servers. However, this research was found to be limited as the firewall was unable to detect the intruders within the organizations and further complex attacks.

Thus, from the above-mentioned research it was noticed that the cloud computing environment were found to be challenged by numerous vulnerable attacks and complex issues such as IP spoofing, DDOS, port scanning, virtual machine attacks, probe, R2L and U2R attacks.

Traditional firewalls follows network protocols, network protection is based on ports, protocols, and IP addresses etc. and they are not intelligent enough to discriminate different types of network traffic. Hence alternatives to the traditional firewalls are next generation firewalls (NGFWs). The top five advantages of NGFWs are, i) multi-functional, ii) application awareness, iii) streamlined infrastructure, iv) threat protection and v) network speed.

Xiangjian He et al. [39] designed and implemented a novel firewall namely, Tree-Rule firewall, in that the rules are presented in a tree based data structure.

D. Cryptography

Cryptographic mechanisms are used to secure the cloud data and services. It is a direct approach to achieve the security in the cloud.

Strong encryption of customers' data can be performed by using algorithms such as Diffie-Hellman, Ron Rivest, Adi Shamir, and Leonard Adleman (RSA), Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) and Triple DES. These algorithms are broadly classified as either symmetric or asymmetric algorithms. Hybrid Cryptographic System integrates the benefits of both symmetric and asymmetric encryption.

Strong authentication mechanisms such as multifactor authentication along with multiple levels of hashing and encryption techniques can also be provided to secure the data in cloud against unauthorized access.

V. CLOUD SECURITY SOLUTIONS THROUGH MACHINE LEARNING APPROACHES

This section provides the details about the machine learning techniques for detection of threats and attacks possible in cloud. In this section, we will study the existing work related to threats and attacks in cloud computing addressed through the application of machine learning techniques to provide security in cloud.

Machine learning can be defined as a field of study of computer algorithms that improve automatically through experience. Machine leaning techniques such as support vector machines, K-nearest neighbors classification,Logistic regression, Naive Bayes classification, Boosting, Random Forest, C4.5, C5.0, Expectation-maximization, Feed forward neural networks, K-means clustering, fuzzy logic, artificial neural networks, and genetic algorithms etc.

Some of the machine learning approaches reviewed on attack detection and these are presented as follows.

1. Pannu et al. [55] presented anomaly detection system, based on support vector machine (SVM) for validating cloud dependability assurance. In contrast to the anomaly detection system presented in this work, unlabelled observed data are used, which are processed by a support vector machine algorithm.

2. Han et al. [56]proposed a defense mechanism against co-resident attacks on virtual machines in cloud and prevention of co-residence attacks by applying clustering analysis, and constructed multiple semi-supervised SVMs. This approach identifies the behavioral differences between illegal and legal users, and this approach classifies all users into three categories low, medium, and high riskby applying semi-supervised learning techniques. The attacker's overall cost is increased dramatically by one to two orders of magnitude because attackers are forced to behavesimilarly to legitimate users.

3. Salman et al. [57]investigated detection of eight major types of anomalies in the cloud environment on UNSW dataset by applying Random Forest and Linear Regression techniques and proved that RandomForestgivesabetteraccuracythan the Linear regression, and also categorized the different attacks with a step-wise attack categorization by using Random Forest and accuracy of categorization is less due to similarities between attacks.

4. Sarat[58] implemented the detection of DoS attacks through feature-based selection method to choose the subset of significant features on KDD dataset then the selected features are given as an input to the classification models such as Random Forest, Decision trees, Kth Nearest Neighbor (KNN), and Naive Bayes etc.

5. Bhamare et al. [59] investigated machine learning models trained with a single dataset generally result in a semantic gap between results and their application, but there is a lack of the effectiveness of these models across multiple datasets obtained in different environments. In this approach, models are trained with supervised machine learning algorithms on UNSW dataset and tested these models with ISOT dataset and results shown that threat detection accuracy rate is very low. The limitation of approach is that the models trained and tested with data from one single environment may not perform well with other datasets in the cloud.

6. Masetic et al. [60] proposed threat classification model based on the machine learning algorithms to detect threats and also considered three different criteria namely, i) the type of learning algorithm like supervised or unsupervised learning, ii) input features to the model, and iii)based on type of threats such as, network specific threats or cloud specific threats.

7. Iyengar et al. [61] proposed a fuzzy logic based mechanism to detect DDoS attacks. The model is first trained with training data set withpredefined rules as per traffic pattern, and also considered some predefined parameters that vary significantly between a normal traffic pattern and attack traffic pattern and detecting malicious packets as output.

8. Raj Kumar et al. [62] proposed neural network classifier, which collects the incoming traffic and compared with the sample traffic. If the current traffic shows any deviation, then the attack is detected.

9. Chen et al. [63] proposed a packet scoring and confidence-based filtering approach to identify threats, which acquire the normal profile and also the attack profile, which has its own computation to predict whether a packet is legitimate or is an attack packet, based on the obtained packet score. Now, based on the score, the packets are allowed to access the server for further processing or filtered outside the network. This mechanism lacks dynamism to detect the attack scenario when the network is extended.

10. Nie et al. [64] proposed the Bayesian network based model to detect the network threats, in which the joint probability distribution of network traffic was obtained.

A comparative analysis of recent research work related to threat and attack detection systems are shown in the Table V.

TABLE V

A Comparative analysis of Threat and Attack Detection Systems

Authors	**Method(s)**	**Dataset(s)**	**Threat/ Attack**	**Accuracy Rate**
Watson et al. [65]	One-class Support Vector Machine (SVM)	Tcp Dump, CAIDA's CoralReef	Malware and DoS Attacks	90%
Mishra et al. [66]	Decision Tree, C 4.5, SVM, and Naïve Bayes	University of New Mexico	Malware Attacks	72%-99%.
Gupta et al.[67]	Immediate System Call Signature Structure	University of New Mexico	Malware Attacks	98%
Nagarajan et al. [68]	Adaptive Neuro Fuzzy Inference System Using Back Propagation Gradient Descent Technique with Least Square Method	DARPA's KDD	Normal, DoS, Probe, U2R, R2L	93.72%, 99.77%, 77.3%, 83.30%, 94.49%
Ge et al. [69]	Memory analysis and fuzzy C-means Clustering	200 Normal Programs and Malicious Programs	Advanced Persistent Threats	90%
Berk Gulmezoglu et al. [70]	Support Vector Machines	40 Benchmark Applications	Last-Level Cache(LLC) Leakage	98% (L1 cache) and 78% (LLC)
Tara Salman et al. [57]	Linear Regression (LR) and Random Forest (RF)	UNSW	DoS Attacks	99%

Authors	**Method(s)**	**Dataset(s)**	**Threat/ Attack**	**Accuracy Rate**
Guha et al. [71]	Artificial Neural Network and Genetic Algorithms	NSL-KDD Cup	DoS, Probe, U2R and R2L	90%
Guha et al. [71]	Artificial Neural Network and Genetic Algorithms	UNSW-NB15	Analysis, DoS , Generic, Exploits, Backdoor, Fuzzers, Shellcode, Reconnaissance, and Worms	90%
Lihua Wu et al. [72]	Automatic Malware Signature Discovery System	10 Million Benign Samples and 35K Malware Samples	Malware	80%
Zhang et al. [73]	Transforming Model and Classifier Model using Naïve Bayes	50.1GB Web Logs	Web-based Attacks	98%
Iyengar et al. [61]	Fuzzy Logic	Simulated Dataset	DDoS-Flooding Attacks	86.93%
Zecheng He et al. [74]	Supervised and Unsupervised techniques	Four DDoS attacks and generate the features of real attacks	DDoS Attacks	66.53% to 99.73%
Moustafa et al. [75]	Decision Trees(DT), Logistic Regression(LR), Naïve-Bayes(NB), Artificial Neural Net works(ANN)	KDD99	Probe, DoS, U2R and R2L	92.30% (DT), 92.75% (LR), 95% (NB), 97.04% (ANN)
Moustafa et al. [75]	Decision Trees(DT), Logistic Regression(LR), Naïve-Bayes (NB), Artificial Neural Net works(ANN), Expectation-Maximization(EM)	UNSW-NB15	Analysis, DoS , Generic, Exploits, Backdoor, Fuzzers, Shellcode, Reconnaissance, and Worms	85.56% (DT), 83.15% (LR), 82.07% (NB), 81.34% (ANN), 78.47% (EM)
Kumar et al. [76]	Integrated Feature Set Using Decision Tree, Random Forest, KNN, Logistic Regression, Linear Discriminant Analysis and Naive Bayes	122 Malware Samples and 30 Benign Samples	Malware Attacks	98%
Q.K.A. Mirza et al. [46]	Boosting on Decision Tree	150000 Malicious and 87000 Benign Files	Malware Attacks	99%

A comprehensive analysis on the security threats and attacks in the cloud computing environment are analyzed based on the above researches. From the aforementioned exhaustive research review it was observed that the proposed models are trained and tested on different datasets. Further the features are captured based on the experimental setup. However, these experimental results are found to be different when compared to the real-time applications as all the possible scenarios could not be considered. Besides, it is noticed that with the change in the behavior of network, the patterns were noticed to change leading to the evolution of the intrusions and the type of attacks on the cloud system.

VI. OPEN CHALLENGING ISSUES

In this section, we consider some open challenging issues such as

1. As the openness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by other unauthorized users. So that protecting users confidential information against a data breaches attack is a highly challenging issue.
2. Development of an advanced machine learning algorithm must be able to improve the accuracy detection and categorization of different types of attacks.
3. The rapid advancement in the cloud computing technology and network has led to the increase in issues in the network security. Thus, it is necessary to model and design an appropriate system to detect the increasing threats in the networks.
4. The complexity involved in the cloud system need to be considered, as these are comprised of numerous components that are developed by the diverse teams and are uploaded in the online system independently. Thus, it was noticed that there are several challenges in maintaining the behavior models for the complex cloud computing system.
5. Any machine learning algorithm should be able to detect variety attacks, rather than a single and specific type of attack.
6. What measures or mechanisms will organizations use to defence APTs since they are almost impossible to detect or stop?
7. Detection of malicious insider attacks can easily compromise data. For example, an administrator responsible for performing regular backups of the systems where client resources are hosted (virtual machines, data stores), could exploit the fact that administrator have a centralized access to data thus, exfiltrate sensitive user data. Detecting such indirect access to confidential and protected data can be a challenging task.
8. When applied to cloud security, development of sophisticated machine learning technique provides fast and accurate threat detection, including zero-day and previously unknown threats is a challenging task.
9. Even though the traditional methodologies will not completely identify those threats or does not provide solutions for the threats. So, it is important to develop an efficient system that could completely identify and eradicate the threats.

VII. CONCLUSION

In this paper, we surveyed existing work to address security issues, threats and attacks in the cloud and provided solutions through various technologies and techniques such as cryptography, software defined networking, next generation firewalls, Intrusion detection and prevention systems and machine learning techniques and also addressed some open challenging issues for further research. So, appropriate countermeasures should be taken care to solve the security issues. Finally, we conclude that machine learning techniques attract the researchers and play a significant role in detecting threats and attacks.

REFERENCES

[1] S. S. Manvi and G. Krishna Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 41, no. 1, pp. 424–440, 2014.

[2] A. Bahga and V. Medisetti, *Cloud Computing A hands-on Approach*. India: University Press, 2014.

[3] J. Brodkin, "Gartner: Seven cloud-computing security risks," *InfoWorld*, July, pp. 2–3, 2008.

[4] R. Padhy, M. Patra, and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges,"*Int. J. Comp. Sci. and Inf. Technol. & Sec*, vol. 1, no. 2, pp. 136–146, 2011.

[5] M. K. Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj, and P. Revathy, "State-of-the-art cloud computing security taxonomies - A classification of security challenges in the present cloud computing environment," in *Proc. Int. Conf. Adv. Comput. Commun. Informatics - ICACCI '12*, p. 470, 2012.

[6] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[7] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, 2017.

[8] Z. Wang, "Security and Privacy Issues within the Cloud Computing," in *Proc.Int. Conf. Comput. Inf. Sci.,* pp. 175–178, 2011.

[9] M. D. H. Parekh, "An Analysis of Security Challenges in Cloud Computing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 38–46, 2013.

[10] Abhinay B. Angadi, Akshata B. Angadi, and K. C. Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey," *Int. J. Adv. Res. Comp. Eng. Technol.*, vol. 2, no. 2, pp. 652–661, 2013.

[11] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey," *Adv. in Comp. and Comm.*, vol. 193, pp. 445-454, 2011.

[12] T. Radwan, M. A. Azer, and N. Abdelbaki, "Cloud computing security: challenges and future trends," *Int. J. Comput. Appl. Technol.*, vol. 55, no. 2, p. 158, 2017.

[13] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data Security and Privacy in Cloud Computing," *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014.

[14] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 5, pp. 1–13, 2013.

[15] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592,

2012.

[16] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” *Inf. Sci. (Ny).*, vol. 305, pp. 357–383, 2015.

[17] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, “Cloud computing features, issues, and challenges: A big picture,” in *Proc.1st Int. Conf. Comput. Intell. Networks,* pp. 116–123, 2015.

[18] S. Singh, Y. S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” *J. Netw. Comput. Appl.*, vol. 75, no. September 2016, pp. 200–222, 2016.

[19] L. Coppolino, S. D’Antonio, G. Mazzeo, and L. Romano, “Cloud security: Emerging threats and current solutions,” *Comput. Electr. Eng.*, vol. 59, pp. 126–140, 2017.

[20] P. Kumar, “Cloud Computing : Threats , Attacks and Solutions,” *Int. J. Emer. Technol. Eng. Research*, vol. 4, no. 8, pp. 24–28, 2016.

[21] S. Iqbal *et al.*, “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” *J. Netw. Comput. Appl.*, vol. 74, pp. 98–120, 2016.

[22] Y. Z. An, Z. F. Zaaba, and N. F. Samsudin, “Reviews on Security Issues and Challenges in Cloud Computing,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 160, no. 1, 2016.

[23] T. Chou, “Security Threats on Cloud Computing,” *Int.J.Comput.Sci. Inf. Technol.*, vol. 5, no. 3, pp. 79–88, 2013.

[24] D. H. Parekh and D. R. Sridaran, “An Analysis of Security Challenges in Cloud Computing,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 3–46, 2013.

[25] M. Ahmed, A. T. Litchfield, and S. Ahmed, “A Generalized Threat Taxonomy for Cloud Computing,” *https://en.wikipedia.org/wiki/List_of_data_breaches*, 2017.

[26] M. Jouini, L. B. A. Rabai, and A. Ben Aissa, “Classification of security threats in information systems,”*Procedia Comput. Sci.*, vol. 32, pp. 489–496, 2014.

[27] Cloud Security Alliance, “The Treacherous 12 Cloud Computing Top Threats in 2016,” 2016.

[28] S. Gupta and P. Kumar, “Taxonomy of cloud security,”*Int. J. Comput. Sci. Eng. Appl., v*ol. 3, no. 5, pp. 47–67, 2013.

[29] S. Ruj, M. Stojmenovic, and A. Nayak, “Decentralized access control with anonymous authentication of data stored in clouds,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394, 2014.

[30] E. E. Mon and T. T. Naing, “The privacy-aware access control system using attribute-and role-based access control in private cloud,” in *Proc. 4th IEEE Int. Conf. Broadband Netw. Multimed. Technol.*, pp. 447–451, 2011.

[31] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, “Secure overlay cloud storage with access control and assured deletion,” *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 6, pp. 903–916, 2012.

[32] L. Wei *et al.*, “Security and privacy for storage and computation in cloud computing,” *Inf. Sci. (Ny).*, vol. 258, pp. 371–386, 2014.

[33] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5789, pp. 587–604, 2009.

[34] Z. Wan, J. Liu, and R. H. Deng, “Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing,” *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 2, pp. 743–754, 2013.

[35] S. J. Yang, P. C. Lai, and J. Lin, “Design role-based multi-tenancy access control scheme for cloud services,” in *Proc. Int. Symp. Biometrics Secur. Technol.*, no. 1, pp. 273–279, 2013.

[36] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” *Inf. Sci. (Ny).*, vol. 258, pp. 355–370, 2014.

[37] R. V Gandhi, M. Seshaiah, A. Srinivas, and C. Reddineelima, “Data Back-Up and Recovery Techniques for Cloud Server Using Seed Block Algorithm,” *Int. J. Eng. Res. Appl.*, vol. 5, no. 2, pp. 89–93, 2015.

[38] L. Sun, J. An, and Y. Yang, “Recovery Strategies for Service Composition in Dynamic Network,” *Sci. Technol.*, pp. 60–64, 2011.

[39] X. He, T. Chomsiri, P. Nanda, and Z. Tan, “Improving cloud network security using the Tree-Rule firewall,” *Futur. Gener. Comput. Syst.*, vol. 30, no. 1, pp. 116–126, 2014.

[40] M.Jouini, A. T. Litchfield, and S. Ahmed, “A Generalized Threat Taxonomy for Cloud Computing,” in *Proc.25th Australasian Conference on Information Systems*, 2014.

41] A. S. Ibrahim, J. Hamlyn-harris, J. Grundy, and M. Almorsy, “CloudSec : A Security Monitoring Appliance for Virtual Machines in the IaaS Cloud Model,” in *proc. 5th International Conference on Network and System Security,* pp. 113–120, 2011.

[42] J. Li, Bo Li, T Wo, C Hu, J Huai, Lu Liu, and K.P. Lam, “CyberGuarder: A virtualization security assurance architecture for green cloud computing,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 2, pp. 379–390, 2012.

[43] S. Chow, Y. He, L. Hui, and S. Yiu, “Spice–simple privacy-preserving identity-management for cloud environment,” *Appl. Cryptogr. Netw.* pp. 526–543, 2012.

[44] N. C. Sriman, N. Iyengar, Gopinath Ganapathy, Ajith Abraham,and P. C. M. Kumar, “A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment,” Int. J. Grid and Utility Comp., vol. 5, no. 4, pp. 236–248, 2014.

[45] M. N. Ismail, A. Aborujilah, S. Musa, and Aa. Shahzad, “Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach,” in *Proc. 7th international conference on ubiquitous information management and communication*, 2013, p. 36.

[46] Q. K. A. Mirza, I. Awan, and M. Younas, “CloudIntell : An Intelligent Malware Detection System,” *Futur. Gener. Comput. Syst.*, 2017.

[47] N. Jeyanthi and N. C. S. N. Iyengar, “Packet Resonance Strategy : A Spoof Attack Detection and Prevention Mechanism in Cloud Computing Environment,” *Int. J.Comm.Netw. Inf. Secur.,* vol. 4, no. 3, pp. 163–173, 2012.

[48] Y. Han, T. Alpcan, J. Chan, C. Leckie, and B. I. P. Rubinstein, “A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 556–570, 2016.

[49] Y. Han, J. Chan, and C. Leckie, “Virtual Machine Allocation Policies against Co-resident Attacks in Cloud,” in *Proc. IEEE International Conference on Communications,* pp. 786–792, 2014.

[50] J. Shi, X. Song, H. Chen, and B. Zang, “Limiting Cache-based Side-Channel in Multi-tenant Cloud using Dynamic Page Coloring,” in *Proc.IEEE 41st International Conference on Dependable Systems and Networks Workshops,* pp. 194–199,2011.

[51] Q. Yan, F. R. Yu, S. Member, Q. Gong, and J. Li, “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments : A Survey , Some Research Issues, and Challenges,” *IEEE Communications Surveys & Tutorials*, pp. 1–23, 2015.

[52] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, “DDoS attack protection in the era of cloud computing and Software-Defined Networking,” *Comput. Networks*, vol. 81, pp. 308–319, 2015.

[53] A. AlEroud and I. Alsmadi, “Identifying cyber-attacks on software defined networks: An inference-based intrusion detection

approach," *J. Netw. Comput. Appl.*, vol. 80, pp. 152–164, 2017.

[54] W. Meng, K. K. R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, "Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 4537, pp. 1–13, 2018.

[55] H. S. Pannu, J. Liu, and S. Fu, "AAD: Adaptive anomaly detection system for cloud computing infrastructures," in *Proc. IEEE Symp. Reliab. Distrib. Syst.*, pp. 396–397, 2012.

[56] Y. Han, T. Alpcan, J. Chan, C. Leckie, and B. I. P. Rubinstein, "A Game Theoretical Approach to Defend Against Co-Resident Attacks in Cloud Computing : Preventing Co-Residence Using Semi-Supervised Learning," *IEEE Transactions on Information Forensics And Security*, vol. 11, no. 3, pp. 556–570, 2016.

[57] T. Salman, D. Bhamare, A. Erbad, R. Jain, and M. Samaka, "Machine Learning for Anomaly Detection and Categorization in Multi-Cloud Environments," in *Proc.IEEE Int. Conf. Cyber Secur. Cloud Comput.* pp. 97–103, 2017.

[58] S. Akasapu, "An Integrated Approach for detecting DDoS attacks in Cloud Computing,"*Int. J. Rec. Inn. Comp. and Comm.,* vol.5, no.6 , pp. 258–261, 2017.

[59] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, "Feasibility of Supervised Machine Learning for Cloud Security," in *Proc.IEEE Int. Conf. Inf. Sci. Secur.*, pp. 31–35, 2016.

[60] Z. Masetic, K. Hajdarevic, and N. Dogru, "Cloud computing threats classification model based on the detection feasibility of machine learning algorithms," in *Information and Communication Technology, Electronics and Microelectronics,* pp. 1314–1318, *2017*.

[61] N. C. S. N. Iyengar, A. Banerjee, and G. Ganapathy, "A Fuzzy Logic based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment," *Int. J . Comm. Netw.Inf. Secur.,* vol. 6, no. 3, pp. 233–245, 2014.

[62] P. A. Raj Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," *Comput. Commun.*, vol. 34, no. 11, pp. 1328–1341, 2011.

[63] Q. Chen, W. Lin, and W. Dou, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Futur. Gener. Comput. Syst.*,Vol. 29, no.7, pp 1838-1850,2013.

[64] L. Nie, D. Jiang, and Z. Lv, "Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks," *Ann. Telecommun.*, vol. 72, no. 5, pp. 297–305, 2017.

[65] M. R. Watson, N. U. H. Shirazi, A. K. Marnerides, A. Mauthe, and D. Hutchison, "Malware Detection in Cloud Computing Infrastructures," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 2, pp. 192–205, 2016.

[66] P. Mishra, E. S. Pilli, V. Varadharajan, and U. K. Tupakula, "Securing Virtual Machines from Anomalies Using Program-Behavior Analysis in Cloud Environment," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun.* pp. 991–998, 2016.

[67] S. Gupta and P. Kumar, "An Immediate System Call Sequence Based Approach for Detecting Malicious Program Executions in Cloud Environment," *Wirel. Pers. Commun.*, vol. 81, no. 1, pp. 405–425, 2015.

[68] P. Nagarajan and G. Perumal, "A neuro fuzzy based intrusion detection system for a cloud data center using adaptive learning," *Cybern. Inf. Technol.*, vol. 15, no. 3, pp. 88–103, 2015.

[69] L. Ge, L. Wang, and L. Xu, "An APT Trojans Detection Method for Cloud Computing Based on Memory Analysis and FCM," in *Proc.3rd Int. Conf. Inf. Sci. Control Eng.*, pp. 179–183, 2016.

[70] B. Gulmezoglu, T. Eisenbarth, and B. Sunar, "Cache-Based Application Detection in the Cloud Using Machine Learning," in *Proc.ACM Asia Conf. Comput. Commun. Secur.*, pp. 288–300, 2017.

[71] S. Guha, S. S. Yau, and A. B. Buduru, "Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection," in *Proc.IEEE 14th Intl Conf Dependable, Auton. Secur. Comput.* pp. 414–419, 2016.

[72] W. Yan and E. Wu, "Toward automatic discovery of malware signature for anti-virus cloud computing," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 4 pp. 724–728, 2009.

[73] S. Zhang, B. Li, J. Li, M. Zhang, and Y. Chen, "A Novel Anomaly Detection Approach for Mitigating Web-Based Attacks Against Clouds," in *Proc.2nd IEEE Int. Conf. Cyber Secur. Cloud Comput.* pp. 289–294, 2016.

[74] Z. He, T. Zhang, and R. B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput.*, pp. 114–120, 2017.

[75] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Inf. Secur. J.*, vol. 25, no. 1–3, pp. 18–31, 2016.

[76] A. Kumar, K. S. Kuppusamy, and G. Aghila, "A Learning Model to Detect Maliciousness of Portable Executable using Integrated Feature Set," *Comput. Inf. Sci.*, vol. 31, pp. 252-265, 2019.

AUTHOR PROFILE

Dr. Gopal Krishna Shyam is a Professor in school of Computing and Information Technology at Reva University, Bengaluru, India. He received BE and M.Tech and Ph.D in Computer science and engineering from VTU, Belagavi, India. He has handled several subjects for UG/PG Students like Algorithms, Computer Networks, Web programming, Advanced Computer architecture, Information security, Computer Concepts and C Programming. His research interest includes Cloud computing, Grid computing, High performance computing etc. He has published about 10 papers in highly reputed National/International Conferences like IEEE, Elsevier etc. and 5 papers in Journals with high impact factor like Elsevier Journal on Network and Computer Applications and International Journal of Cloud computing (INDERSCIENCE). His research articles on Cloud computing co-authored by Dr. Sunilkumar S. Manvi have been cited by several researchers. He is a lifetime member of CSI and is actively involved in motivating students/faculties to join CSI/IEEE/ACM societies.

Ms. Doddi Srilatha is presently working as an Assistant Professor in Department of Computer Science and Engineering in Sreenidhi Institute of Science and Technology, Hyderabad, India. She received B.Tech and M.Tech from JNTU Hyderabad, India. She is a PhD research scholar at Reva University, Bengaluru, India. Her research interests include: Cloud security, data mining, and machine learning.